

Complementos de Matemática II

Licenciatura en Ciencias de la Computación



Departamento de Matemática - Departamento de Ciencias de la Computación

Escuela de Ciencias Exactas y Naturales

Facultad de Ciencias Exactas, Ingeniería y Agrimensura

Universidad Nacional de Rosario

Equipo docente: Francisco Vittone, Delfina Martín, Katherine Sullivan

Índice general

Capítulo 1. Relaciones y funciones	1
§1.1. Introducción	1
§1.2. Relaciones	2
§1.3. Representación matricial y grafo de una relación	6
§1.4. Operaciones entre relaciones	9
§1.5. Propiedades de las relaciones en un conjunto	15
§1.6. Clases de equivalencia y conjunto cociente	20
§1.7. Ejercicios	25
Capítulo 2. Conjuntos ordenados	31
§2.1. Conjuntos parcialmente ordenados (Posets)	31
§2.2. Elementos minimales, maximales, mínimos y máximos	35
§2.3. Buen orden en \mathbb{N} y sus consecuencias	38
§2.4. Subconjuntos acotados, ínfimo y supremo	44
§2.5. Morfismos de posets	48
§2.6. El Axioma de Elección, el Lema de Zorn y el Principio de Buena Ordenación.	54
§2.7. Ejercicios	63
Capítulo 3. Retículos	67
§3.1. Definición y primeros ejemplos	67
§3.2. Las operaciones “join” y “meet”	70
§3.3. Subretículos	74
§3.4. Morfismos de retículos	76
§3.5. Retículos acotados y complementados	82

§3.6. Retículos distributivos y modulares	86
§3.7. Álgebras de Boole	97
§3.8. Ejercicios	107
Capítulo 4. Semigrupos, monoides y grupos	111
§4.1. Operaciones binarias	111
§4.2. Subconjuntos cerrados, productos y cocientes	118
§4.3. Semigrupos, monoides y grupos	124
§4.4. Potencias	129
§4.5. Subestructuras	134
§4.6. Grupos cíclicos	140
§4.7. Morfismos	142
§4.8. Ejercicios	149
Capítulo 5. Grupos	153
§5.1. Coclasas a derecha e izquierda	153
§5.2. Subgrupos normales y grupo cociente	157
§5.3. Primer Teorema de Isomorfismo	162
§5.4. Propiedades y clasificación de los grupos cíclicos	166
§5.5. Producto directo y producto libre de grupos	170
§5.6. Aplicaciones a la aritmética modular	184
§5.7. Ejercicios	189
Capítulo 6. Categorías	195
§6.1. Breve digresión sobre la Teoría de Conjuntos	195
§6.2. Primeras definiciones y ejemplos	198
§6.3. Funtores	206
§6.4. Monomorfismos, epimorfismos e isomorfismos	213
§6.5. Objetos iniciales, terminales y nulos	224
§6.6. Productos y coproductos	225
§6.7. Ecualizadores y coecualizadores	237
§6.8. Conos, coconos, límites y colímites	243
§6.9. Exponenciales - Categorías cartesianas cerradas.	249
§6.10. Ejercicios	255
Capítulo 7. Equivalencias, adjunciones y mónadas	261

§7.1. Transformaciones naturales	261
§7.2. Equivalencias de categorías	265
§7.3. Adjunciones.	274
§7.4. Mónadas	280
§7.5. Lema de Yoneda	282
§7.6. Ejercicios	284
Bibliografía	287

Relaciones y funciones

1.1. Introducción

Las relaciones entre elementos de distintos conjuntos aparecen naturalmente en todas las ramas de la matemática, y constituyen posiblemente uno de los conceptos más claros e intuitivos. Supongamos que tenemos un conjunto A formado por todas las personas nacidas en la provincia de Santa Fe y un conjunto B formado por todas las ciudades de la provincia y nos interesa saber en qué localidad nació cada persona. Podemos establecer una relación entre los elementos del conjunto A y los del conjunto B que coloquialmente indicamos como “la persona x está relacionada con la localidad y si x nació en y ”. Si indicamos $x \mathcal{R} y$ si x nació en y , tendremos por ejemplo los siguientes elementos relacionados:

Fito Paez \mathcal{R} Rosario, Luciana Aymar \mathcal{R} Rosario, Lionel Scaloni \mathcal{R} Pujato,

Soledad Pastorutti \mathcal{R} Arequito, José Pedroni \mathcal{R} Gálvez

Una forma diferente de denotar estos elementos relacionados es directamente listarlos como pares, claramente ordenados, donde el primer elemento del par debe pertenecer a A y el segundo a B . Así, una forma equivalente de denotar a la relación \mathcal{R} es

(Fito Paez,Rosario), (Luciana Aymar,Rosario), (Lionel Scaloni,Pujato)

(Soledad Pastorutti,Arequito), (José Pedroni,Gálvez)

Que los pares deben ser ordenados (es decir, que importa el orden en que los listemos para que la relación tenga sentido) resulta claro dado que expresiones como Rosario \mathcal{R} Fito Paez carecen de sentido, pues deberían leerse como “Rosario nació en Fito Paez”.

La relación que acabamos de definir es de un tipo muy particular: es de hecho una *función*, dado que a cada elemento del conjunto A se le “asigna” un único elemento del conjunto B . Como función, \mathcal{R} es claramente no inyectiva, pues muchas personas distintas pueden haber nacido en la misma localidad, y por lo tanto no admite una función inversa.

Podemos sin embargo definir una relación \mathcal{R}' entre los elementos de B y los de A que sea $x \in B$ está relacionado con $y \in A$ si x es la localidad de nacimiento de y . La relación parecería ser la misma, solo que estamos invirtiendo el orden de los elementos. Así tendremos

Rosario \mathcal{R}' Fito Paez, Rosario \mathcal{R}' Luciana Aymar, Pujato \mathcal{R}' Lionel Scaloni, etc.

que como pares ordenados denotaremos como $(\text{Rosario}, \text{Fito Paez})$, $(\text{Rosario}, \text{Luciana Aymar})$, $(\text{Pujato}, \text{Lionel Scaloni})$, etc. A diferencia de lo que ocurre con \mathcal{R} , en la relación \mathcal{R}' cada elemento de B estará relacionado con muchos elementos de A (dado que cada ciudad es lugar de nacimiento de muchas personas). Por lo tanto \mathcal{R}' no es una función. Como veremos, tiene sentido hablar de la relación inversa de una relación dada, con lo cual las relaciones generalizan y permiten en muchos casos entender mejor el concepto de función. Abordaremos estos y otros conceptos en las próximas secciones, comenzamos dando una definición formal de qué entendemos por una relación. Más detalles sobre los temas que aquí trataremos pueden encontrarse en [10, 13, 20]

1.2. Relaciones

Dados dos conjuntos A y B hemos visto que resulta bastante intuitivo qué se entiende por una relación entre los elementos de A y los elementos de B . Sin embargo, cualquier forma de expresar esto coloquialmente (por ejemplo diciendo que una relación entre A y B es una correspondencia entre los elementos de A y de B , o es una ley que asigna a los elementos de A uno o algunos elementos de B) no es lo suficientemente formal como para poder utilizarla en las distintas áreas de la matemática. Para dar una definición “correcta”, aunque menos intuitiva, basta notar que toda relación entre A y B queda completamente definida por los pares ordenados (x, y) , con $x \in A$ e $y \in B$ que pretendemos que estén relacionados. De esta manera tenemos:

Definición 1.2.1. Sean A y B dos conjuntos. Una **relación** \mathcal{R} de A en B es un subconjunto \mathcal{R} del producto cartesiano $A \times B = \{(a, b) : a \in A, b \in B\}$. Si $A = B$, una relación de A en A se dice una **relación** (o relación binaria) en A .

Notación 1.2.2. Si \mathcal{R} es una relación de A en B y $(a, b) \in \mathcal{R}$, lo denotaremos también por $a \mathcal{R} b$, que leemos “ a está relacionado con b por la relación \mathcal{R} ”. Si a no está relacionado con b , o sea $(a, b) \notin \mathcal{R}$, lo denotaremos también por $a \not\mathcal{R} b$.

Como cualquier conjunto, una relaciones puede definirse por extensión (listando todos los pares ordenados que constituirán sus elementos) o por comprensión, dando alguna propiedad que la defina. En este último caso solemos hablar de la “ley” que define la relación. Sin embargo es importante notar que hay muchas formas diferentes de dar una misma relación por comprensión.

En los ejemplos de la introducción, las relaciones están dadas por comprensión, aunque es posible, si desearamos, listarlas por extensión dado que tanto el conjunto A de personas nacidas en la provincia de Santa Fe como el conjunto B de todas las localidades de la provincia son conjuntos finitos. Veamos ahora otros ejemplos:

Ejemplo 1.2.3. Relaciones triviales. Existen dos relaciones particulares de un conjunto A en un conjunto B , denominadas *relaciones triviales*, y están dadas por $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = A \times B$. En la primera, ningún elemento de A está relacionado con ningún elemento de B , y en la segunda cualquier elemento de A está relacionado con todos los elementos de B .

Ambas pueden darse por comprensión de muchas maneras distintas. Tomemos por ejemplo $A = \mathbb{R}^+$, $B = \mathbb{R}^-$. Entonces

$$\mathcal{R}_1 = \{(x, y) \in A \times B : x \cdot y \in \mathbb{R}\} = \{(x, y) \in A \times B : x \cdot y < 0\} = A \times B$$

$$\mathcal{R}_0 = \{(x, y) \in A \times B : x \cdot y > 0\} = \{(x, y) \in A \times B : y = x^2\} = \emptyset$$

■

Ejemplo 1.2.4. Sea $B = \{1, 2\}$ y sea $A = \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Definamos la siguiente relación binaria en A :

$$\mathcal{R} = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}$$

En este caso \mathcal{R} está dada por extensión. Es fácil verificar que \mathcal{R} también puede definirse comprensión por

$$C \mathcal{R} D \iff C \subset D.$$

o equivalentemente

$$\mathcal{R} = \{(C, D) : C, D \subset B \wedge C \subset D\}.$$

■

Ejemplo 1.2.5. Sea $i \in \mathbb{C}$ la unidad imaginaria y definamos una relación en \mathbb{Z} pidiendo que $m \mathcal{R} n$ si $i^m = i^n$. Como bien sabemos, las potencias de i se repiten en ciclos de 4, esto es $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$ y a partir de allí todas se repiten. Tomemos $m \in \mathbb{Z}$ cualquiera y escribamos $m = 4k + r$, donde $0 \leq r < 4$ pues es el resto de dividir m por 4. Luego

$$i^m = i^{4k+r} = i^{4k} i^r = (i^4)^k i^r = 1^k i^r = i^r.$$

Concluimos que $m \mathcal{R} n$ si m y n tienen el mismo resto al dividirlos por 4. Resulta claro en este caso que $m \mathcal{R} n$ si y sólo si $n \mathcal{R} m$.

Además si escribimos $m = 4k + r$, $n = 4k' + r'$, entonces

$$m \mathcal{R} n \iff r = r' \iff m - n \text{ es múltiplo de } 4$$

(dejamos como ejercicio verificar esta última equivalencia). Si denotamos por $r_4(m)$ el resto de dividir m por 4, entonces:

$$\begin{aligned} \mathcal{R} &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : i^m = i^n\} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : r_4(m) = r_4(n)\} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n - m = 4k \text{ para algún } k \in \mathbb{Z}\}. \end{aligned}$$

son todas formas de definir por comprensión la misma relación.

■

Ejemplo 1.2.6. Consideremos la relación \mathcal{R} de \mathbb{N} en \mathbb{Z} dada por $x \mathcal{R} y$ si $y = x/2$. Entonces

$$\mathcal{R} = \{(x, y) \in \mathbb{N} \times \mathbb{Z} : y = x/2\}.$$

Podemos observar que existen elementos de \mathbb{N} que no están relacionados con ningún elemento de \mathbb{Z} . Por ejemplo, dado $x = 1 \in \mathbb{N}$, no existe $y \in \mathbb{Z}$ tal que $y = 1/2$. De la misma manera, si $y \in \mathbb{Z}$ y $y \leq 0$, no existe ningún $x \in \mathbb{N}$ tal que $x \mathcal{R} y$, dado que $x/2$, en caso de ser entero, es siempre positivo. ■

A partir de lo observado en el ejemplo 1.2.6, resulta importante definir los siguientes subconjuntos de A y B respectivamente:

Definición 1.2.7. Sea \mathcal{R} una relación de A en B . El **dominio** de \mathcal{R} es el subconjunto de A dado por

$$\text{Dom}(\mathcal{R}) = \{a \in A : \exists b \in B / (a, b) \in \mathcal{R}\}$$

La **imagen** de \mathcal{R} es el subconjunto de B dado por

$$\text{Im}(\mathcal{R}) = \{b \in B : \exists a \in A / (a, b) \in \mathcal{R}\}$$

Ejemplo 1.2.8. Consideremos las relaciones $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = A \times B$. Entonces es inmediato verificar que $\text{Dom}(\mathcal{R}_0) = \emptyset$ e $\text{Im}(\mathcal{R}_0) = \emptyset$, y $\text{Dom}(\mathcal{R}_1) = A$ e $\text{Im}(\mathcal{R}_1) = B$.

Por otra parte, para la relación \mathcal{R} del Ejemplo 1.2.6, tenemos que

$$\text{Dom}(\mathcal{R}) = \{x \in \mathbb{N} : \exists y \in \mathbb{Z} / y = x/2\} = \{x \in \mathbb{N} : x = 2y \text{ para algún } y \in \mathbb{Z}\}$$

es el conjunto de los naturales pares. Por otro lado, si $y \in \mathbb{Z}^+$, existe $x = 2y \in \mathbb{N}$ tal que $x \mathcal{R} y$. Pero si $y \in \mathbb{Z}$ es tal que $y \leq 0$, no existe $x \in \mathbb{N}$ tal que $y = x/2$, con lo cual $y \notin \text{Im}(\mathcal{R})$. Concluimos que $\text{Im}(\mathcal{R}) = \mathbb{Z}^+ = \mathbb{N}$. ■

Definición 1.2.9. Sean A y B dos conjuntos. Una **función parcial** de A en B es una relación \mathcal{R} de A en B tal que cada elemento de A está relacionado con a lo sumo un elemento de B , es decir:

- si $(x, y) \in \mathcal{R}$ y $(x, y') \in \mathcal{R}$, entonces $y = y'$.

Si \mathcal{R} es una función parcial que además verifica que $\text{Dom}(\mathcal{R}) = A$ (es decir, todo elemento de A está relacionado con un único elemento de B), \mathcal{R} se denomina una **relación funcional**, o directamente una **función** de A en B . Es decir, \mathcal{R} es una función de A en B si se cumplen:

- para todo $x \in A$, existe $y \in B$ tal que $(x, y) \in \mathcal{R}$ (o sea que $\text{Dom}(\mathcal{R}) = A$);
- si $(x, y) \in \mathcal{R}$ y $(x, y') \in \mathcal{R}$, entonces $y = y'$.

Notación 1.2.10. Como es usual, denotaremos una relación funcional o una función parcial \mathcal{R} de A en B por $f : A \rightarrow B$. Si $(a, b) \in \mathcal{R}$, dado que b es el único elemento de B relacionado con a , lo denotamos como de costumbre $b = f(a)$. El dominio y la imagen de \mathcal{R} se denotan por $\text{Dom}(f)$ e $\text{Im}(f)$ respectivamente. Observemos que si f es una función, $\text{Dom}(f) = A$.

Si $X \subset A$ denotamos por $f(X)$ al subconjunto de B dado por

$$f(X) = \{b \in B : b = f(a) \text{ para algún } a \in X\}$$

En particular, $\text{Im}(f) = f(A)$.

Si $Y \subset B$, denotamos por $f^{-1}(Y)$ al subconjunto de A dado por

$$f^{-1}(Y) = \{a \in \text{Dom}(f) : f(a) \in Y\}.$$

En el caso particular de $Y = \{b\}$, $b \in B$, denotamos a $f^{-1}(\{b\})$ directamente por $f^{-1}(b)$, es decir,

$$f^{-1}(b) = \{a \in A : f(a) = b\}.$$

Ejemplo 1.2.11. La relación \mathcal{R} del Ejemplo 1.2.6 es una función parcial, dado que si $(x, y), (x, y') \in \mathcal{R}$, entonces $y = x/2 = y'$. Sin embargo no es una función pues $\text{Dom}(\mathcal{R}) \subsetneq \mathbb{N}$. ■

Finalizaremos esta sección introduciendo las propiedades básicas que puede tener una función:

Definición 1.2.12. Sea $f : A \rightarrow B$ una relación funcional. Decimos que f es:

- **inyectiva** si para cada $x \neq x' \in A$, $f(x) \neq f(x')$, o equivalentemente, si se verifica que para cada $x, x' \in A$

$$f(x) = f(x') \implies x = x'.$$

- **sobreyectiva** si $\text{Im}(f) = B$, o sea, para cada $y \in B$, existe $x \in A$ tal que $f(x) = y$.
- **biyectiva** si f es inyectiva y sobreyectiva.

Teorema 1.2.13. Sean A y B conjuntos finitos, no vacíos, del mismo cardinal $|A| = |B| = n$ y $f : A \rightarrow B$ una función. Entonces las siguientes afirmaciones son equivalentes:

1. f es biyectiva.
2. f es inyectiva.
3. f es sobreyectiva.

Demostración. Que la propiedad 1 implica la propiedad 2 es trivial.

Veamos que 2 implica 3. Supongamos que $f : A \rightarrow B$ es una función inyectiva. Entonces $\text{Im}(f)$ también tiene cardinal n . Como $\text{Im}(f) \subset B$ y ambos conjuntos tienen el mismo cardinal, resulta $\text{Im}(f) = B$. Luego f es sobreyectiva.

Veamos ahora que 3 implica 1. Supongamos entonces que $f : A \rightarrow B$ es sobreyectiva. Entonces $\text{Im}(f) = B$ y por lo tanto $\text{Im}(f)$ tiene el mismo cardinal que B , y por lo tanto que A . Si f no fuese inyectiva, debería ser $|\text{Im}(f)| < |A|$, lo que lleva a una contradicción. Luego f es inyectiva y por lo tanto biyectiva. □

1.3. Representación matricial y grafo de una relación

En el caso de relaciones entre conjuntos finitos, existe una forma muy efectiva de representar la relación a través de una matriz:

Definición 1.3.1. Si A y B son conjuntos finitos y \mathcal{R} es una relación de A en B , podemos ordenar los elementos de ambos conjuntos poniendo $A = \{a_1, a_2, \dots, a_n\}$, $B = \{b_1, b_2, \dots, b_m\}$. Construimos una matriz $n \times m$ que denotamos por $M(\mathcal{R})$ del modo siguiente: si M_{ij} denota la entrada ij de la matriz $M(\mathcal{R})$ entonces

$$M_{ij} = \begin{cases} 1 & \text{si } (a_i, b_j) \in \mathcal{R} \\ 0 & \text{si } (a_i, b_j) \notin \mathcal{R} \end{cases}$$

$M(\mathcal{R})$ se denomina la **matriz de la relación** \mathcal{R} .

Ejemplo 1.3.2. Es fácil verificar que las matrices de las relaciones triviales $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = A \times B$ de un conjunto finito A en un conjunto finito B son la matriz nula (cuyas entradas son todas 0) en el primer caso, y la matriz cuyas entradas son todos 1 en el segundo. ■

Ejemplo 1.3.3. Consideremos a relación \mathcal{R} de $A = \{0, 1, 2, 3, 4, 5\}$ en $B = \{2, 4, 6, 8\}$ dada por $x \mathcal{R} y$ si $y = 2x$. Entonces

$$M(\mathcal{R}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Como podemos observar en cada fila de $M(\mathcal{R})$ hay a lo sumo un 1, y todos los demás elementos son 0. Esto nos indica que \mathcal{R} es una función parcial de A en B , pues cada elemento de A está relacionado con a lo sumo un elemento de B .

Para determinar el dominio de \mathcal{R} basta encontrar los elementos de A que corresponden a filas no idénticamente nulas (lo que indica que son elementos de A relacionados con algún elemento). Así, $\text{Dom}(\mathcal{R}) = \{1, 2, 3, 4\}$. Para determinar la imagen, debemos encontrar los elementos de B que corresponden a las columnas que presentan al menos un 1 (o sea, no sean idénticamente nulas). En este caso, $\text{Im}(\mathcal{R}) = \{2, 4, 6, 8\} = B$. ■

A través del análisis de la matriz $M(\mathcal{R})$ de una relación podemos identificar si se trata de una función parcial o de una función, y en este último caso, si es inyectiva y/o sobreyectiva. Resumimos estas propiedades en el siguiente resultado, cuya prueba dejamos como **ejercicio**.

Lema 1.3.4. Sea \mathcal{R} una relación de $A = \{a_1, \dots, a_m\}$ en $B = \{b_1, \dots, b_n\}$ y sea $M(\mathcal{R}) = (M_{ij})$ la matriz de \mathcal{R} . Pongamos f_i la i -ésima fila de $M(\mathcal{R})$ y c_j la j -ésima columna de $M(\mathcal{R})$, $i = 1, \dots, m$, $j = 1, \dots, n$. Decimos que $f_i = 0$ si $M_{ij} = 0$ para cada $j = 1, \dots, n$ y que $c_j = 0$ si $M_{ij} = 0$ para cada $i = 1, \dots, m$. Entonces

1. $\text{Dom}(\mathcal{R}) = \{a_i \in A : f_i \neq 0\}$.
2. $\text{Im}(\mathcal{R}) = \{b_j \in B : c_j \neq 0\}$.
3. \mathcal{R} es una función parcial si y sólo si para cada $i = 1, \dots, m$, f_i tiene a lo sumo una entrada no nula.
4. \mathcal{R} es una función si y sólo si para cada $i = 1, \dots, m$, f_i tiene exactamente una entrada no nula.
5. Si \mathcal{R} es una función, \mathcal{R} es inyectiva si y sólo si para cada $j = 1, \dots, n$, c_j tiene a lo sumo una entrada no nula.
6. Si \mathcal{R} es una función, \mathcal{R} es sobreyectiva si y sólo si $c_j \neq 0$ para cada $j = 1, \dots, n$.

Ejemplo 1.3.5. Sean $A = \{a_1, a_2, a_3\}$ y $B = \{b_1, b_2, b_3, b_4\}$ y consideremos la relación \mathcal{R} de A en B cuya matriz (para esa ordenación de los elementos de A y B) es

$$M(\mathcal{R}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

De la matriz podemos obtener que $\mathcal{R} = \{(a_1, b_2), (a_2, b_3), (a_3, b_1)\}$. En cada fila de la matriz hay un único 1, y por lo tanto \mathcal{R} es una relación funcional. Además en cada columna hay a lo sumo un 1, y por lo tanto deducimos que se trata de una función inyectiva. Por último, como hay una columna nula, la función no es sobreyectiva. En efecto, $\text{Im}(\mathcal{R}) = \{b_1, b_2, b_3\} \neq B$. ■

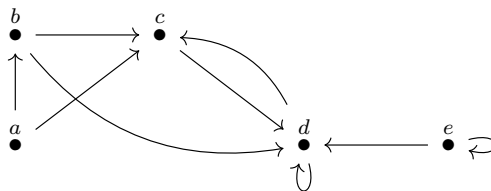
Cuando $A = B$, o sea \mathcal{R} es una relación en A , y A es un conjunto finito, podemos representar la relación a través de un grafo dirigido:

Definición 1.3.6. Sea V un conjunto finito no vacío. Un **grafo dirigido** (o **digrafo**) G sobre V está formado por los elementos de V , llamados **vértices** o **nodos** de G y un subconjunto E de $V \times V$, cuyos elementos se denominan **aristas dirigidas** o **arcos** de G . Denotamos $G = (V, E)$ a un grafo dirigido cuyos vértices son los elementos de V y cuyas aristas son los elementos de E .

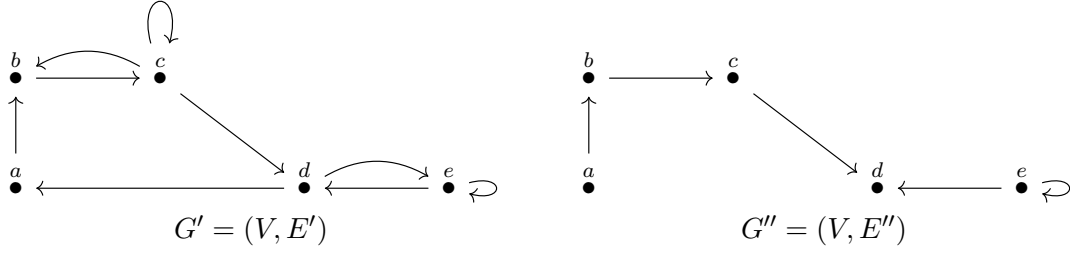
Si $(a, b) \in E$, la arista se representa gráficamente con una flecha dirigida de a hacia b . Una arista de la forma (a, a) se denomina un **lazo** o **bucle** en a .

Si $G' = (V', E')$ es un grafo dirigido tal que $V' \subseteq V$ y $E' \subseteq E$, decimos que G' es un **subgrafo** de G y lo denotamos $G' \subseteq G$.

Ejemplo 1.3.7. Sea $V = \{a, b, c, d, e\}$ y sea $E = \{(a, b), (a, c), (b, c), (b, d), (c, d), (d, c), (d, d), (e, d), (e, e)\}$. Entonces el grafo dirigido $G = (V, E)$ se representa de la manera siguiente:



Consideremos ahora $G' = (V, E')$ donde $E' = \{(a, b), (b, c), (c, b), (c, c), (c, d), (d, a), (d, e), (e, d), (e, e)\}$ y sea $G'' = (V, E'')$ donde $E'' = E \cap E'$. Estos grafos se representan como sigue:



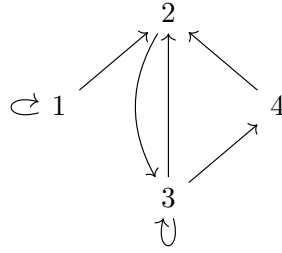
Como el conjunto de vértices V es común a los tres grafos y $E'' = E \cap E'$, resulta que G'' es un subgrafo tanto de G como de G' . ■

Definición 1.3.8. Si \mathcal{R} es una relación en el conjunto finito no vacío A , el **grafo dirigido asociado a \mathcal{R}** es aquel cuyos vértices son los elementos de A y sus aristas son los elementos de \mathcal{R} , es decir, $G = (A, \mathcal{R})$.

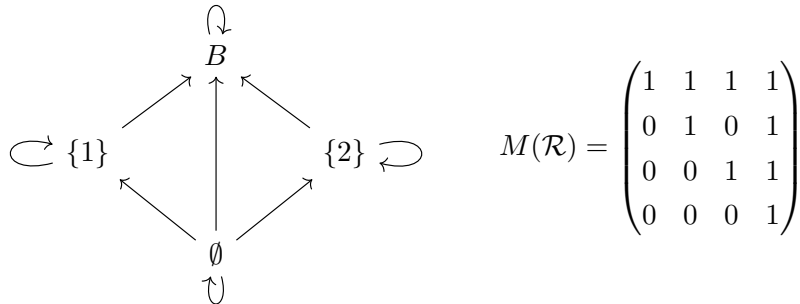
Ejemplo 1.3.9. Consideremos $A = \{1, 2, 3, 4\}$ y \mathcal{R} la relación en A cuya matriz asociada es

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Entonces $\mathcal{R} = \{(1, 1), (1, 2), (2, 3), (3, 2), (3, 3), (3, 4), (4, 2)\}$ y su grafo dirigido asociado es



Ejemplo 1.3.10. Consideremos el conjunto $B = \{1, 2\}$ y la relación \mathcal{R} en $A = \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, B\}$ dada por $C \mathcal{R} D$ si $C \subseteq D$. Entonces el grafo dirigido de \mathcal{R} y la matriz de \mathcal{R} son los siguientes:



1.4. Operaciones entre relaciones

En esta sección introduciremos el concepto de *relación inversa* de una relación dada y distintas operaciones entre relaciones.

Definición 1.4.1. Sea $\mathcal{R} \subset A \times B$ una relación de A en B . Se define la **relación inversa** de \mathcal{R} como la relación $\mathcal{R}^{-1} \subset B \times A$ de B en A dada por

$$\mathcal{R}^{-1} = \{(b, a) \in B \times A : (a, b) \in \mathcal{R}\}.$$

Lema 1.4.2. Sea \mathcal{R} una relación de A en B y \mathcal{R}^{-1} su relación inversa. Entonces:

1. $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.
2. $\text{Dom}(\mathcal{R}^{-1}) = \text{Im}(\mathcal{R})$ e $\text{Im}(\mathcal{R}^{-1}) = \text{Dom}(\mathcal{R})$.

Demostración. Probemos el punto 1. Observemos que

$$(x, y) \in (\mathcal{R}^{-1})^{-1} \iff (y, x) \in \mathcal{R}^{-1} \iff (x, y) \in \mathcal{R}$$

con lo cual $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.

Veamos ahora el punto 2. Supongamos que $b \in \text{Dom}(\mathcal{R}^{-1})$. Entonces existe $a \in A$ tal que $(b, a) \in \mathcal{R}^{-1}$, es decir, $(a, b) \in \mathcal{R}$, con lo cual $b \in \text{Im}(\mathcal{R})$. Luego $\text{Dom}(\mathcal{R}^{-1}) \subset \text{Im}(\mathcal{R})$. La otra contención es análoga.

La segunda igualdad es inmediata del punto 1. En efecto, $\text{Im}(\mathcal{R}^{-1}) = \text{Dom}((\mathcal{R}^{-1})^{-1}) = \text{Dom}(\mathcal{R})$. \square

Ejemplo 1.4.3. Si $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = A \times B$ son las relaciones triviales de A en B , entonces sus inversas son las respectivas relaciones triviales de B en A , es decir, $\mathcal{R}_0^{-1} = \emptyset$ y $\mathcal{R}_1^{-1} = B \times A$. \blacksquare

Ejemplo 1.4.4. Consideremos la relación \mathcal{R} del Ejemplo 1.2.5 tenemos que

$$(n, m) \in \mathcal{R}^{-1} \iff (m, n) \in \mathcal{R} \iff m - n \text{ es múltiplo de } 4 \iff n - m \text{ es múltiplo de } 4 \iff (n, m) \in \mathcal{R}$$

con lo cual $\mathcal{R}^{-1} = \mathcal{R}$. \blacksquare

Ejemplo 1.4.5. Consideremos la relación dada en el Ejemplo 1.3.5 de $A = \{a_1, a_2, a_3\}$ en $B = \{b_1, b_2, b_3, b_4\}$,

$$\mathcal{R} = \{(a_1, b_2), (a_2, b_3), (a_3, b_1)\}.$$

Entonces $\mathcal{R}^{-1} = \{(b_2, a_1), (b_3, a_2), (b_1, a_3)\}$. Observemos que las matrices de \mathcal{R} y \mathcal{R}^{-1} están dadas por

$$M(\mathcal{R}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad M(\mathcal{R}^{-1}) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

es decir, $M(\mathcal{R}^{-1}) = M(\mathcal{R})^\top$, donde M^\top representa la matriz transpuesta de M .

\mathcal{R} es una relación funcional inyectiva con $\text{Dom}(\mathcal{R}) = A$ e $\text{Im}(\mathcal{R}) = \{b_1, b_2, b_3\}$, con lo cual $\text{Dom}(\mathcal{R}^{-1}) = \text{Im}(\mathcal{R}) = \{b_1, b_2, b_3\} \neq B$ y por lo tanto \mathcal{R}^{-1} no es una relación funcional. Pero como

\mathcal{R} es inyectiva, las columnas de \mathcal{R} , que coinciden con las filas de $M(\mathcal{R}^{-1})$, tienen a lo sumo un 1 y por lo tanto \mathcal{R}^{-1} es una función parcial. ■

Lema 1.4.6. Sean A y B conjuntos finitos, \mathcal{R} una relación de A en B y $M(\mathcal{R})$ la matriz de \mathcal{R} . Entonces la matriz de \mathcal{R}^{-1} es $M(\mathcal{R}^{-1}) = (M(\mathcal{R}))^\top$.

Demostración. Observemos que la entrada ij de $M(\mathcal{R}^{-1})$ es

$$M(\mathcal{R}^{-1})_{ij} = \begin{cases} 1 & \text{si } (b_i, a_j) \in \mathcal{R}^{-1} \\ 0 & \text{si } (b_i, a_j) \notin \mathcal{R}^{-1} \end{cases} = \begin{cases} 1 & \text{si } (a_j, b_i) \in \mathcal{R} \\ 0 & \text{si } (a_j, b_i) \notin \mathcal{R} \end{cases} = M(\mathcal{R})_{ji}$$

con lo cual $M(\mathcal{R}^{-1}) = M(\mathcal{R})^\top$ como queríamos ver. □

Lema 1.4.7. Sea \mathcal{R} una relación funcional. Entonces

1. \mathcal{R} es inyectiva si y sólo si \mathcal{R}^{-1} es una función parcial.
2. \mathcal{R}^{-1} es una relación funcional si y sólo si \mathcal{R} es biyectiva.

Demostración. Probemos el punto 1. Supongamos que $\mathcal{R} = f$ es una relación funcional inyectiva de A en B . Sea $b \in B$ y sean $a, a' \in A$ tales que $(b, a), (b, a') \in \mathcal{R}^{-1}$. Entonces $(a, b), (a', b) \in \mathcal{R}$, es decir, $b = f(a) = f(a')$. Como \mathcal{R} es inyectiva, $a = a'$ y por lo tanto \mathcal{R}^{-1} es una función parcial.

Supongamos ahora que \mathcal{R}^{-1} es una función parcial y sean $a, a' \in A$ tales que $f(a) = f(a') = b$, es decir, $(a, b), (a', b) \in \mathcal{R}$. Entonces $(b, a), (b, a') \in \mathcal{R}^{-1}$, y como \mathcal{R}^{-1} es una función parcial deberá ser $a = a'$, con lo cual \mathcal{R} es inyectiva.

Para probar el punto 2, supongamos primero que $\mathcal{R} = f$ es una relación funcional biyectiva. Entonces \mathcal{R} es en particular inyectiva y por el punto 1 \mathcal{R}^{-1} es una función parcial. Como además \mathcal{R} es sobreyectiva, entonces $\text{Im}(\mathcal{R}) = B$ y por lo tanto $\text{Dom}(\mathcal{R}^{-1}) = \text{Im}(\mathcal{R}) = B$. Luego \mathcal{R}^{-1} es una relación funcional.

Supongamos finalmente que $\mathcal{R} = f$ es una relación funcional tal que \mathcal{R}^{-1} también es una relación funcional. Entonces por el punto 1 \mathcal{R} es inyectiva. Además $\text{Im}(\mathcal{R}) = \text{Dom}(\mathcal{R}^{-1}) = B$, y por lo tanto \mathcal{R} es sobreyectiva. Concluimos que \mathcal{R} es biyectiva. □

Dadas dos relaciones \mathcal{R} y \mathcal{R}' de A en B , como ambas son subconjuntos de $A \times B$, podemos aplicar a ellas las operaciones usuales entre conjuntos y obtener nuevas relaciones de A en B . Definimos:

Definición 1.4.8. Si \mathcal{R} y \mathcal{R}' son relaciones de A en B , entonces se definen:

- la relación **complemento** de \mathcal{R} como $\mathcal{C}\mathcal{R} = \{(a, b) \in A \times B : (a, b) \notin \mathcal{R}\}$;
- la relación **unión** de \mathcal{R} y \mathcal{R}' como $\mathcal{R} \cup \mathcal{R}' = \{(a, b) : a \mathcal{R} b \vee a \mathcal{R}' b\}$;
- la relación **intersección** de \mathcal{R} y \mathcal{R}' como $\mathcal{R} \cap \mathcal{R}' = \{(a, b) : a \mathcal{R} b \wedge a \mathcal{R}' b\}$;
- la relación **diferencia** de \mathcal{R} y \mathcal{R}' como $\mathcal{R} - \mathcal{R}' = \{(a, b) : (a, b) \in \mathcal{R} \wedge (a, b) \notin \mathcal{R}'\}$

Ejemplo 1.4.9. Para las relaciones triviales de un conjunto A en un conjunto B cualquiera, $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = A \times B$, es inmediato verificar que $\mathcal{C}\mathcal{R}_0 = \mathcal{R}_1$, $\mathcal{C}\mathcal{R}_1 = \mathcal{R}_0$, $\mathcal{R}_0 \cap \mathcal{R}_1 = \mathcal{R}_0$, $\mathcal{R}_0 \cup \mathcal{R}_1 = \mathcal{R}_1$. ■

Ejemplo 1.4.10. Consideremos las relaciones “ $<$ ”, “ \leq ”, “ $>$ ”, “ \geq ” y “ $=$ ” en \mathbb{R} . Entonces tendremos $\mathcal{C} \geq$ es $<$; $\mathcal{C} >$ es \leq ; $(= \cup <)$ es \leq ; $(= \cup >)$ es \geq ; $(\leq - =)$ es $<$; $(\leq \cup >)$ es \mathcal{R}_1 ; $(\leq \cap >)$ es \mathcal{R}_0 donde $\mathcal{R}_0 = \emptyset$ y $\mathcal{R}_1 = \mathbb{R} \times \mathbb{R}$ son las relaciones triviales en \mathbb{R} . ■

Ejemplo 1.4.11. Supongamos que \mathcal{R} y \mathcal{R}' son dos relaciones de un conjunto $A = \{a_1, a_2, a_3\}$ en $B = \{b_1, b_2, b_3, b_4\}$ dadas por las siguientes matrices:

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M(\mathcal{R}') = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Es posible determinar todas las operaciones entre \mathcal{R} y \mathcal{R}' observando simplemente las matrices de ambas relaciones (sin necesidad de expresarlas por extensión). Por ejemplo, para encontrar la matriz de $\mathcal{C}\mathcal{R}$, basta observar que si una entrada de $M(\mathcal{R})$ es 1, entonces la correspondiente entrada de $M(\mathcal{C}\mathcal{R})$ debe ser 0, y viceversa. Por lo tanto, la matriz de $M(\mathcal{R})$ es

$$M(\mathcal{C}\mathcal{R}) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Determinemos ahora la matriz de $\mathcal{R} \cup \mathcal{R}'$. A esta nueva relación pertenecen todos los pares de elementos de $A \times B$ que pertenezcan a \mathcal{R} o a \mathcal{R}' . Por lo tanto, siempre que en $M(\mathcal{R})$ o en $M(\mathcal{R}')$ una entrada sea 1, la correspondiente entrada en $M(\mathcal{R} \cup \mathcal{R}')$ será 1. Dicho de otra forma, una entrada en $M(\mathcal{R} \cup \mathcal{R}')$ es cero si y sólo si las correspondientes entradas en $M(\mathcal{R})$ y $M(\mathcal{R}')$ son ambas cero. Por lo tanto tenemos que

$$M(\mathcal{R} \cup \mathcal{R}') = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Al contrario de lo que ocurre con la unión, en $\mathcal{R} \cap \mathcal{R}'$ están los pares de elementos que pertenecen a ambas relaciones. Por lo tanto una entrada de $M(\mathcal{R} \cap \mathcal{R}')$ será 1 si y sólo si las correspondientes entradas de $M(\mathcal{R})$ y $M(\mathcal{R}')$ son ambas 1. Así.

$$M(\mathcal{R} \cap \mathcal{R}') = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Finalmente, en $\mathcal{R} - \mathcal{R}'$ están aquellos pares que pertenecen a \mathcal{R} y no pertenecen a \mathcal{R}' . Por lo tanto una entrada en $M(\mathcal{R} - \mathcal{R}')$ es 1 si y sólo si la entrada correspondiente de $M(\mathcal{R})$ es 1 y la entrada correspondiente de $M(\mathcal{R}')$ es 0. Así

$$M(\mathcal{R} - \mathcal{R}') = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Observemos que otra forma de encontrar $M(\mathcal{R} - \mathcal{R}')$ es pensar que $\mathcal{R} - \mathcal{R}' = \mathcal{R} \cap (\mathcal{C}\mathcal{R}')$. ■

Observando el ejemplo anterior, introduciremos dos operaciones en el conjunto $\{0, 1\}$, denominadas *operaciones Booleanas*, que nos permitirán determinar la matriz de las distintas operaciones entre relaciones a partir de las matrices de las relaciones dadas.

Definición 1.4.12. Se denomina **suma booleana** en $\{0, 1\}$ a una operación que denotamos por \oplus definida por

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \quad 1 \oplus 1 = 1.$$

Denominamos **producto booleano** en $\{0, 1\}$ a una operación que denotamos por \odot , definida por

$$0 \odot 0 = 0, \quad 0 \odot 1 = 1 \odot 0 = 0, \quad 1 \odot 1 = 1.$$

Observación 1.4.13. El producto booleano, a diferencia de la suma, coincide con el producto usual de números reales. Sin embargo, los valores 0 o 1 representan, en general, valores de verdad de proposiciones. En este contexto, la operación \oplus coincide “or” (\vee) y \odot coincide con “and” (\wedge).

Definición 1.4.14. Sean $M = (M_{ij})$ y $N = (N_{ij})$ dos matrices $m \times n$ cuyas entradas pertenecen a $\{0, 1\}$.

- Denominamos **complemento de M** a la matriz que denotamos $\neg M$ cuyas entradas son

$$(\neg M)_{ij} = \begin{cases} 0 & \text{si } M_{ij} = 1 \\ 1 & \text{si } M_{ij} = 0 \end{cases}$$

- la **suma booleana de M y N** es una matriz $m \times n$ que denotamos $M \oplus N$ cuyas entradas son $(M \oplus N)_{ij} = M_{ij} \oplus N_{ij}$.
- el **producto puntual de M y N** es una matriz $m \times n$ que denotamos $M \odot N$, cuyas entradas son $(M \odot N)_{ij} = M_{ij} \odot N_{ij}$.

Ejemplo 1.4.15. Consideremos las matrices $M(\mathcal{R})$ y $M(\mathcal{R}')$ de las relaciones \mathcal{R} y \mathcal{R}' del Ejemplo 1.4.11. Entonces

$$\neg M(\mathcal{R}) = \neg \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = M(\mathcal{C}\mathcal{R}).$$

Por otro lado,

$$\begin{aligned} M(\mathcal{R}) \oplus M(\mathcal{R}') &= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \oplus 1 & 0 \oplus 1 & 0 \oplus 1 & 1 \oplus 1 \\ 0 \oplus 0 & 1 \oplus 0 & 1 \oplus 0 & 1 \oplus 1 \\ 0 \oplus 0 & 0 \oplus 1 & 0 \oplus 0 & 0 \oplus 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = M(\mathcal{R} \cup \mathcal{R}') \end{aligned}$$

Además

$$\begin{aligned} M(\mathcal{R}) \odot M(\mathcal{R}') &= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \odot 1 & 0 \odot 1 & 0 \odot 1 & 1 \odot 1 \\ 0 \odot 0 & 1 \odot 0 & 1 \odot 0 & 1 \odot 1 \\ 0 \odot 0 & 0 \odot 1 & 0 \odot 0 & 0 \odot 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = M(\mathcal{R} \cap \mathcal{R}'). \end{aligned}$$

Finalmente, es fácil comprobar que $M(\mathcal{R} - \mathcal{R}') = M(\mathcal{R} \cap (\mathcal{R}')) = M(\mathcal{R}) * (\neg M(\mathcal{R}'))$. ■

Resumimos en el siguiente resultado cómo obtener la matriz de las distintas operaciones entre relaciones a partir de las matrices de dos relaciones dadas. La prueba sigue un razonamiento análogo al que hicimos en el Ejemplo 1.4.11 y la dejamos como **ejercicio**.

Lema 1.4.16. Sean \mathcal{R} y \mathcal{R}' dos relaciones de $A = \{a_1, \dots, a_m\}$ en $B = \{b_1, \dots, b_n\}$ cuyas matrices son $M(\mathcal{R})$ y $M(\mathcal{R}')$ respectivamente (para un orden determinado de los elementos de A y B). Entonces:

1. La matriz de $\mathcal{C}\mathcal{R}$ es $M(\mathcal{C}\mathcal{R}) = \neg M(\mathcal{R})$.
2. La matriz de $\mathcal{R} \cup \mathcal{R}'$ es $M(\mathcal{R} \cup \mathcal{R}') = M(\mathcal{R}) \oplus M(\mathcal{R}')$.
3. La matriz de $\mathcal{R} \cap \mathcal{R}'$ es $M(\mathcal{R} \cap \mathcal{R}') = M(\mathcal{R}) \odot M(\mathcal{R}')$.
4. La matriz de $\mathcal{R} - \mathcal{R}'$ es $M(\mathcal{R} - \mathcal{R}') = M(\mathcal{R}) \odot (\neg M(\mathcal{R}'))$.

Si ahora tenemos una relación \mathcal{R} de un conjunto A en un conjunto B y una relación \mathcal{R}' de B en un conjunto C , podemos definir su *composición*:

Definición 1.4.17. Sean \mathcal{R}_1 una relación de A en B y \mathcal{R}_2 una relación de B en C . Se denomina **composición** de \mathcal{R}_1 y \mathcal{R}_2 a la relación de A en C dada por

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(a, c) \in A \times C : \exists b \in B / (a, b) \in \mathcal{R}_1 \wedge (b, c) \in \mathcal{R}_2\}.$$

Ejemplo 1.4.18. Sea $A = \{1, 2, 3, 4\}$, $B = \{x, y, z, w\}$, $C = \{5, 6, 7\}$. Consideremos la relación \mathcal{R} de A en B dada por $\mathcal{R}_1 = \{(1, x), (2, x), (3, y), (3, z)\}$ y las relaciones \mathcal{R}' y \mathcal{R}'' de B en C dadas por $\mathcal{R}' = \{(x, 6), (w, 5)\}$, $\mathcal{R}'' = \{(w, 5), (w, 6)\}$. Entonces tendremos que $\mathcal{R}' \circ \mathcal{R} = \{(1, 6), (2, 6)\}$, $\mathcal{R}'' \circ \mathcal{R} = \emptyset$. ■

Para determinar la matriz de la composición de relaciones entre conjuntos finitos introduciremos una nueva operación entre matrices con entradas en $\{0, 1\}$:

Definición 1.4.19. Si M es una matriz $m \times l$ y N es una matriz $l \times n$, el **producto booleano** de M y N es una matriz $m \times n$ que denotamos $M * N$ cuyas entradas son

$$(M * N)_{ij} = \bigoplus_{k=1}^l M_{ik} \odot N_{kj} = (M_{i1} \odot N_{1j}) \oplus (M_{i2} \odot N_{2j}) \oplus \dots \oplus (M_{il} \odot N_{lj})$$

Ejemplo 1.4.20. Tomemos las matrices $M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ y $N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Podemos hacer el producto $M * N$ siguiendo el esquema usual, pero cambiando la suma y la multiplicación usuales por las respectivas operaciones booleanas:

		0	1	1	
		1	0	0	
					$M * N$
1	0	$(1 \odot 0) \oplus (0 \odot 1)$	$(1 \odot 1) \oplus (0 \odot 0)$	$(1 \odot 1) \oplus (0 \odot 0)$	$= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$
1	1	$(1 \odot 0) \oplus (1 \odot 1)$	$(1 \odot 1) \oplus (1 \odot 0)$	$(1 \odot 1) \oplus (1 \odot 0)$	

■

Ejemplo 1.4.21. Sean $A = \{a_1, a_2\}$, $B = \{b_1, b_2\}$, $C = \{c_1, c_2, c_3\}$ y sean M y N las matrices del Ejemplo 1.4.20. Consideremos las relaciones \mathcal{R} de A en B cuya matriz es $M(\mathcal{R}) = M$ y \mathcal{R}' de B en C cuya matriz es N . Entonces

$$\mathcal{R} = \{(a_1, b_1), (a_2, b_1), (a_2, b_2)\}, \quad \mathcal{R}' = \{(b_1, c_2), (b_1, c_3), (b_2, c_1)\}.$$

Luego

$$\mathcal{R}' \circ \mathcal{R} = \{(a_1, c_2), (a_1, c_3), (a_2, c_2), (a_2, c_3), (a_2, c_1)\}$$

y por lo tanto $M(\mathcal{R}' \circ \mathcal{R}) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = M * N.$

■

Lema 1.4.22. Sean A, B, C conjuntos finitos, \mathcal{R} una relación de A en B y \mathcal{R}' una relación de B en C . Entonces $M(\mathcal{R}' \circ \mathcal{R}) = M(\mathcal{R}) * M(\mathcal{R}')$.

Demostración. Supongamos que $A = \{a_1, \dots, a_n\}$, $B = \{b_1, \dots, b_m\}$, $C = \{c_1, \dots, c_l\}$. Entonces $(a_i, c_j) \in \mathcal{R}' \circ \mathcal{R}$ si y sólo si existe $b_k \in B$ tal que $a_i \mathcal{R} b_k$ y $b_k \mathcal{R}' c_j$. Por lo tanto $M(\mathcal{R}' \circ \mathcal{R})_{ij} = 1$ si y sólo si existe k tal que $M(\mathcal{R})_{ik} = 1$ y $M(\mathcal{R}')_{kj} = 1$.

Ahora bien, observemos que $\bigoplus_{s=1}^m M(\mathcal{R})_{is} M(\mathcal{R}')_{sj} = 1$ si y sólo si existe k tal que $M(\mathcal{R})_{ik} = 1$ y $M(\mathcal{R}')_{kj} = 1$, con lo cual

$$M(\mathcal{R}' \circ \mathcal{R})_{ij} = \bigoplus_{s=1}^m M(\mathcal{R})_{is} \odot M(\mathcal{R}')_{sj} = (M(\mathcal{R}) * M(\mathcal{R}'))_{ij}.$$

Como i y j son índices arbitrarios, concluimos que $M(\mathcal{R}' \circ \mathcal{R}) = M(\mathcal{R}) * M(\mathcal{R}')$. □

En el caso de que dos relaciones sean relaciones funcionales y su composición tenga sentido, la relación resultante de la composición es nuevamente una relación funcional. Dejamos la prueba del siguiente resultado como **ejercicio**:

Lema 1.4.23. Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ dos relaciones funcionales. Entonces $g \circ f$ es una relación funcional y la definición 1.4.17 coincide en este caso con la noción usual de composición de funciones. Más aún, si f y g son inyectivas (resp. sobreyectivas, biyectivas) entonces $g \circ f$ es inyectiva (resp. sobreyectiva, biyectiva).

En muchos casos es útil restringir la relación de un conjunto A en B a subconjuntos de A y B , para obtener una nueva relación. Por ejemplo si \mathcal{R} es una función parcial, su restricción a su dominio dará una relación funcional. Si \mathcal{R} fuese una relación funcional inyectiva, la restricción de B a $Im(\mathcal{R})$ permitirá definir una función biyectiva (y por lo tanto invertible).

Definición 1.4.24. Sea \mathcal{R} una relación de un conjunto A en un conjunto B y sean $A' \subset A$, $B' \subset B$. La **restricción** de \mathcal{R} a $A' \times B'$ es una relación de A' en B' , denotada $\mathcal{R}_{|A' \times B'}$ definida por

$$\mathcal{R}_{|A' \times B'} = \{(a, b) \in A' \times B' : a \mathcal{R} b\} = \mathcal{R} \cap (A' \times B').$$

Ejemplo 1.4.25. Consideremos la relación \mathcal{R} de \mathbb{R} en \mathbb{R} dada por $x \mathcal{R} y$ si y sólo si $x = y^2$. Observemos que \mathcal{R} no es una relación funcional, dado que cada $x \neq 0$ está relacionado con exactamente dos elementos: \sqrt{x} y $-\sqrt{x}$. Podemos considerar la restricción $\mathcal{R}_{|\mathbb{R} \times \mathbb{R}_0^+}$ y obtendremos una relación funcional. ■

Ejemplo 1.4.26. Consideremos la relación \mathcal{R} de un conjunto $A = \{a_1, a_2, a_3\}$ en $B = \{b_1, b_2, b_3, b_4\}$ cuya matriz es

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Tomemos $A' = \{a_1, a_3\}$, $B' = \{b_1, b_4\}$. Entonces para obtener la matriz de $\mathcal{R}_{|A' \times B'}$ identificamos en primer lugar las filas de $M(\mathcal{R})$ correspondientes a los elementos de A' , en este caso se trata de la primera y la cuarta. Nos interesa posteriormente restringirnos a las columnas correspondientes a elementos de B , o sea, la primera y la cuarta.

$$M(\mathcal{R}) = \begin{pmatrix} \boxed{1} & 1 & 1 & \boxed{1} \\ \mathbf{0} & 0 & 0 & 1 \\ \boxed{0} & 1 & 0 & \boxed{0} \end{pmatrix}$$

De esta forma

$$M(\mathcal{R}_{|A' \times B'}) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

o sea que $\mathcal{R}_{|A' \times B'} = \{(a_1, b_1), (a_1, b_2)\}$. Otra forma de obtener $M(\mathcal{R}_{|A' \times B'})$ consiste en eliminar las filas y las columnas de $M(\mathcal{R})$ correspondientes a los elementos que no están en A' (para el caso de las filas) y que no están en B' (para el caso de las columnas). ■

Notación 1.4.27. En el caso de relaciones funcionales solemos restringir la función a un subconjunto del dominio. De esta manera si $f : A \rightarrow B$ es una relación funcional y $A' \subset A$, es usual denotar $f_{|A'} : A' \rightarrow B$ a la restricción $f_{|A' \times B}$. Si \mathcal{R} es además una relación en A y $B \subseteq A$, denotamos $\mathcal{R}_{|B}$ a la restricción $\mathcal{R}_{|B \times B}$.

1.5. Propiedades de las relaciones en un conjunto

En esta sección nos dedicaremos a estudiar relaciones en un conjunto A . En estos casos las relaciones pueden poseer o no una serie de propiedades particulares que dan lugar a las denominadas *relaciones de equivalencia* y *relaciones de orden*.

Definición 1.5.1. Sea \mathcal{R} una relación en un conjunto A . Decimos que \mathcal{R} es:

- **reflexiva** si para cada $x \in A$ se verifica que $x \mathcal{R} x$ (o sea, $(x, x) \in \mathcal{R}$).
- **simétrica** si cada vez que $x \mathcal{R} y$, entonces $y \mathcal{R} x$, esto es,

$$(x, y) \in \mathcal{R} \implies (y, x) \in \mathcal{R}.$$

- **transitiva** si cada vez que $x \mathcal{R} y$ e $y \mathcal{R} z$ entonces $x \mathcal{R} z$, esto es,

$$(x, y) \in \mathcal{R} \wedge (y, z) \in \mathcal{R} \implies (x, z) \in \mathcal{R}.$$

- **antisimétrica** si cada vez que $x \mathcal{R} y$ e $y \mathcal{R} x$ entonces $x = y$, esto es,

$$(x, y) \in \mathcal{R} \wedge (y, x) \in \mathcal{R} \implies x = y.$$

Observación 1.5.2. Observemos que una relación \mathcal{R} en un conjunto A es simétrica si y sólo si se verifica que

$$(x, y) \in \mathcal{R} \iff (y, x) \in \mathcal{R}.$$

En efecto, por definición, tenemos la implicación que si $(x, y) \in \mathcal{R}$ entonces $(y, x) \in \mathcal{R}$. Pero obviamente, si $(y, x) \in \mathcal{R}$, aplicando nuevamente la definición, obtenemos $(x, y) \in \mathcal{R}$.

Ejemplo 1.5.3. La relación trivial $\mathcal{R}_0 = \emptyset$ en un conjunto A cualquiera es simétrica, transitiva y antisimétrica (el antecedente de todas las proposiciones es falso, y por lo tanto la proposición es verdadera). Sin embargo no es reflexiva.

La relación trivial $\mathcal{R}_1 = A \times A$ en un conjunto A cualquiera es trivialmente reflexiva, simétrica y transitiva (pues todos los elementos de A están relacionados con todos los elementos de A) pero no es antisimétrica.

Ejemplo 1.5.4. Relación de igualdad o diagonal. Existe en A una única relación que verifica todas las propiedades listadas en la definición 1.5.1: la relación de *igualdad*, o *relación diagonal*, que denotamos por Δ , y está dada por $a \Delta b$ si y sólo si $a = b$ (la denominación de relación diagonal proviene del hecho que como subconjunto de $A \times A$,

$$\Delta = \{(a, a) : a \in A\},$$

denominado la diagonal de $A \times A$). Observemos que si $A = \{a_1, \dots, a_n\}$ es un conjunto finito, entonces $M(\mathcal{R})_{ij} = 1$ si y sólo si $i = j$. Por lo tanto $M(\mathcal{R}) = \text{Id}_n$, la matriz identidad $n \times n$. ■

Observación 1.5.5. Las únicas relaciones que son al mismo tiempo simétricas y antisimétricas son aquellas en que los elementos de A están relacionados a lo sumo con sí mismos, es decir, \mathcal{R} es simultáneamente simétrica y antisimétrica si y sólo si $\mathcal{R} \subset \Delta$. En efecto, si \mathcal{R} es una relación simétrica en un conjunto A , dados $a, b \in A$ cualesquiera tales que $a \mathcal{R} b$, tendremos también $b \mathcal{R} a$. Si además \mathcal{R} es antisimétrica, entonces tendremos que $a = b$. O sea, $a \mathcal{R} b$ sólo si $a = b$. Si \mathcal{R} es además reflexiva, entonces \mathcal{R} es la relación de igualdad en A .

Ejemplo 1.5.6. Sea \mathcal{R} la relación en \mathbb{N} definida por $a \mathcal{R} b$ si a divide a b (es decir, si existe $k \in \mathbb{N}$ tal que $b = ka$). La relación \mathcal{R} se denota comunmente como “ $|$ ”, es decir, denotamos por $a | b$ para indicar que a divide a b . Entonces

- $\mathcal{R} = |$ es reflexiva: como $a = 1 \cdot a$ cualquiera sea $a \in \mathbb{N}$, resulta que $a | a$.
- $\mathcal{R} = |$ es transitiva: si $a | b$ y $b | c$ quiere decir que existen $k_1, k_2 \in \mathbb{N}$ tales que $b = k_1 a$ y $c = k_2 b$, de donde $c = k_2 b = (k_2 k_1) a$ con $k_2 k_1 \in \mathbb{N}$. Por lo tanto $a | c$.
- $\mathcal{R} = |$ es antisimétrica: si $a | b$ y $b | a$ entonces existen $k_1, k_2 \in \mathbb{N}$ tales que $b = k_1 a$ y $a = k_2 b$, donde $b = (k_1 k_2) b$. Luego $k_1 k_2 = 1$, y como k_1 y k_2 son números naturales debe ser $k_1 = k_2 = 1$, o sea, $a = b$.

La relación claramente no es simétrica pues por ejemplo $1 | 2$ pero $2 \nmid 1$. ■

Ejemplo 1.5.7. Fijemos $m \in \mathbb{Z}$ y definamos una relación \mathcal{R} en \mathbb{Z} poniendo $a \mathcal{R} b$ si $b - a$ es múltiplo de m (un ejemplo particular de esta relación fue visto en el Ejemplo 1.2.5 para $m = 4$). Es decir, $a \mathcal{R} b$ si existe $k \in \mathbb{Z}$ tal que $b - a = km$. Entonces:

- \mathcal{R} es reflexiva: dado $a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot m$ con lo cual $a \mathcal{R} a$.
- \mathcal{R} es simétrica: si $a \mathcal{R} b$ entonces existe $k \in \mathbb{Z}$ tal que $a - b = km$. Pero entonces

$$b - a = -(a - b) = (-k)m$$

con $-k \in \mathbb{Z}$. Por lo tanto $b \mathcal{R} a$.

- \mathcal{R} es transitiva: si $a \mathcal{R} b$ y $b \mathcal{R} c$, existirán $k_1, k_2 \in \mathbb{Z}$ tales que $b - a = k_1 m$ y $c - b = k_2 m$. Sumando miembro a miembro ambas igualdades resulta

$$c - a = (c - b) + (b - a) = (k_2 + k_1)m$$

con lo cual $a \mathcal{R} c$.

Esta relación es particularmente importante y recibe el nombre de **congruencia módulo m** . Volveremos a ella más adelante. ■

Ejemplo 1.5.8. Sea $A = \{a_1, a_2, a_3\}$ y sea \mathcal{R} la relación en A cuya matriz es

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Observemos primero que $M(\mathcal{R})$ tiene todos 1 en la diagonal, es decir que $a_i \mathcal{R} a_i$ para cada $i = 1, 2, 3$, con lo cual \mathcal{R} es reflexiva.

Por otra parte, $M(\mathcal{R})^\top = M(\mathcal{R})$. Esto implica que si $a_i \mathcal{R} a_j$, entonces la entrada ij de la matriz será 1 y al ser $M(\mathcal{R})$ una matriz simétrica también tendremos que la entrada ji es 1, o sea, $a_j \mathcal{R} a_i$. Por lo tanto \mathcal{R} es una relación simétrica.

De la Observación 1.5.5 concluimos que \mathcal{R} no es antisimétrica. Explícitamente, tenemos en este ejemplo particular que $a_1 \mathcal{R} a_3$ y $a_3 \mathcal{R} a_1$ y sin embargo $a_1 \neq a_3$. Observemos finalmente que $a_1 \mathcal{R} a_3$ y $a_3 \mathcal{R} a_2$ pero sin embargo $a_1 \not\mathcal{R} a_2$, con lo cual \mathcal{R} no es transitiva. ■

Lema 1.5.9. *Sea \mathcal{R} una relación en un conjunto A y sea Δ la relación de igualdad en A . Entonces:*

1. \mathcal{R} es reflexiva si y sólo si $\Delta \subset \mathcal{R}$.
2. \mathcal{R} es simétrica si y sólo si $\mathcal{R}^{-1} = \mathcal{R}$.
3. \mathcal{R} es transitiva si y sólo si $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$.
4. \mathcal{R} es antisimétrica si y sólo si $\mathcal{R} \cap \mathcal{R}^{-1} \subset \Delta$.

Demostración. El punto 1 es inmediato, basta notar que $\Delta = \{(a, a) : a \in A\}$ y que \mathcal{R} es reflexiva si y sólo si $(a, a) \in \mathcal{R}$ para cada $a \in A$.

Por otra parte, \mathcal{R} es simétrica si y sólo si para cada $x, y \in A$ se verifica que

$$(x, y) \in \mathcal{R} \iff (y, x) \in \mathcal{R}$$

(ver Observación 1.5.2). Luego, si \mathcal{R} es simétrica,

$$(x, y) \in \mathcal{R}^{-1} \iff (y, x) \in \mathcal{R} \iff (x, y) \in \mathcal{R}$$

con lo cual $\mathcal{R} = \mathcal{R}^{-1}$. Recíprocamente, si $\mathcal{R} = \mathcal{R}^{-1}$ resulta que

$$(x, y) \in \mathcal{R} \iff (x, y) \in \mathcal{R}^{-1} \iff (y, x) \in \mathcal{R}$$

y por lo tanto \mathcal{R} es simétrica. Esto prueba el punto 2.

Sea ahora \mathcal{R} una relación transitiva en A . Sea $(x, z) \in \mathcal{R} \circ \mathcal{R}$. Entonces existe $y \in A$ tal que $(x, y) \in \mathcal{R}$ y $(y, z) \in \mathcal{R}$. Como \mathcal{R} es transitiva, tenemos que $(x, z) \in \mathcal{R}$ con lo cual $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$.

Si ahora suponemos $\mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$ y sean $x, y, z \in A$ tales que $(x, y) \in \mathcal{R}$ y $(y, z) \in \mathcal{R}$. Entonces $(x, z) \in \mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$, con lo cual $(x, z) \in \mathcal{R}$. Luego \mathcal{R} es transitiva. Esto concluye la prueba del punto 3.

Sea finalmente \mathcal{R} una relación antisimétrica. Si $(x, y) \in \mathcal{R} \cap \mathcal{R}^{-1}$ tenemos que $(x, y) \in \mathcal{R}$ y $(x, y) \in \mathcal{R}^{-1}$, con lo cual $(y, x) \in \mathcal{R}$. Como \mathcal{R} es antisimétrica deberá ser $x = y$, es decir, $(x, y) = (x, x) \in \Delta$. Concluimos que $\mathcal{R} \cap \mathcal{R}^{-1} \subset \Delta$.

Supongamos ahora que $\mathcal{R} \cap \mathcal{R}^{-1} \subset \Delta$. Sean $x, y \in A$ tales que $(x, y) \in \mathcal{R}$ y $(y, x) \in \mathcal{R}$. Entonces $(x, y) \in \mathcal{R} \cap \mathcal{R}^{-1}$ y por lo tanto $x = y$. Luego vale el punto 4. □

El Lema 1.5.9 resulta particularmente útil al trabajar con relaciones en conjuntos finitos. Para poder obtener las propiedades de una relación a partir del análisis de su matriz, como hicimos en el Ejemplo 1.5.8, necesitamos poder comparar las entradas de dos matrices:

Definición 1.5.10. *Sean $A = (A_{ij})$ y $B = (B_{ij})$ dos matrices $m \times n$ con entradas en \mathbb{R} . Decimos que $A \leq B$ si $A_{ij} \leq B_{ij}$ para cada $i = 1, \dots, m$, $j = 1, \dots, n$.*

Combinando el Lema 1.5.9 con los Lemas 1.4.16 y 1.4.22 obtenemos inmediatamente el siguiente resultado. Dejamos los detalles de la prueba como **ejercicio**:

Lema 1.5.11. Sea $A = \{a_1, \dots, a_n\}$ un conjunto finito. Sea \mathcal{R} una relación en A y $M(\mathcal{R})$ su matriz. Si Id_n denota la matriz identidad $n \times n$, entonces:

1. \mathcal{R} es reflexiva si y sólo si $\text{Id}_n \leq M(\mathcal{R})$.
2. \mathcal{R} es simétrica si y sólo si $M(\mathcal{R}) = M(\mathcal{R})^\top$.
3. \mathcal{R} es transitiva si y sólo si $M(\mathcal{R}) * M(\mathcal{R}) \leq M(\mathcal{R})$.
4. \mathcal{R} es antisimétrica si y sólo si $M(\mathcal{R}) \odot M(\mathcal{R})^\top \leq \text{Id}_n$.

Finalizamos esta sección introduciendo los conceptos de *equivalencia* y *orden*. Dedicaremos el resto del capítulo a estudiar las relaciones de equivalencia, y abordaremos el estudio de las relaciones de orden en el próximo.

Definición 1.5.12. Una relación \mathcal{R} en un conjunto A se denomina

- un **preorden** si \mathcal{R} es reflexiva y transitiva.
- una relación de **equivalencia** si \mathcal{R} es reflexiva, simétrica y transitiva.
- una relación de **orden** (u **orden parcial**) si \mathcal{R} es reflexiva, antisimétrica y transitiva.

Observación 1.5.13. Toda relación de equivalencia es un preorden y toda relación de orden es un preorden. Sin embargo, como la única relación reflexiva que es simultáneamente simétrica y antisimétrica es la igualdad, ninguna relación distinta de esta puede ser al mismo tiempo una relación de equivalencia y una relación de orden.

Ejemplo 1.5.14. La relación $\mathcal{R} = |$ en \mathbb{N} dada por $a \mathcal{R} b$ si a divide a b definida en el Ejemplo 1.5.6 es una relación de orden.

Consideremos la relación $\mathcal{R} = |$ en \mathbb{Z} . Necesitamos aquí hacer una salvedad: dados $a, b \in \mathbb{Z}$ con $a \neq 0$, decimos que a divide a b si existe $k \in \mathbb{Z}$ tal que $b = ka$. Hemos excluido de la definición la posibilidad de que 0 divida a b , cualquiera sea $b \in \mathbb{Z}$. Por lo tanto \mathcal{R} no es una relación reflexiva, pues $0 \nmid 0$. Con los mismos argumentos que en el Ejemplo 1.5.6 resulta \mathcal{R} una relación transitiva.

Si ponemos $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ la restricción $\mathcal{R}|_{\mathbb{Z}^* \times \mathbb{Z}^*}$ resulta reflexiva y transitiva, por lo tanto es un preorden. Observemos que \mathcal{R} no es antisimétrica pues por ejemplo $1 \mid (-1)$ y $(-1) \mid 1$, siendo $-1 \neq 1$. ■

Ejemplo 1.5.15. Las relaciones \leq y \geq (en \mathbb{N} , \mathbb{Z} , \mathbb{Q} o \mathbb{R}) son relaciones de orden. Observemos que ni $<$ ni $>$ son relaciones de orden, ni siquiera son preordenes, porque no son reflexivas. ■

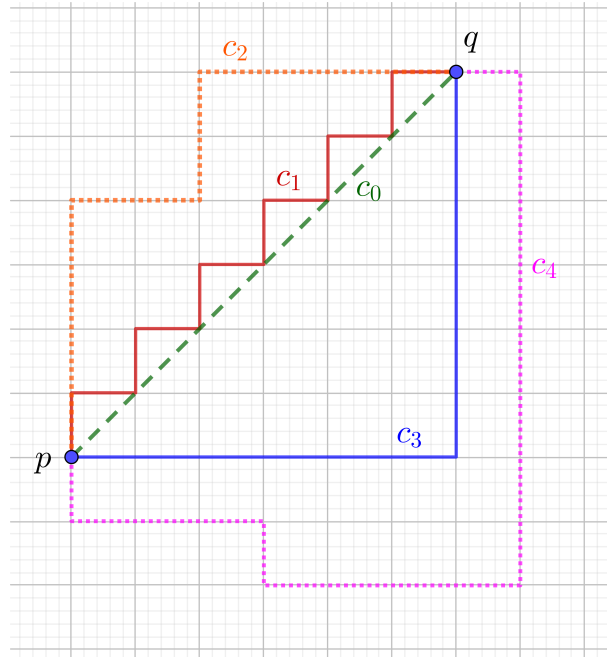
Ejemplo 1.5.16. La relación de congruencia módulo m en \mathbb{Z} (definida en el Ejemplo 1.5.7) es una relación de equivalencia. ■

Notación 1.5.17. Es usual denotar por \preceq o \leq a una relación de orden genérica en un conjunto A y por \sim , \equiv o \simeq a una relación de equivalencia genérica. Aquí utilizaremos frecuentemente las dos primeras notaciones, es decir, \preceq para los órdenes y \sim para las relaciones de equivalencia.

1.6. Clases de equivalencia y conjunto cociente

La relación de equivalencia por excelencia en un conjunto A es la relación de igualdad. En muchos problemas sin embargo resulta conveniente considerar elementos que en algún sentido sean equivalentes, sin que necesariamente sean iguales. Las relaciones de equivalencia por lo tanto generalizan el concepto de igualdad y permiten “clasificar” objetos que tengan las mismas propiedades (aquellas, justamente, que definen la relación) en un mismo conjunto.

Consideremos por ejemplo dos puntos p y q en el plano que representan dos ubicaciones en una ciudad y sea A el conjunto de todos los caminos entre p y q . Supongamos que interesa estudiar qué camino elegir para ir de p a q de modo que la distancia recorrida sea la menor posible. Podemos considerar la relación en A dada por $c_1 \sim c_2$ si c_1 y c_2 son caminos de igual longitud. Es inmediato verificar que \sim define una relación de equivalencia (dejamos como ejercicio verificar los detalles).



En la figura, la distancia entre p y q se realiza por el segmento de recta c_0 . Pero c_0 no es en realidad un camino válido (o sea $c_0 \notin A$) pues en el medio habrá seguramente obstáculos (como edificios) que debemos sortear. Los caminos c_1 , c_2 y c_3 tienen la misma longitud 12, y por lo tanto son equivalentes. Quiere decir que para ir de p a q por cualquiera de ellos recorreremos la misma distancia. El camino c_4 tiene longitud 18, y por lo tanto no es equivalente a los demás.

Si agrupamos todos los caminos equivalentes entre sí en un mismo conjunto, tendremos definido lo que llamaremos una *clase de equivalencia*. Cada uno de los caminos que pertenecen a la clase será un *representante* de la clase. Más aún, la propiedad que comparten los elementos de la clase permite “etiquetarlos”:

12 representará la clase de todos los caminos de longitud 12 (o sea equivalentes a c_1 , c_2 o c_3), 18 la de los caminos de longitud 18 (equivalentes a c_4), etc. Tendremos garantizado así que cualquier elemento que elijamos en la clase con la etiqueta 12 será un camino de longitud 12, y lo mismo con cualquier otra clase.

Estas clases tienen además dos propiedades fundamentales que generalizaremos a cualquier relación de equivalencia: la unión de todas ellas es todo el conjunto A , es decir, cualquier camino entre p y q está en alguna clase; la intersección de dos cualesquiera de ellas (distintas) es vacío, es decir, no puede haber un camino que tenga simultáneamente dos longitudes diferentes.

Formalizaremos estas consideraciones en la siguiente

Definición 1.6.1. Sea \sim una relación de equivalencia en un conjunto A . Para cada $x \in A$ se define la **clase de equivalencia** de x como el conjunto

$$[x] = \{y \in A : x \sim y\} = \{y \in A : y \sim x\}.$$

En muchos casos usaremos también la notación \bar{x} para denotar la clase de equivalencia de x .

Las clases de equivalencia tienen las siguientes propiedades:

Teorema 1.6.2. Sea \sim una relación de equivalencia en un conjunto no vacío A . Entonces:

1. $[x] \neq \emptyset$ para cada $x \in A$. Más aún, $x \in [x]$ para cada $x \in A$.
2. $x \sim y$ si y sólo si $[x] = [y]$.
3. $x \not\sim y$ si y sólo si $[x] \cap [y] = \emptyset$.
4. la unión de todas las clases de equivalencia es el conjunto A .

Demostración. El punto 1 es trivial, pues al ser \sim una relación reflexiva, $x \in [x]$ para cada $x \in A$.

Para probar el punto 2 supongamos primero que $x \sim y$. Como la relación es simétrica, $y \sim x$. Luego si $z \in [x]$, entonces $x \sim z$, y como la relación es transitiva resultará $y \sim z$, o sea, $z \in [y]$. Hemos probado que $[x] \subset [y]$. La prueba de la contención $[y] \subset [x]$ es análoga y se deja como ejercicio.

Supongamos ahora que $x, y \in A$ son tales que $[x] = [y]$. Entonces, como la relación es reflexiva, en particular $y \sim y$, es decir, $y \in [y] = [x]$, y por lo tanto $x \sim y$.

Observemos que por el punto 2 resulta $x \not\sim y$ si y sólo si $[x] \neq [y]$. En particular, si $[x] \cap [y] = \emptyset$, deberá ser $x \not\sim y$. Para probar el punto 3 sólo nos queda probar que si $x \not\sim y$ entonces $[x] \cap [y] = \emptyset$. Probaremos la contrarecíproca. Supongamos que $[x] \cap [y] \neq \emptyset$. Entonces existe $z \in A$ tal que $z \in [x]$ y $z \in [y]$. Por el punto 2 resultará $[z] = [x]$ y $[z] = [y]$, con lo cual $[x] = [y]$ y por lo tanto $x \sim y$.

Probemos finalmente el punto 4. Claramente cada clase de equivalencia es, por definición, un subconjunto de A y por lo tanto la unión de todas ellas también es un subconjunto de A . Para probar la otra contención, basta observar que para cualquier $x \in A$, $x \sim x$ y por lo tanto $x \in [x]$. Luego x está en la unión de todas las clases de equivalencia. \square

Este resultado muestra que una relación de equivalencia *parte* al conjunto A en subconjuntos disjuntos 2 a 2 (las clases de equivalencia) cuya unión es todo A . Esto motiva la siguiente definición:

Definición 1.6.3. Sea $A \neq \emptyset$ un conjunto. Una **partición** de A es una colección $\mathcal{P} = \{B_i\}_{i \in I}$ de subconjuntos no vacíos de A tales que:

1. $\bigcup_{i \in I} B_i = A$;
2. si $i \neq j$, $B_i \cap B_j = \emptyset$.

Es decir, una partición de A es una colección de subconjuntos disjuntos 2 a 2 cuya unión es todo A .

Del Teorema 1.6.2 resulta que toda relación de equivalencia en A determina una partición de A (el conjunto de las clases de equivalencia definidas por la relación). Veremos que vale la recíproca:

Teorema 1.6.4. Sea $\mathcal{P} = \{B_i\}_{i \in I}$ una partición de un conjunto $A \neq \emptyset$. Entonces la relación \sim en A dada por $x \sim y$ si $x, y \in B_i$ para algún $i \in I$ es una relación de equivalencia en A . Más aún, si $x \in B_i$ entonces $[x] = B_i$.

Demostración. Observemos que como $\bigcup_{i \in I} B_i = A$, entonces para cada $x \in A$ existe $i \in I$ tal que $x \in B_i$, y por lo tanto $x \sim x$, o sea, \sim es reflexiva.

Si ahora tomamos $x \sim y$, tendremos que existe $i \in I$ tal que $x, y \in B_i$, con lo cual $y, x \in B_i$ y por lo tanto $y \sim x$. Luego \sim es simétrica.

Veamos finalmente que \sim es transitiva. Sean $x, y, z \in A$ tales que $x \sim y$ e $y \sim z$. Existirán $i, j \in I$ tales que $x, y \in B_i$ y $y, z \in B_j$. Si fuese $i \neq j$, tendríamos que $B_i \cap B_j = \emptyset$, pero esto no puede ocurrir pues $y \in B_i \cap B_j$. Luego $i = j$ y por lo tanto $x, z \in B_i$. Concluimos que $x \sim z$.

La última afirmación es inmediata, dado que si $x \in B_i$, B_i es el conjunto de los elementos de A relacionados con x , por definición de \sim . \square

Tenemos entonces que toda relación de equivalencia en A define una partición en A y, recíprocamente, que toda partición en A define una relación de equivalencia en A . Veremos que esta correspondencia es *biunívoca*:

Definición 1.6.5. Dados dos conjuntos no vacíos A y B , una **correspondencia biunívoca** entre A y B es una función biyectiva de A en B .

Teorema 1.6.6. Existe una correspondencia biunívoca entre el conjunto de relaciones de equivalencia en un conjunto $A \neq \emptyset$ y el conjunto de particiones de A .

Demostración. Sea \mathcal{E} el conjunto de todas las relaciones de equivalencia en A y \mathcal{P}_A el conjunto de todas las particiones de A . Sea

$$f : \mathcal{E} \rightarrow \mathcal{P}_A$$

tal que $f(\sim) = \mathcal{P}_\sim$ donde $\mathcal{P}_\sim = \{[x] : x \in A\}$ es el conjunto de clases de equivalencia definidas por \sim , que como vimos es una partición de A .

Por el Teorema 1.6.4, para cada partición $\mathcal{P} \in \mathcal{P}_A$, existe una relación de equivalencia \sim en A tal que las clases de equivalencia definidas por \sim coinciden con los subconjuntos que forman la partición. Por lo tanto, para cada $P \in \mathcal{P}_A$ existe $\sim \in \mathcal{E}$ tal que $f(\sim) = P$. Luego f es sobreyectiva.

Si \sim y \sim^* son dos relaciones de equivalencia en A tales que $f(\sim) = f(\sim^*)$ entonces las clases de equivalencia de \sim coinciden con las clases de equivalencia de \sim^* (pues ambas inducen la misma partición de A). Si $x \in A$, denotemos por $[x]$ y $[x]^*$ las clases de equivalencia de x para las relaciones \sim y \sim^* respectivamente. Por lo tanto tenemos que si $f(\sim) = f(\sim^*)$, entonces $[x] = [x]^*$ para cada $x \in A$. Luego, por el ítem 2 del Teorema 1.6.2, si $x, y \in A$ tendremos que

$$x \sim y \Leftrightarrow [x] = [y] \Leftrightarrow [x]^* = [y]^* \Leftrightarrow x \sim^* y$$

con lo cual $\sim = \sim^*$ y por lo tanto f es inyectiva.

Concluimos que f es una función biyectiva. □

Corolario 1.6.7. Sean \sim y \sim^* dos relaciones de equivalencia en un conjunto $A \neq \emptyset$. Para cada $x \in A$, sean $[x]$ y $[x]^*$ las clases de equivalencia de x para \sim y \sim^* respectivamente. Entonces \sim es igual a \sim^* si y sólo si para cada $x \in A$, $[x] = [x]^*$.

Definición 1.6.8. Sea A un conjunto no vacío y \sim una relación de equivalencia en A . Se denomina **conjunto cociente** de A por \sim y se denota A/\sim a la partición

$$A/\sim = \{[x] : x \in A\}$$

que \sim induce en A .

Ejemplo 1.6.9. Consideremos la relación \mathcal{R} en un conjunto finito $A = \{a_1, a_2, a_3, a_4, a_5\}$ dada por la matriz

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Aplicaremos los resultados del Lema 1.5.11 para probar que \mathcal{R} es una relación de equivalencia en A .

Observemos primero que todos los elementos de la diagonal de $M(\mathcal{R})$ son 1 con lo cual $\text{Id}_n \leq M(\mathcal{R})$ y por lo tanto \mathcal{R} es una relación reflexiva.

Por otra parte, $M(\mathcal{R})$ es una matriz simétrica, es decir, $M(\mathcal{R})^\perp = M(\mathcal{R})$, y por lo tanto \mathcal{R} es simétrica.

Finalmente, es fácil ver que $M(\mathcal{R}) * M(\mathcal{R}) = M(\mathcal{R})$ y por lo tanto \mathcal{R} es transitiva.

Para obtener las clases de equivalencia, debemos recordar que cada elemento de A pertenece a una única clase. Por lo tanto, como

$$[a_1] = \{a_1, a_4\}$$

automáticamente $[a_4] = [a_1]$. Tenemos además

$$[a_2] = \{a_2, a_5\}, \quad [a_3] = \{a_3\}$$

y como todos los elementos de A ya aparecen en alguna de las clases de equivalencia anteriores, estas son todas. Por lo tanto, el conjunto cociente A/\mathcal{R} está dado por

$$A/\mathcal{R} = \{[a_1], [a_2], [a_3]\} = \{\{a_1, a_4\}, \{a_2, a_5\}, \{a_3\}\}.$$

Observemos que también podríamos haber escrito $A/\mathcal{R} = \{[a_4], [a_5], [a_3]\}$, o $A/\mathcal{R} = \{[a_1], [a_5], [a_3]\}$, etc. ■

Ejemplo 1.6.10. Los enteros módulo m . Consideremos la relación de congruencia módulo m en \mathbb{Z} definida en el Ejemplo 1.5.7. De ahora en más denotaremos $x \equiv y (m)$ para indicar esta relación. Es decir,

$$x \equiv y (m) \Leftrightarrow \exists k \in \mathbb{Z} : x - y = km.$$

Ya vimos que \equiv es una relación de equivalencia en \mathbb{Z} . Veamos cuál es el conjunto cociente que define.

Sea $x \in \mathbb{Z}$ cualquiera. Por el algoritmo de la división (ver Teorema 2.3.2) existen únicos $c \in \mathbb{Z}$ y $r \in \mathbb{Z}$ tal que $0 \leq r < m$ y

$$x = cm + r.$$

c es el *cociente* y r es el *resto* de dividir x por m . Para simplificar la notación escribiremos $r = r_m(x)$ para indicar el resto de dividir x por m . Observemos que

$$(1.1) \quad x - r = cm, \quad c \in \mathbb{Z} \implies x \equiv r (m) \implies [x] = [r].$$

Quiere decir que todo entero x está relacionado con $r_m(x)$, y como el resto de la división por m puede variar entre 0 y $m - 1$, hay a lo sumo m clases de equivalencia distintas para esta relación.

Más aún, si $0 \leq r, r' < m$, entonces $-m < r - r' < m$, con lo cual $r - r'$ es múltiplo de m si y sólo si $r - r' = 0$, es decir, si y sólo si $r = r'$.

Concluimos que los números $0, 1, \dots, m - 1$ no están relacionados entre sí, y por lo tanto definen clases de equivalencia distintas.

El conjunto cociente \mathbb{Z}/\equiv se denota como \mathbb{Z}_m y la clase de equivalencia $[k]$ de $k \in \mathbb{Z}$ suele denotarse en este caso por \bar{k} . Por lo tanto tenemos que

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

es un conjunto finito de m elementos. Observemos que $\bar{0}$ es el conjunto de los múltiplos de m .

Por otra parte, en función de 1.1 y del Teorema 1.6.2 tendremos que

$$x \equiv y (m) \Leftrightarrow [x] = [y] \Leftrightarrow [r_m(x)] = [r_m(y)] \Leftrightarrow r_m(x) = r_m(y)$$

lo que nos da una forma equivalente de definir la congruencia módulo m en términos del resto de la división por m .

Para el caso particular de $m = 2$, tendremos que $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, donde $\bar{0}$ es el conjunto de los números pares (los múltiplos de 2) y $\bar{1}$ es el conjunto de números impares. ■

Ejemplo 1.6.11. Sea \mathcal{V} el conjunto de todos los espacios vectoriales reales de dimensión finita y definamos en \mathcal{V} la relación $V_1 \sim V_2$ si existe un isomorfismo lineal $T : V_1 \rightarrow V_2$. Dejamos como ejercicio probar que se trata efectivamente de una relación de equivalencia. Dado un espacio vectorial V cualquiera, la clase de equivalencia $[V]$ estará compuesta por todos los espacios vectoriales isomorfos a V . Como sabemos del álgebra lineal, dos espacios vectoriales de dimensión finita son isomorfos si y sólo si tienen la misma dimensión. Por lo tanto podemos “etiquetar” cada clase de equivalencia con un número natural n , de modo que n represente la clase de equivalencia formada por todos los espacios vectoriales de dimensión n . De esta manera podemos identificar el conjunto cociente \mathcal{V}/\sim con \mathbb{N} , y un representante “canónico” de la clase de equivalencia etiquetada por $n \in \mathbb{N}$ es \mathbb{R}^n . ■

Como veremos en múltiples oportunidades este ejemplo es típico en matemática. Cada vez que estudiamos una estructura (algebraica, diferenciable, etc), es importante definir qué se entiende por una estructura equivalente (en este caso se usa más comunmente la palabra *isomorfa*), lo que definirá siempre una relación de equivalencia y permitirá clasificar las estructuras en clases de equivalencia.

Todos los elementos de la clase compartirán así las mismas propiedades relativas a la estructura que estamos estudiando, y por lo tanto para determinar las propiedades de cualquier elemento de la clase bastará estudiar un representante adecuado. Por ejemplo, en álgebra lineal, como hemos notado, \mathbb{R}^n es un representante de la clase de equivalencia de los espacios vectoriales reales de dimensión n . Por lo tanto basta estudiar las propiedades de \mathbb{R}^n (como espacio vectorial) para deducir propiedades sobre cualquier otro espacio vectorial de dimensión n .

1.7. Ejercicios

1. Para cada una de las siguientes relaciones \mathcal{R}_i , $i = 1, \dots, 6$, determinar su dominio, su imagen y la relación inversa \mathcal{R}_i^{-1} . Decidir si se trata de una relación funcional, y en ese caso si es inyectiva y/o sobreyectiva.

a) $\mathcal{R}_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = x^2 + 7\}$.

b) $\mathcal{R}_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^4 = x\}$.

c) $\mathcal{R}_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 3x + 1\}$.

d) $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3, b_4\}$ y \mathcal{R}_4 es la relación de A en B tal que

$$M(\mathcal{R}_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

e) $B = \{b_1, b_2, b_3, b_4\}$, $C = \{u, v, x, y, z\}$ y \mathcal{R}_5 es la relación de B en C tal que

$$M(\mathcal{R}_5) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

2. Probar el Lema 1.3.4.

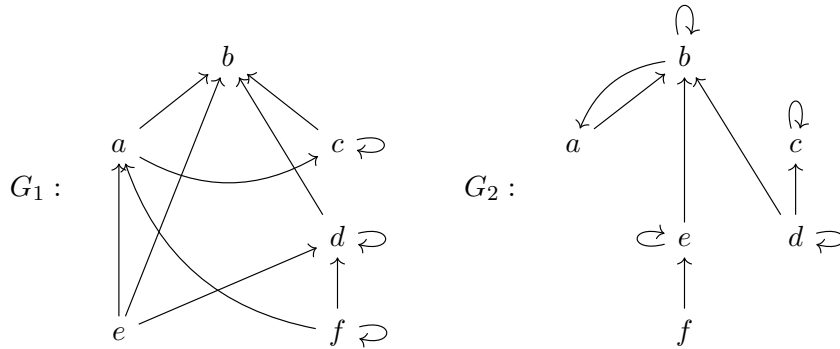
3. Probar el Lema 1.4.16.

4. Considerar las relaciones \mathcal{R}_1 y \mathcal{R}_2 en $A = \{1, 2, 3, 4, 5\}$ cuyas matrices asociadas son

$$M(\mathcal{R}_1) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad M(\mathcal{R}_2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

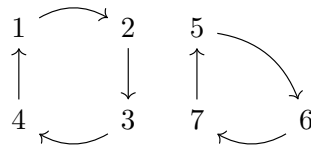
Determinar los grafos dirigidos asociados a \mathcal{R}_1 , \mathcal{R}_2 y las matrices y los grafos dirigidos asociados a las relaciones $\mathcal{R}_3 = \mathcal{R}_1 \cup \mathcal{R}_2$, $\mathcal{R}_4 = \mathcal{R}_1 \cap \mathcal{R}_2$ y $\mathcal{R}_5 = \mathcal{R}_2 \circ \mathcal{R}_1$.

5. Considerar las relaciones \mathcal{R}_1 y \mathcal{R}_2 cuyos grafos dirigidos asociados son los grafos G_1 y G_2 de la siguiente figura:



Determinar las matrices asociadas a \mathcal{R}_1 y \mathcal{R}_2 y las matrices y los grafos dirigidos asociados a las relaciones $\mathcal{R}_3 = \mathcal{R}_1 \circ \mathcal{R}_2$ y $\mathcal{R}_4 = \mathcal{R}_2 \circ \mathcal{R}_1$.

6. Sea \mathcal{R} la relación sobre $A = \{1, 2, 3, 4, 5, 6, 7\}$ cuyo grafo dirigido asociado es



- Si $\mathcal{R}^1 = \mathcal{R}$, $\mathcal{R}^2 = \mathcal{R} \circ \mathcal{R}$ y $\mathcal{R}^n = \mathcal{R}^{n-1} \circ \mathcal{R}$ para cada $n \in \mathbb{N}$, $n \geq 3$, encontrar el número natural $n \geq 2$ más pequeño tal que $\mathcal{R}^n = \mathcal{R}$.
- ¿Cuál es el $n \in \mathbb{N}$ más pequeño para el cual el grafo de \mathcal{R}^n contiene al menos un lazo?
- ¿Existe $n \in \mathbb{N}$ tal que el grafo de \mathcal{R}^n consta sólo de lazos?

7. Sean \mathcal{R} y \mathcal{S} relaciones de A en B . Probar que

- $\mathcal{C}(\mathcal{R}^{-1}) = (\mathcal{C}\mathcal{R})^{-1}$.
- $(\mathcal{R} \cup \mathcal{S})^{-1} = \mathcal{R}^{-1} \cup \mathcal{S}^{-1}$.
- $(\mathcal{R} \cap \mathcal{S})^{-1} = \mathcal{R}^{-1} \cap \mathcal{S}^{-1}$.
- $(\mathcal{R} - \mathcal{S})^{-1} = \mathcal{R}^{-1} - \mathcal{S}^{-1}$.

8. Sea \mathcal{R} una relación de A en B . Probar que \mathcal{R} es una relación funcional biyectiva si y sólo si \mathcal{R}^{-1} es una relación funcional biyectiva.

9. Sea \mathcal{R} una relación en un conjunto A y sean B, C subconjuntos tales que $C \subseteq B \subseteq A$. Probar que $(\mathcal{R}|_B)|_C = \mathcal{R}|_C$.
10. Probar el Lema 1.4.23
11. Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ funciones y sea $A' \subseteq A$.
- Probar que:
 - Si f es inyectiva, entonces $f|_{A'}$ es inyectiva.
 - Si $f|_{A'}$ es sobreyectiva, entonces f es sobreyectiva.
 - Si $g \circ f$ es inyectiva entonces f es inyectiva.
 - Si $g \circ f$ es sobreyectiva entonces g es sobreyectiva.
 - Mostrar que todas las recíprocas de las proposiciones anteriores son falsas.
12. Probar el Lema 1.5.11.
13. En cada uno de los siguientes casos, determinar si la relación \mathcal{R} en \mathbb{Z} es reflexiva, simétrica, antisimétrica, o transitiva.
- $x\mathcal{R}y \Leftrightarrow x = y^2$.
 - $x\mathcal{R}y \Leftrightarrow x + y$ es par.
 - $x\mathcal{R}y \Leftrightarrow x - y$ es impar.
14. Sea \mathcal{R} y \mathcal{S} relaciones en A . Determinar la validez de los siguientes enunciados:
- Si \mathcal{R} y \mathcal{S} son reflexivas, entonces:
 - $\mathcal{R} \cup \mathcal{S}$ es reflexiva.
 - $\mathcal{R} \cap \mathcal{S}$ es reflexiva.
 - $\mathcal{R} \circ \mathcal{S}$ es reflexiva.
 - Repetir el ejercicio anterior sustituyendo “reflexiva” por simétrica, antisimétrica, o transitiva.
15. Sea \mathcal{R} una relación en un conjunto A . Probar que:
- Si \mathcal{R} es reflexiva (resp. simétrica, antisimétrica, transitiva), entonces \mathcal{R}^{-1} también lo es.
 - Sea $A' \subset A$. Si \mathcal{R} es reflexiva (resp. simétrica, antisimétrica, o transitiva), entonces $\mathcal{R}|_{A' \times A'}$ también lo es.
16. Sea X un conjunto no vacío y sea \mathcal{R} la relación en $\mathcal{P}(X)$ dada por $A\mathcal{R}B$ si $A \subseteq B$. Probar que \mathcal{R} es una relación de orden.
17. Sean \mathcal{R} y \mathcal{S} relaciones en un conjunto A . Pongamos $\mathcal{R}^1 = \mathcal{R}$ y $\mathcal{R}^{n+1} = \mathcal{R}^n \circ \mathcal{R}$ para cada $n \in \mathbb{N}$, y lo mismo para \mathcal{S} . Probar que:
- Si $\mathcal{R} \subset \mathcal{S}$, entonces $\mathcal{R}^n \subset \mathcal{S}^n$ para cada $n \in \mathbb{N}$.
 - Si $\mathcal{R}^k = \mathcal{R}^j$ para algún $j > k$, entonces $\mathcal{R}^{j+m} = \mathcal{R}^{k+m}$ para cada $m \in \mathbb{N}$.
 - Si \mathcal{R} es transitiva, entonces \mathcal{R}^n es transitiva para cada $n \in \mathbb{N}$.
 - \mathcal{R} es transitiva si y sólo si $\mathcal{R}^n \subset \mathcal{R}$ para cada $n \in \mathbb{N}$.
18. Sea \mathcal{R} una relación en un conjunto A y sea

$$\mathcal{R}^* = \bigcup_{n \in \mathbb{N}} \mathcal{R}^n.$$

- Probar que \mathcal{R}^* es una relación transitiva.

b) Probar que si A es finito y $|A| = n$, entonces

$$\mathcal{R}^* = \bigcup_{k=1}^n \mathcal{R}^k = \mathcal{R} \cup \mathcal{R}^2 \cup \dots \cup \mathcal{R}^n.$$

19. Sea \mathcal{R} una relación en un conjunto A . Se denomina *clausura reflexiva* de \mathcal{R} , y se la denota $\text{CR}(\mathcal{R})$, a la relación reflexiva más pequeña en A que contiene a \mathcal{R} , es decir, a una relación $\text{CR}(\mathcal{R})$ en A que verifica:

- i) $\mathcal{R} \subset \text{CR}(\mathcal{R})$;
- ii) $\text{CR}(\mathcal{R})$ es reflexiva;
- iii) Si \mathcal{R}' es una relación reflexiva tal que $\mathcal{R} \subset \mathcal{R}'$, entonces $\text{CR}(\mathcal{R}) \subset \mathcal{R}'$.

Probar que para cualquier relación \mathcal{R} en A la clausura reflexiva de \mathcal{R} siempre existe y es única. Probar además que:

- a) $\text{CR}(\mathcal{R}) = \mathcal{R} \cup \Delta$, donde $\Delta = \{(a, a) : a \in A\}$.
- b) \mathcal{R} es reflexiva si y sólo si $\text{CR}(\mathcal{R}) = \mathcal{R}$.

20. Sea \mathcal{R} una relación en un conjunto A . Se denomina *clausura simétrica* de \mathcal{R} , y se la denota $\text{CS}(\mathcal{R})$, a la relación simétrica más pequeña en A que contiene a \mathcal{R} , es decir, a una relación $\text{CS}(\mathcal{R})$ en A que verifica:

- i) $\mathcal{R} \subset \text{CS}(\mathcal{R})$;
- ii) $\text{CS}(\mathcal{R})$ es simétrica;
- iii) Si \mathcal{R}' es una relación simétrica tal que $\mathcal{R} \subset \mathcal{R}'$, entonces $\text{CS}(\mathcal{R}) \subset \mathcal{R}'$.

Probar que para cualquier relación \mathcal{R} en A la clausura simétrica de \mathcal{R} siempre existe y es única. Probar además que:

- a) $\text{CS}(\mathcal{R}) = \mathcal{R} \cup \mathcal{R}^{-1}$.
- b) \mathcal{R} es simétrica si y sólo si $\text{CS}(\mathcal{R}) = \mathcal{R}$.

21. Sea \mathcal{R} una relación en A y sea $\mathcal{S} = \text{CS}(\text{CR}(\mathcal{R}))$. Probar que \mathcal{S} es reflexiva y simétrica.

22. Sea \mathcal{R} la relación en $A = \{a_1, a_2, a_3\}$ cuya matriz es $M(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Hallar $\text{CR}(\mathcal{R})$ y $\text{CS}(\mathcal{R})$.

23. Sea \mathcal{R} la relación en \mathbb{R} dada por $x\mathcal{R}y$ si y sólo si $x + y = 1$ o $x - y = 1$. Hallar $\text{CS}(\mathcal{R})$.

24. Sea \mathcal{R} una relación en un conjunto A . Se denomina *clausura transitiva* de \mathcal{R} , y se la denota $\text{CT}(\mathcal{R})$, a la relación transitiva más pequeña en A que contiene a \mathcal{R} , es decir, a una relación $\text{CT}(\mathcal{R})$ en A que verifica:

- i) $\mathcal{R} \subset \text{CT}(\mathcal{R})$;
- ii) $\text{CT}(\mathcal{R})$ es transitiva;
- iii) Si \mathcal{R}' es una relación transitiva tal que $\mathcal{R} \subset \mathcal{R}'$, entonces $\text{CT}(\mathcal{R}) \subset \mathcal{R}'$.

Probar que para cualquier relación \mathcal{R} en A la clausura transitiva de \mathcal{R} siempre existe y es única. Probar además que:

- a) $\text{CT}(\mathcal{R}) = \mathcal{R}^*$, donde \mathcal{R}^* es la relación definida en el Ejercicio 18.

b) \mathcal{R} es transitiva si y sólo si $\text{CT}(\mathcal{R}) = \mathcal{R}$.

25. Hallar $\text{CT}(\mathcal{R})$ para la relación \mathcal{R} en $A = \{a_1, a_2, a_3, a_4\}$ cuya matriz es $M(\mathcal{R}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

26. Sea \mathcal{R} una relación cualquiera en un conjunto A . Probar que $\mathcal{S} = \text{CT}(\text{CR}(\mathcal{R}))$ es un preorden.

27. Analizar en cada caso si la relación dada en el conjunto A es de equivalencia. En caso de serlo, describir su conjunto cociente:

a) $A = \mathbb{Z}$, $x \sim y \Leftrightarrow x - y$ es un entero par.

b) $A = \mathbb{R}$, $x \sim y \Leftrightarrow xy > 0$.

c) $A = \mathbb{R}$, $x \sim y \Leftrightarrow xy \geq 0$.

d) $A = \mathbb{R} \times \mathbb{R}$, $(a, b) \sim (c, d) \Leftrightarrow a + d = c + b$.

28. Dada una función $f : A \rightarrow B$, se define una relación \mathcal{K}_f en A como

$$\mathcal{K}_f = \{(a, a') \in A \times A : f(a) = f(a')\}$$

a) Probar que \mathcal{K}_f es de equivalencia.

b) Dar una definición alternativa para \mathcal{K}_f en términos de f , la composición y la inversa de relaciones.

c) Mostrar que toda relación de equivalencia en un conjunto A cualquiera es \mathcal{K}_f para alguna función $f : A \rightarrow B$, para algún conjunto B adecuado.

29. Sea $\text{espar} : \mathbb{N} \rightarrow \mathbb{B}$ la función que retorna valor **true** en los pares y valor **false** en los impares. Calcular $\mathbb{N}/\mathcal{K}_{\text{espar}}$.

30. Probar el **Teorema de factorización**: Dada una función $f : A \rightarrow B$ y una relación de equivalencia $\sim \subseteq \mathcal{K}_f$, probar que existe una única función $\tilde{f} : A/\sim \rightarrow B$ tal que $f = \tilde{f} \circ \pi$, donde $\pi : A \rightarrow A/\sim$ se define como $\pi(a) = \bar{a}$ para todo $a \in A$.

Conjuntos ordenados

2.1. Conjuntos parcialmente ordenados (Posets)

Recordemos que una relación \mathcal{R} en un conjunto A es una relación de **orden (parcial)** en A si \mathcal{R} es reflexiva, antisimétrica y transitiva. En general, denotaremos por \preceq a un orden parcial. Es decir, si \mathcal{R} es un orden parcial en A , escribimos

$$x \preceq y$$

para indicar que $x \mathcal{R} y$.

Si \preceq es un orden (parcial) en A , decimos que (A, \preceq) (o simplemente A si se sobreentiende cuál es la relación) es un **conjunto (parcialmente) ordenado**, o un **Poset** (del inglés *partially ordered set*).

Muchas veces decimos que x **precede** a y o es **anterior** a y o directamente que es **menor** a y si $x \preceq y$ y $x \neq y$. En este caso decimos también que y **sigue** a x o **posterior** a x . Trataremos de evitar en lo posible la terminología de “*menor a*” que reservaremos para el orden usual en los conjuntos numéricos. Sin embargo es usual encontrarla en la bibliografía, junto con la notación \leq para lo que aquí hemos denotado \preceq .

Notación 2.1.1. Sea \preceq una relación de orden en un conjunto A . Escribiremos $x \prec y$ para indicar que $x \preceq y$ y $x \neq y$.

Definición 2.1.2. Sea \preceq una relación de orden en un conjunto A . Dados $x, y \in A$, decimos que x e y son elementos **comparables** si se verifica $x \preceq y$ o $y \preceq x$ (observemos que como \preceq es antisimétrica, estas dos condiciones se verifican simultáneamente sólo cuando $x = y$).

La relación \preceq se denomina un **orden total** si todo par de elementos de A son comparables. En ese caso, A se dice un conjunto **totalmente ordenado**.

Esta última definición justifica por qué llamamos *orden parcial* a una relación de orden.

A partir del Ejercicio 15 del Capítulo 1 obtenemos que:

Lema 2.1.3. Sea \preceq una relación de orden en un conjunto A y sea $B \subseteq A$, entonces:

1. $\preceq|_B$ es un orden en B . Si \preceq es un orden total, entonces $\preceq|_B$ también lo es.
2. La relación inversa a \preceq , \preceq^{-1} , es una relación de orden en A , denominada el **orden inverso** a \preceq y denotada por \succeq . Si \preceq es un orden total, entonces \succeq también es un orden total.

A partir de la definición de la relación inversa, tendremos que

$$x \preceq y \iff y \succeq x.$$

Ejemplo 2.1.4. El orden usual \leq (“menor o igual”) en los conjuntos numéricos (\mathbb{N} , \mathbb{Z} , \mathbb{Q} o \mathbb{R}) es un orden total. Su orden inverso es la relación \geq (“mayor o igual”) que también es un orden total. ■

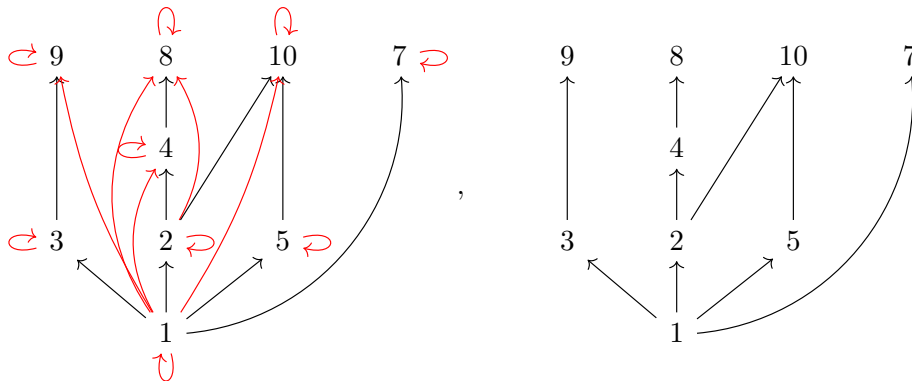
Ejemplo 2.1.5. Divisibilidad. Vimos que la relación $n \mathcal{R} m$ si $n \mid m$ es un preorden en $\mathbb{Z} - \{0\}$, pero $\mathcal{R}|_{\mathbb{N}}$ es una relación de orden en \mathbb{N} que denotamos directamente por $\mathcal{R} = \mid$. Se trata de un orden parcial, pues por ejemplo dos números primos cualesquiera no son comparables entre si (por ejemplo $2 \nmid 3$ y $3 \nmid 2$). Su orden inverso es $n \mathcal{R}^{-1} m$ si n es múltiplo de m . ■

La forma privilegiada de representar conjuntos parcialmente ordenados es a través de su grafo. Sin embargo, una vez que sabemos que se trata de una relación de orden, se eliminan las aristas que brindan información superflua y se ordenan los elementos de manera ascendente para obtener un grafo simplificado:

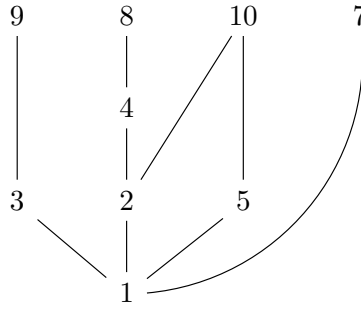
Definición 2.1.6. Sea (A, \preceq) un conjunto parcialmente ordenado finito. Se denomina **diagrama de Hasse** de (A, \preceq) a un grafo que se obtiene a partir del grafo G de la relación \preceq de la siguiente manera:

- Se eliminan todos los lazos, sobreentendiendo que la relación es reflexiva.
- Si $a \preceq b$ y $b \preceq c$, se elimina la arista (a, c) , sobreentendiendo que la relación es transitiva.
- Se ubican los elementos de manera ascendente, es decir, si $a \preceq b$, a debe ubicarse en el grafo debajo de b , y se eliminan las flechas de las aristas.

Ejemplo 2.1.7. Consideremos la relación “divide a” en \mathbb{N} del Ejemplo 2.1.5 restringida al subconjunto finito $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ de \mathbb{N} . En la siguiente figura mostramos el grafo dirigido de A , con las aristas que debemos eliminar en rojo, y el grafo que se obtiene después de eliminarlas. Hemos ubicado además los elementos de manera ascendente:



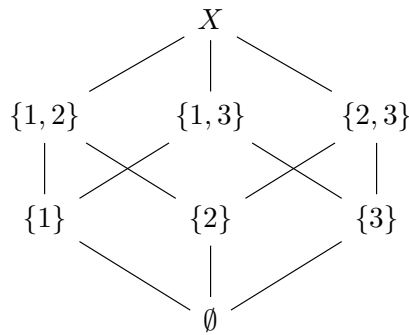
Para obtener el diagrama de Hasse de la relación, solo resta eliminar las flechas de las aristas:



■

Ejemplo 2.1.8. Contención de conjuntos Consideremos un conjunto X cualquiera. La relación de contención $C \preceq D$ si $C \subseteq D$ define una relación de orden en $\mathcal{P}(X)$ (ver Ejercicio 16 del Capítulo 1).

Tomemos por ejemplo el conjunto $X = \{1, 2, 3\}$. El diagrama de Hasse de la relación es en este caso:



Aquí podemos notar fácilmente que \subseteq no es un orden total en $\mathcal{P}(X)$, pues por ejemplo $\{1\}$ y $\{2\}$ no son comparables. ■

Ejemplo 2.1.9. Orden producto. Sean (A, \preceq_A) y (B, \preceq_B) dos conjuntos parcialmente ordenados. Definamos en $A \times B$ la relación \preceq_{prod} dada por

$$(x, y) \preceq_{prod} (x', y') \text{ si } x \preceq_A x' \text{ y } y \preceq_B y'$$

Veamos que \preceq_{prod} es una relación de orden en $A \times B$:

- Es reflexiva: dado $(x, y) \in A \times B$, $x \preceq_A x$ e $y \preceq_B y$. Luego $(x, y) \preceq_{prod} (x, y)$.
- Es antisimétrica: si $(x, y) \preceq_{prod} (x', y')$ y $(x', y') \preceq_{prod} (x, y)$, entonces tendremos:

$$\begin{cases} x \preceq_A x' \text{ y } x' \preceq_A x \\ y \preceq_B y' \text{ y } y' \preceq_B y \end{cases} \implies \begin{cases} x = x' \\ y = y' \end{cases}$$

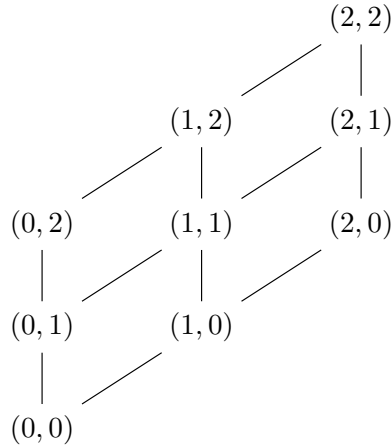
con lo cual $(x, y) = (x', y')$.

- Es transitiva: Si $(x, y) \preceq_{prod} (x', y')$ y $(x', y') \preceq_{prod} (x'', y'')$, entonces $x \preceq_A x'$, $x' \preceq_A x''$, $y \preceq_B y'$ y $y' \preceq_B y''$. De la transitividad de \preceq_A y \preceq_B resulta $x \preceq_A x''$ y $y \preceq_B y''$, con lo cual $(x, y) \preceq_{prod} (x'', y'')$.

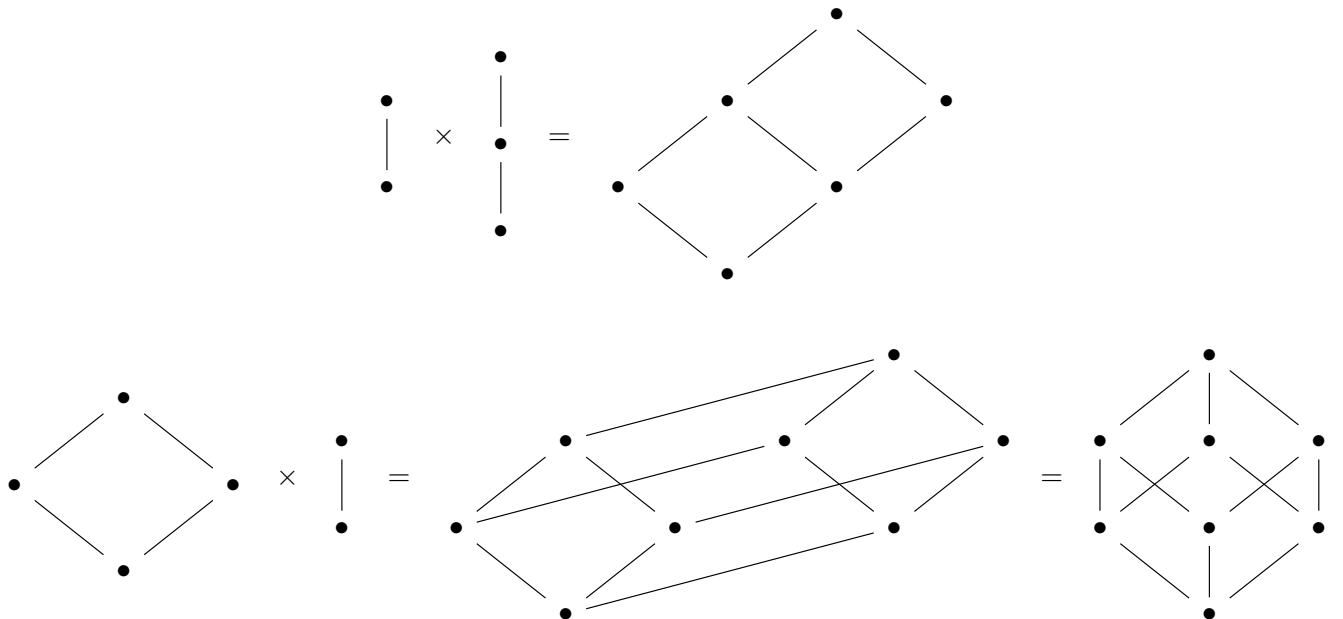
El orden \preceq_{prod} en $A \times B$ se denomina **orden producto**.

En general, \preceq_{prod} no es un orden total, incluso si (A, \preceq_A) y (B, \preceq_B) son totalmente ordenados. Consideremos por ejemplo el orden usual en \mathbb{R} y tomemos el orden producto en $\mathbb{R} \times \mathbb{R}$. (\mathbb{R}, \leq) es totalmente ordenado, pues dos elementos cualesquiera son comparables. Sin embargo $(\mathbb{R} \times \mathbb{R}, \preceq_{prod})$ no es totalmente ordenado para pues por ejemplo $(0, 1)$ y $(1, 0)$ no son comparables.

Consideremos ahora el conjunto $A = \{0, 1, 2\}$ con el orden usual \leq . Entonces es fácil verificar que el diagrama de Hasse para $(A \times A, \preceq_{prod})$ es



Informalmente, podemos dibujar el diagrama de Hasse de un producto $A \times B$ (o reconocer cuándo un determinado diagrama se corresponde con un producto) reemplazando cada punto del diagrama de A por una copia del diagrama de B , y conectando “puntos correspondientes”, colocando siempre los puntos de modo que se respete el modo ascendente de construir un diagrama de Hasse. En las figuras siguientes damos algunos ejemplos:



■

Ejemplo 2.1.10. Orden lexicográfico. Sean (A, \preceq_A) y (B, \preceq_B) conjuntos parcialmente ordenados. Otro orden posible en $A \times B$ es el denominado **orden lexicográfico**. Definimos la relación \preceq_{lex} en $A \times B$ por

$$(a, b) \preceq_{lex} (c, d) \text{ si } (a \prec_A c) \vee (a = c \wedge b \preceq_B d)$$

El nombre de esta forma de ordenar un producto proviene del orden usual del diccionario: comparamos primero los primeros elementos, y sólo si estos son iguales procedemos a comparar los que siguen. Puede generalizarse a cualquier producto finito de conjuntos ordenados. Dejamos como ejercicio probar que \preceq_{lex} es efectivamente una relación de orden, y en este caso se trata de un orden total si A y B son conjuntos totalmente ordenados.

Por ejemplo, para el conjunto $A = \{0, 1, 2\}$ con el orden usual \preceq , tenemos que para el orden lexicográfico en $A \times A$,

$$(0, 0) \preceq_{lex} (0, 1) \preceq_{lex} (0, 2) \preceq_{lex} (1, 0) \preceq_{lex} (1, 1) \preceq_{lex} (1, 2) \preceq_{lex} (2, 0) \preceq_{lex} (2, 1) \preceq_{lex} (2, 2)$$

Por lo tanto $(A \times A, \preceq_{lex})$ es totalmente ordenado y su diagrama de Hasse es una “línea vertical”, es decir son trazos verticales entre cada nodo. ■

2.2. Elementos minimales, maximales, mínimos y máximos

Definición 2.2.1. Sea (A, \preceq) es un conjunto parcialmente ordenado. Sean $x_0, y_0 \in A$. Decimos que:

- x_0 es un elemento **minimal** si para cada $x \in A$ se verifica

$$x \preceq x_0 \implies x = x_0.$$

- y_0 es un elemento **maximal** si para cada $x \in A$ se verifica

$$y_0 \preceq x \implies x = y_0.$$

- x_0 es un **mínimo** si para cada $x \in A$, $x_0 \preceq x$.

- y_0 es un **máximo** si para cada $x \in A$, $x \preceq y_0$.

Si $B \subseteq A$, decimos que $b \in B$ es un elemento minimal (resp. maximal, mínimo o máximo) de B , si b es un elemento minimal (resp. maximal, mínimo o máximo) del conjunto parcialmente ordenado $(B, \preceq|_{B \times B})$.

Observación 2.2.2. Claramente todo elemento máximo es maximal, y todo elemento mínimo es minimal. La recíproca es obviamente falsa, como veremos en los ejemplos siguientes.

Observemos que si x_0 es un elemento mínimo de A , entonces A no admite otros elementos minimales distintos de x_0 . En efecto, si x'_0 es un elemento minimal, al ser x_0 un mínimo resulta $x_0 \preceq x'_0$ y al ser x'_0 minimal debe ser $x_0 = x'_0$. De manera análoga, si y_0 es un máximo de A , y_0 es el único elemento maximal.

A partir de la contrarecíproca de las proposiciones que intervienen en las definiciones de elementos minimales y maximales tenemos la siguiente caracterización:

Lema 2.2.3. Sea (A, \preceq) un conjunto parcialmente ordenado y sea $a \in A$. Entonces:

- x_0 es minimal si y sólo si para cada $x \neq x_0$ comparable con x_0 resulta $x_0 \prec x$.
- y_0 es maximal si y sólo si para cada $x \neq y_0$ comparable con y_0 resulta $x \prec y_0$.

Ejemplo 2.2.4. Consideremos el conjunto parcialmente ordenado $(\mathbb{N}, |)$. En este caso es fácil ver que existe un mínimo, 1, que el único número que divide a todos los naturales. Al ser mínimo, es el único elemento minimal posible.

Observemos que si $a | b$, entonces $a \leq b$ (dado que $b = ka$ para algún número natural k). Luego $|$ no tiene máximo. En efecto, supongamos que b_0 fuese un máximo. Entonces debería ser $a | b_0$ para cada $a \in \mathbb{N}$, y en particular $a \leq b_0$ para cada $a \in \mathbb{N}$, lo que es absurdo.

Restrinjamos ahora la relación al subconjunto finito $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ de \mathbb{N} como en el Ejemplo 2.1.7. A partir del diagrama de Hasse de $(A, |)$ es inmediato verificar que 1 es un elemento mínimo y A no tiene elementos máximos. Además, 7, 8, 9 y 10 son elementos maximales.

Si ahora restringimos la relación “divide a” al subconjunto $B = \{n \in \mathbb{N} : n \geq 2\}$, existen infinitos elementos minimales, todos los números primos, y no hay elementos mínimos ni máximos. ■

Ejemplo 2.2.5. Si consideramos un conjunto X cualquiera y la relación de contención \subseteq en $\mathcal{P}(X)$, existe siempre un elemento mínimo, \emptyset , y un elemento máximo, X . En efecto, para cualquier $A \in \mathcal{P}(X)$ se verifica que $\emptyset \subset A$ y $A \subset X$. ■

Ejemplo 2.2.6. Supongamos que (A, \preceq_A) y (B, \preceq_B) son conjuntos ordenados y a_0 y b_0 son elementos mínimos de A y B respectivamente. Veamos que (a_0, b_0) es un mínimo para $(A \times B, \preceq_{prod})$. En efecto, dado $(x, y) \in A \times B$, tenemos que $a_0 \preceq_A x$ y $b_0 \preceq_B y$, con lo cual $(a_0, b_0) \preceq_{prod} (x, y)$. Un razonamiento análogo puede hacerse para los máximos. ■

Teorema 2.2.7. Sea (A, \preceq) un conjunto parcialmente ordenado. Si $B \neq \emptyset$ es un subconjunto finito de A , entonces $(B, \preceq|_B)$ tiene al menos un elemento minimal y al menos un elemento maximal.

Demostración. Haremos la prueba por inducción sobre el cardinal de B .

Supongamos primero que $|B| = 1$, es decir $B = \{b_1\}$. Entonces es evidente que b_1 es un elemento minimal y maximal de B .

Supongamos ahora que dado $n \in \mathbb{N}$, $n > 1$, todo subconjunto no vacío C de A de cardinal $|C| < n$ tiene al menos un elemento minimal y un elemento maximal y sea $B \subseteq A$ tal que $|B| = n$.

Sea $b_1 \in B$ cualquiera y consideremos los conjuntos

$$B_1 = \{b \in B : b \prec b_1\} \quad \text{y} \quad B'_1 = \{b \in B : b_1 \prec b\}.$$

Observemos que $b_1 \notin B_1$ y $b_1 \notin B'_1$, y por lo tanto B_1 y B'_1 tienen cardinal menor o igual a $n - 1$.

Si $B_1 = \emptyset$, entonces del Lema 2.2.3 tenemos que b_1 es un elemento minimal de B . Si $B_1 \neq \emptyset$, como $|B_1| < n$, B_1 tiene un elemento minimal, digamos b_0 . Veamos que b_0 es un elemento minimal de B .

Si ahora $B'_1 = \emptyset$, entonces b_1 es un elemento maximal de B . Si $B'_1 \neq \emptyset$, con un razonamiento análogo al anterior se prueba que B'_1 tiene un elemento maximal que es un elemento maximal de B . \square

Demostración. Supongamos que (A, \preceq) es un conjunto parcialmente ordenado y x_0, x'_0 son mínimos de A . Entonces como x_0 es mínimo $x_0 \preceq x$ para todo $x \in A$. En particular $x_0 \preceq x'_0$. Aplicando ahora la definición de mínimo a x'_0 obtenemos que $x'_0 \preceq x_0$. Como \preceq es antisimétrica concluimos que $x_0 = x'_0$. La demostración de la unicidad del máximo es análoga y la dejamos como **ejercicio**. \square

$$x_0 = \min A, \quad y_0 = \max A.$$

1. $x_0 = \min A$ si y sólo si x_0 es el único elemento minimal A
2. $y_0 = \max A$ si y sólo si y_0 es el único elemento maximal de A

Supongamos entonces que x_0 es el único elemento minimal de A . Dado $x \in A$ existen tres posibilidades:

- (i) $x_0 \prec x$; (ii) $x \prec x_0$; (iii) x y x_0 no son comparables.

$$B = \{a \in A : a \prec x\}.$$

La prueba del punto 2.2.10 es análoga y la dejamos como **ejercicio**).

Como consecuencia de los resultados anteriores, obtenemos la siguiente propiedad de los conjuntos finitos totalmente ordenados:

Corolario 2.2.11. *Todo conjunto finito totalmente ordenado tiene un mínimo y un máximo.*

Demostración. Sea (A, \preceq) un conjunto finito totalmente ordenado. Por el Teorema 2.2.7 A tiene un elemento minimal x_0 . Supongamos que A tiene otro elemento minimal x'_0 . Como A es totalmente ordenado x_0 y x'_0 son comparables, esto es, $x_0 \preceq x'_0$ o $x'_0 \preceq x_0$. En cualquier caso, como x_0 y x'_0 son minimales $x_0 = x'_0$. Luego x_0 es el único elemento minimal y por el Lema 2.2.10 x_0 es mínimo.

La prueba de la existencia de máximo es análoga y la dejamos como **ejercicio**. \square

Observación 2.2.12. *El Corolario 2.2.11 no necesariamente vale para conjuntos infinitos, Por ejemplo (\mathbb{R}, \leq) es totalmente ordenado y no tiene mínimo ni máximo. Garantizar la existencia de elementos maximales o minimales depende fuertemente de la hipótesis que el conjunto ordenado (A, \preceq) sea finito. El Teorema 2.2.7 puede generalizarse parcialmente a partir del Lema de Zorn que enunciaremos en la sección 2.6*

2.3. Buen orden en \mathbb{N} y sus consecuencias

Haremos una breve pausa en el desarrollo general de la teoría para investigar una propiedad fundamental del orden usual en \mathbb{N} y sus consecuencias en la aritmética de los números enteros. Presentaremos algunos resultados básicos. Más detalles sobre los temas que trataremos en esta sección pueden encontrarse en [4, 10, 13, 20]

Teorema 2.3.1 (Principio del Buen Orden). *Todo subconjunto no vacío de (\mathbb{N}, \leq) tiene un mínimo.*

Demostración. Sea $A \subset \mathbb{N}$, $A \neq \emptyset$. Tomemos $n \in A$ cualquiera y sea $B = \{a \in A : a \leq n\}$. Entonces $(B, \leq|_B)$ es totalmente ordenado y finito, con lo cual por el Corolario 2.2.11, B tiene un mínimo x_0 . Si ahora $m \in A$, existen dos opciones: $n \leq m$ o $m \leq n$. En el primer caso, como $x_0 \leq n$, resulta $x_0 \leq m$. En el segundo, $m \in B$, con lo cual $x_0 \leq m$. Concluimos que x_0 es un mínimo de A . \square

Como primera consecuencia importante del Principio del Buen Orden podemos demostrar el Algoritmo de la División en \mathbb{Z} :

Teorema 2.3.2 (Algoritmo de la División). *Sean a y b números enteros con $a > 0$. Entonces existen únicos números enteros q y r tales que $b = qa + r$ y $0 \leq r < a$.*

Demostración. *Existencia:* Comencemos observando que si $a \mid b$, entonces el resultado es válido tomando $r = 0$. Supongamos entonces que $a \nmid b$.

Sea $S = \{b - ta : t \in \mathbb{Z}, b - ta > 0\}$. Veamos primero que $S \neq \emptyset$. Si $b > 0$, tomando $t = 0$ resulta $b = b - ta > 0$ y por lo tanto $b \in S$. Si fuese $b \leq 0$, tomemos $t = b - 1 \in \mathbb{Z}$. Entonces

$$b - ta = b - (b - 1)a = b(1 - a) + a > 0$$

puesto que $a > 0$ y $(1 - a) \leq 0$. Luego $b - ta = b(1 - a) + a \in S$ y nuevamente $S \neq \emptyset$.

Como $S \subseteq \mathbb{N}$ y $S \neq \emptyset$, por el Teorema 2.3.1 S tiene un elemento mínimo que denotaremos por r . En particular, como $r \in S$, existirá $q \in \mathbb{Z}$ tal que $r = b - qa$ y $r > 0$. Solo nos queda probar que $r < a$. Si

fuese $r = a$, tendríamos que $b = (q + 1)a$ de donde $a \mid b$, en contra de lo que estamos suponiendo. Si fuese $r > a$, entonces $r = a + c$ para algún $c \in \mathbb{N}$ y entonces

$$b - qa = r = a + c \Rightarrow c = b - (q + 1)a > 0$$

con lo cual $b - (q + 1)a \in S$. Pero $b - (q + 1)a < b - qa = r$ contradiciendo que r es el elemento mínimo de S . Concluimos que $0 \leq r < a$ como queríamos ver. Dejamos la prueba de la unicidad como **ejercicio**. \square

Consideremos ahora b_1, \dots, b_n números naturales. Denotemos por

$$\text{Div}(b_1, \dots, b_n) = \{a \in \mathbb{N} : a \mid b_j, \forall j = 1, \dots, n\}$$

el conjunto de divisores comunes de b_1, \dots, b_n y por

$$\text{Mul}(b_1, \dots, b_n) = \{a \in \mathbb{N} : b_j \mid a, \forall j = 1, \dots, n\}$$

el conjunto de múltiplos comunes de b_1, \dots, b_n .

Observemos que si $a \in \text{Div}(b_1, \dots, b_n)$, entonces en particular $a \leq b_j$ para cada $j = 1, \dots, n$, y por lo tanto $a \leq b = \min\{b_1, \dots, b_n\}$ (este mínimo siempre existe pues $(\{b_1, \dots, b_n\}, \leq)$ es finito y totalmente ordenado). Por lo tanto

$$\text{Div}(b_1, \dots, b_n) \subseteq \{1, 2, \dots, b\}$$

y en consecuencia es un conjunto finito. Luego por el Corolario 2.2.11, $\text{Div}(b_1, \dots, b_n)$ tiene un máximo (también tiene un mínimo, que es 1).

Por otra parte, $\text{Mul}(b_1, \dots, b_n)$ es no vacío, dado que $M = b_1 \cdot b_2 \cdots b_n \in \text{Mul}(b_1, \dots, b_n)$. Observemos que para cada $k \in \mathbb{N}$, $kM \in \text{Mul}(b_1, \dots, b_n)$, con lo cual $\text{Mul}(b_1, \dots, b_n)$ es un conjunto infinito y no podemos aplicar el Corolario 2.2.11. Sin embargo, por el Teorema 2.3.1, podemos garantizar que $\text{Mul}(b_1, \dots, b_n)$ tiene un mínimo.

Definición 2.3.3. Sean b_1, b_2, \dots, b_n números naturales. Se denomina **máximo común divisor** de b_1, \dots, b_n y se lo denota $\text{m. c. d.}(b_1, \dots, b_n)$ al número natural

$$\text{m. c. d.}(b_1, \dots, b_n) = \max \text{Div}(b_1, \dots, b_n).$$

Se denomina **mínimo común múltiplo** de b_1, \dots, b_n y se lo denota $\text{m. c. m.}(b_1, \dots, b_n)$ al número natural

$$\text{m. c. m.}(b_1, \dots, b_n) = \min \text{Mul}(b_1, \dots, b_n).$$

Teorema 2.3.4. Dados $b_1, b_2, \dots, b_n \in \mathbb{N}$, se verifica

$$\text{m. c. d.}(a, b) = \min\{b_1 s_1 + b_2 s_2 + \cdots + b_n s_n : s_i \in \mathbb{Z} \forall i = 1, \dots, n, b_1 s_1 + \cdots + b_n s_n > 0\}$$

es decir, el máximo común divisor de b_1, b_2, \dots, b_n es la menor combinación lineal entera positiva de b_1, \dots, b_n .

Demostración. Consideremos el conjunto

$$(2.1) \quad S = \{b_1 s_1 + b_2 s_2 + \cdots + b_n s_n : s_i \in \mathbb{Z} \forall i = 1, \dots, n, \ b_1 s_1 + \cdots + b_n s_n > 0\} \subseteq \mathbb{N}$$

de las combinaciones lineales enteras positivas de b_1, \dots, b_n . Observemos que como $b_i > 0$ para todo i , tomando $s_i = 1$ para cada $i = 1, \dots, n$ resulta

$$b_1 + b_2 + \cdots + b_n \in S$$

y por lo tanto $S \neq \emptyset$. Por el Teorema 2.3.1 existe $d = \min S$. Probaremos que $d = \text{m.c.d.}(b_1, \dots, b_n)$. Veamos primero que $d \in \text{Div}(b_1, \dots, b_n)$.

Como $d \in S$, existirán $x_i \in \mathbb{Z}$, $i = 1, \dots, n$ tales que

$$d = b_1 x_1 + \cdots + b_n x_n.$$

Fijemos $j \in \{1, \dots, n\}$ cualquiera y supongamos que $d \nmid b_j$. Por el Algoritmo de la División (Teorema 2.3.2), existirán $q \in \mathbb{Z}$ y $r \in \mathbb{N}$ tales que $b_j = qd + r$ y $0 < r < d$. Entonces

$$r = b_j - qd = b_j - q(b_1 x_1 + \cdots + b_n x_n) = (1 - qx_j)b_j + \sum_{i \neq j} (-qx_i)b_i > 0.$$

Luego $r \in S$, lo cual es absurdo pues $r < d$ y d es el mínimo de S . Por lo tanto $d \mid b_j$. Como j es arbitrario, concluimos que $d \in \text{Div}(b_1, \dots, b_n)$.

Si ahora $c \in \text{Div}(b_1, \dots, b_n)$, entonces $c \mid b_i$ para cada $i = 1, \dots, n$, con lo cual existen $k_i \in \mathbb{N}$, $i = 1, \dots, n$, tales que $b_i = k_i c$. Luego

$$d = \sum_{i=1}^n b_i x_i = \left(\sum_{i=1}^n x_i k_i \right) c.$$

Es decir, $c \mid d$, y por lo tanto $c \leq d$. Luego $d = \max \text{Div}(b_1, \dots, b_n)$ como queríamos probar. \square

Corolario 2.3.5. *El máximo común divisor entre los números naturales b_1, \dots, b_n es la única combinación entera positiva de b_1, \dots, b_n que divide a b_i para cada $i = 1, \dots, n$.*

Demostración. Sea $d = \text{m.c.d.}(b_1, \dots, b_n)$. Por el Teorema 2.3.4, d es una combinación lineal entera positiva de b_1, \dots, b_n que divide a todos ellos. Supongamos que $c = \sum_{i=1}^n s_i b_i > 0$ es un divisor común de b_1, \dots, b_n . Entonces $c \leq d$ pues d es el máximo entre los divisores comunes de b_1, \dots, b_n . Pero a su vez $c \in S$, donde S es el conjunto dado por 2.1. Como $d = \min S$, resulta $d \leq c$. Luego $c = d$. \square

Teorema 2.3.6. *Sean b_1, b_2, \dots, b_n números naturales. $d = \text{m.c.d.}(b_1, \dots, b_n)$ si y sólo si d verifica:*

1. $d \in \text{Div}(b_1, \dots, b_n)$
2. *si $c \in \text{Div}(b_1, \dots, b_n)$, entonces $c \mid d$.*

Demostración. Supongamos primero que $d = \text{m.c.d.}(b_1, \dots, b_n)$. Entonces $d \in \text{Div}(b_1, \dots, b_n)$ y con el mismo razonamiento que en la prueba del Teorema 2.3.4 es inmediato ver que si $c \in \text{Div}(b_1, \dots, b_n)$ entonces $c \mid d$.

Recíprocamente, si $d \in \mathbb{N}$ verifica los puntos 1 y 2, entonces d es un divisor común de b_1, \dots, b_n , y si c es otro divisor común, entonces $c \mid d$, con lo cual $c \leq d$. Luego $d = \max \text{Div}(b_1, \dots, b_n)$. \square

Teorema 2.3.7. Sean b_1, b_2, \dots, b_n números naturales. $m = \text{m.c.m.}(b_1, \dots, b_n)$ si y sólo si m verifica

1. $m \in \text{Mul}(b_1, \dots, b_n)$
2. si $c \in \text{Mul}(b_1, \dots, b_n)$ entonces $m \mid c$, o sea, c es múltiplo de m .

Demostración. Supongamos primero que $m = \text{m.c.m.}(b_1, \dots, b_n)$. Claramente m verifica el punto 1, es decir, existen $x_1, \dots, x_n \in \mathbb{N}$ tales que $m = x_i b_i$ para cada $i = 1, \dots, n$.

Veamos que m verifica el punto 2. Sea c un múltiplo común de b_1, \dots, b_n . Entonces existen $y_1, \dots, y_n \in \mathbb{N}$ tales que $c = y_i b_i$, para cada $i = 1, \dots, n$. Supongamos que $m \nmid c$. Aplicamos el Algoritmo de la División para dividir c por m y obtenemos $q \in \mathbb{Z}$, $r \in \mathbb{N}$ con $0 < r < m$ tales que $c = qm + r$. Entonces

$$r = c - qm = y_i b_i - q x_i b_i = (y_i - q x_i) b_i, \quad \forall i = 1, \dots, n$$

es decir, $r \in \text{Mul}(b_1, \dots, b_n)$, lo cual es absurdo pues $r < m$ y m es el mínimo de este conjunto.

Si ahora m verifica los puntos 1 y 2, entonces $m \in \text{Mul}(b_1, \dots, b_n)$, y para cualquier otro elemento c de este conjunto, como $m \mid c$, resulta $m \leq c$. Luego $m = \min \text{Mul}(b_1, \dots, b_n)$. \square

Teorema 2.3.8 (Algoritmo de Euclides). Sean $a, b \in \mathbb{N}$. Aplicamos reiteradamente el algoritmo de la división como sigue:

$$\begin{aligned} a &= q_1 b + r_1 & 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ &\dots \end{aligned}$$

$$\begin{aligned} r_i &= q_{i+2} r_{i+1} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\ &\dots \end{aligned}$$

$$\begin{aligned} r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} &= q_k r_{k-1} + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k. \end{aligned}$$

Entonces r_k , el último resto no nulo, es el máximo común divisor de a y b .

Demostración. Observemos primero que el algoritmo termina en una cantidad finita de pasos puesto que para cada i , $0 \leq r_{i+1} < r_i$ y por lo tanto en algún momento el resto debe ser cero (si no deberían existir infinitos números naturales menores que un número natural dado). Por otro lado, si recorremos el proceso anterior hacia arriba tenemos: $r_k \mid r_{k-1}$, y como $r_k \mid r_k$, es inmediato verificar que $r_k \mid q_k r_{k-1} + r_k = r_{k-2}$. Subiendo un renglón y aplicando la misma propiedad, vemos que r_k divide a r_{k-3} . Siguiendo así hacia arriba, llegamos a que $r_k \mid b$ y $r_k \mid a$.

Supongamos ahora que $c \mid a$ y $c \mid b$. Entonces del primer renglón del algoritmo, $c \mid r_1$. Del segundo renglón tenemos $c \mid b$ y $c \mid r_1$, entonces $c \mid r_2$. Siguiendo así hacia abajo, llegamos a que $c \mid r_k$ como queríamos probar. \square

Ejemplo 2.3.9. Determinemos m. c. d.(250, 111). El primer paso es dividir 250 por 111 y obtener el resto. Así:

$$250 = 2 \cdot 111 + 28.$$

Luego $r_1 = 28$. Aplicamos nuevamente el algoritmo de la división, dividiendo 111 por 28. Obtenemos

$$111 = 3 \cdot 28 + 27$$

de donde $r_2 = 27$. Dividimos ahora r_1 por r_2 para obtener:

$$28 = 1 \cdot 27 + 1$$

con lo cual $r_3 = 1$. Dividiendo r_2 por r_3 , o sea 27 por 1, obtenemos finalmente resto 0. Concluimos que m. c. d.(250, 111) = 1.

El Algoritmo de Euclides nos permite además expresar el máximo común divisor como combinación entera de ambos números. Para ello debemos “recorrerlo hacia atrás”:

$$\begin{aligned} 1 &= 28 - 1 \cdot 27 = 28 - 1 \cdot (111 - 3 \cdot 28) = (-1) \cdot 111 + 4 \cdot 28 \\ &= (-1) \cdot 111 + 4 \cdot (250 - 2 \cdot 111) = 4 \cdot 250 + (-9) \cdot 111. \end{aligned}$$

■

Finalizaremos esta sección introduciendo los conceptos de números primos y coprimos:

Definición 2.3.10. Un número entero k se dice **primo** si tiene exactamente dos divisores positivos: 1 y k . Si k tiene más de dos divisores positivo, k se dice **compuesto** (en consecuencia 1 no es ni primo ni compuesto).

Dos enteros a y b se denominan **coprimos** o **primos relativos** si m. c. d.(a, b) = 1.

Lema 2.3.11. Dos números naturales a y b son coprimos si y sólo si existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$.

Demostración. Si a y b son coprimos, entonces m. c. d.(a, b) = 1 y por el Teorema 2.3.4, 1 puede expresarse como una combinación lineal entera de a y b .

Supongamos ahora que existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$. Entonces 1 es una combinación lineal entera positiva de a y b que trivialmente divide a a y b . Luego por el Corolario 2.3.5 debe ser $1 = \text{m. c. d.}(a, b)$. □

Teorema 2.3.12. Sea $n \in \mathbb{N}$ un número compuesto. Entonces existe un número primo p tal que $p \mid n$.

Demostración. Supongamos lo contrario y consideremos el conjunto S de todos los números naturales compuestos que no tienen divisores primos. Estamos suponiendo que $S \neq \emptyset$, y por el Teorema 2.3.1, S tiene un elemento mínimo m . Entonces m es compuesto y por lo tanto $m = m_1 \cdot m_2$, con $1 < m_1 < m$ y $1 < m_2 < m$. De estas desigualdades obtenemos que ni m_1 ni m_2 están en S . Pero entonces alguno de los dos es primo, o alguno tiene un divisor primo, que a su vez será divisor de m . Esto contradice el hecho que $m \in S$, con lo cual $S = \emptyset$. □

Teorema 2.3.13 (Euclides). *Existen infinitos números primos.*

Demostración. Supongamos por el contrario que existe sólo una cantidad finita p_1, \dots, p_k de números primos positivos y definamos

$$B = p_1 p_2 \cdots p_k + 1.$$

Como $B > p_i$ para cada $1 \leq i \leq k$, B no puede ser primo. Como además $B > 1$, B es compuesto. Así, por el Teorema 2.3.12, existe un primo, que deberá ser alguno de los p_i , digamos p_j , tal que $p_j \mid B$. Pero además $p_j \mid p_1 p_2 \cdots p_k$ de donde resulta que $p_j \mid 1$ lo cual es absurdo. \square

Teorema 2.3.14 (Teorema Fundamental de la Aritmética). *Cada número natural $n > 1$ puede escribirse de manera única como un producto de factores primos, excepto por el orden de los mismos.*

Demostración. *Existencia:* Supongamos que la existencia de la factorización por primos no fuese cierta. Entonces el conjunto S de los números naturales $n > 1$ que no pueden escribirse como producto de factores primos es no vacío, y por el Teorema 2.3.1 existirá un primer natural $m > 1$ tal que m no puede expresarse como producto de factores primos. En particular m no es primo (pues en ese caso constaría de un único factor primo) y por lo tanto, al ser $m > 1$, m debe ser compuesto.

Sean m_1, m_2 con $1 < m_1, m_2 < m$ tales que $m = m_1 m_2$. Como m es el menor número que no puede expresarse como producto de números primos, tanto m_1 como m_2 admitirán una factorización en factores primos, y por consiguiente también lo hará m , lo cual es absurdo.

Unicidad: Puesto que el Teorema es sobre números naturales mayores que uno, aplicaremos la forma alternativa del principio de inducción para el caso base $n_0 = 2$. El teorema es en este caso trivialmente cierto: siendo 2 un número primo, no admite ninguna otra descomposición en factores de ningún tipo. Supongamos que la unicidad es válida para todos los números naturales $2, 3, 4, \dots, n-1$ y veamos que también es válida para n . Supongamos que n puede escribirse como

$$n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r}$$

donde cada p_i y cada q_j es un número primo. También supondremos que los números están ordenados de modo que $p_1 < p_2 < \cdots < p_k$ y $q_1 < q_2 < \cdots < q_r$ y que cada $s_i \geq 1$, $r_j \geq 1$.

Tomemos el número primo p_1 y supongamos que $p_1 \neq q_j$ para cada $j = 1, \dots, r$. Como p_1 y cada q_j son primos distintos, es fácil ver que $(p_1 : q_j^{t_j}) = 1$ para cada $j = 1, \dots, r$. Por otra parte p_1 divide a $n = q_1^{t_1} \cdots q_r^{t_r}$. Como $(p_1 : q_1^{t_1}) = 1$, por el Ejercicio 18 de la Unidad 2, deberá ser

$$p_1 \mid q_2^{t_2} \cdots q_r^{t_r}.$$

Pero nuevamente, $(p_1 : q_2^{t_2}) = 1$ y por lo tanto

$$p_1 \mid q_3^{t_3} \cdots q_r^{t_r}.$$

Si aplicamos reiteradamente el mismo argumento llegaremos a que debe ser $p_1 \mid q_r^{s_r}$ lo que es absurdo. Por lo tanto, deberá existir j_0 tal que $p_1 = q_{j_0}$. Observemos que j_0 debe ser igual a 1. En efecto, tenemos que

$q_1 \mid n$, y con el mismo argumento, existirá p_{i_0} tal que $q_1 = p_{i_0}$. Si $i_0 > 1$, como hemos ordenado los factores primos de menor a mayor, tendremos:

$$p_1 < p_{i_0} = q_1 < q_{j_0}$$

lo cual es absurdo. Concluimos que $p_1 = q_1$.

Veamos ahora que $s_1 = t_1$. Recordemos que estamos realizando la prueba por inducción. Aplicaremos en este momento la hipótesis inductiva. Como $p_1 \mid n$ y $s_1 \geq 1$, tenemos que

$$n_1 = \frac{n}{p_1} = p_1^{s_1-1} p_2^{s_2} \cdots p_k^{s_k} = p_1^{t_1-1} q_2^{t_2} \cdots q_r^{t_r} \in \mathbb{Z}.$$

Pero $n_1 < n$, luego por hipótesis inductiva su factorización en primos es única salvo orden. Pero como los primos están ordenados de menor a mayor, concluimos que $k = r$, cada $p_i = q_i$ y cada $s_i = t_i$. \square

Dejamos como **ejercicio** probar la siguiente consecuencia del Teorema Fundamental de la Aritmética:

Corolario 2.3.15. Sean $x, y \in \mathbb{N}$, $x = p_1^{s_1} \cdots p_k^{s_k}$, $y = q_1^{t_1} \cdots q_r^{t_r}$ con p_i, q_j primos, $p_i \neq p_j$ y $q_i \neq q_j$ si $i \neq j$. Entonces m.c.d.(x, y) es el producto de los factores primos comunes de x e y elevados al mínimo exponente en el que aparecen y m.c.m.(x, y) es el producto de los factores comunes y no comunes elevados al máximo exponente en el que aparecen.

2.4. Subconjuntos acotados, ínfimo y supremo

Retomemos ahora la teoría general para un poset cualquiera. Estudiaremos en esta sección algunos elementos característicos importantes de un subconjunto de un poset.

Definición 2.4.1. Sea (A, \preceq) un poset, $B \subseteq A$ y sean $x_0, y_0 \in A$. Decimos que

- x_0 es **cota inferior** de B si $x_0 \preceq b$ para cada $b \in B$. Si existe una cota inferior de B decimos también que B está **acotado inferiormente**.
- y_0 es **cota superior** de B si $b \preceq y_0$ para cada $b \in B$. Si existe una cota superior de B decimos también que B está **acotado superiormente**.
- x_0 es un **ínfimo** de B si x_0 es el máximo de

$$\{c \in A : c \text{ es cota inferior de } B\}$$

- y_0 es un **supremo** de B si y_0 es el mínimo de

$$\{c \in A : c \text{ es cota superior de } B\}$$

De la unicidad del mínimo y máximo de un conjunto (Teorema 2.2.8) obtenemos inmediatamente:

Teorema 2.4.2. Sea (A, \preceq) un poset y sea $B \subset A$. Si B posee ínfimo (resp. supremo) entonces éste es único.

Notación 2.4.3. Dado un subconjunto B de un poset (A, \preceq) , si x_0 es el (único) ínfimo de B e y_0 es el (único) supremo de B los denotamos

$$x_0 = \inf B, \quad y_0 = \sup B.$$

Lema 2.4.4. Sea (A, \preceq) un poset y $B \subset A$. Entonces:

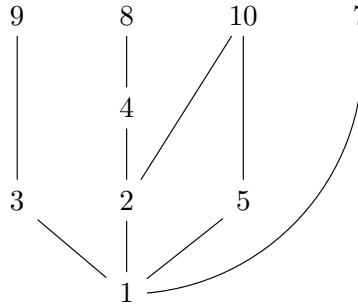
1. $x_0 = \min B$ si y sólo si $x_0 = \inf B$ y $x_0 \in B$.
2. $y_0 = \max B$ si y sólo si $y_0 = \sup B$ e $y_0 \in B$.

Demostración. Supongamos primero que x_0 es un mínimo de B . Entonces para cada $x \in B$, $x_0 \preceq x$. Si ahora $c \in A$ es una cota inferior de B , entonces $c \preceq x$ para cada $x \in B$. En particular, como $x_0 \in B$, $c \preceq x_0$. Luego x_0 es el máximo del conjunto de cotas inferiores de B , y por lo tanto $x_0 = \inf B$.

Recíprocamente, supongamos que existe $x_0 = \inf B$ y $x_0 \in B$. Entonces x_0 es en particular una cota inferior de B , esto es, $x_0 \preceq x$ para cada $x \in B$. Como $x_0 \in B$, resulta $x_0 = \min B$.

La prueba del punto 2 es análoga y se deja como **ejercicio**. □

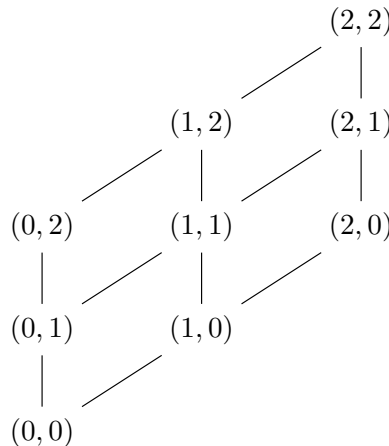
Ejemplo 2.4.5. Consideremos la relación “divide a” en el conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, cuyo diagrama de Hasse, presentado en el Ejemplo 2.1.7 es el siguiente:



Consideremos el subconjunto $B = \{2, 5\} \subset A$, tenemos que 10 es la única cota superior de B y es su supremo, a la vez que 1 es la única cota inferior de B , y es su ínfimo.

Si tomamos $C = \{3, 5\}$, podemos observar que este subconjunto no tiene cotas superiores, y por lo tanto no tiene supremo. Nuevamente, 1 es la única cota inferior y el ínfimo de C . ■

Ejemplo 2.4.6. Sea $A = \{0, 1, 2\}$ con el orden usual \leq y consideremos el poset $(A \times A, \preceq_{prod})$. El diagrama de Hasse para $(A \times A, \preceq_{prod})$ (introducido en el Ejemplo 2.1.9) es



Aquí tenemos que $\min(A \times A) = (0, 0)$ y $\max A \times A = (2, 2)$. Consideremos el subconjunto

$$B = \{(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0)\}$$

tendremos que $\min B = (0, 0)$, y por el Lema 2.4.4 resulta $x_0 = \inf B$. Por otra parte B posee tres elementos maximales, $(0, 2)$, $(1, 1)$ y $(2, 0)$. Luego del Lema 2.2.10, B no posee máximo. B tiene además una única cota superior, $(2, 2)$, y por lo tanto $\sup B = (2, 2)$.

Ejemplo 2.4.7. Consideremos el conjunto parcialmente ordenado $(\mathbb{N}, |)$ y sea $B = \{b_1, b_2, \dots, b_n\} \subset \mathbb{N}$ un subconjunto finito cualquiera de \mathbb{N} . Observemos que B está acotado inferiormente por 1, y superiormente por $M = b_1 \cdot b_2 \cdots b_n$. Analicemos la existencia de ínfimo y el supremo de B .

Observemos que un elemento d será el ínfimo de B si:

- d es una cota inferior de B , es decir, $d \mid b_j$ para cada $j = 1, \dots, n$.
- d es la mayor cota inferior de B , o sea, si c es otra cota inferior (i.e., $c \mid b_j$ para cada $j = 1, \dots, n$), entonces $c \mid d$.

Resulta inmediato del Teorema 2.3.6 que existe el ínfimo de B y resulta

$$\inf B = \text{m. c. d.}(b_1, \dots, b_n).$$

De manera análoga puede probarse a partir del Teorema 2.3.7 que siempre existe el supremo de B y es

$$\sup B = \text{m. c. m.}(b_1, \dots, b_n).$$

Si consideramos por ejemplo el conjunto $B = \{30, 70, 80\}$, tenemos que las cotas inferiores de B , que son los divisores comunes de sus elementos, son 1, 2, 5 y 10. Por lo tanto

$$\inf B = \text{m. c. d.}(30, 70, 80) = \max\{1, 2, 5, 10\} = 10.$$

B está acotado superiormente por infinitos elementos, pero una cota superior obvia es $M = 30 \cdot 70 \cdot 80 = 168000$. Sin embargo, la menor de las cotas inferiores es $y_0 = 1680$, que es el mínimo común múltiplo de 30, 70 y 80. Por lo tanto $\sup B = \text{m. c. m.}(30, 70, 80) = 1680$. ■

Observación 2.4.8. *Un axioma fundamental en la teoría axiomática de los números reales es el Axioma del supremo, que establece que un subconjunto B de (\mathbb{R}, \leq) acotado superiormente tiene supremo. Los ejemplos que vimos hasta acá pueden hacernos pensar que este resultado es válido para cualquier poset (A, \preceq) . Sin embargo esto es falso, como veremos en el ejemplo siguiente.*

Ejemplo 2.4.9. Consideremos el poset (\mathbb{Q}, \leq) y sea $A = \{x \in \mathbb{Q} : x^2 < 2\}$. Es fácil verificar que 2 es una cota superior de A y -2 es una cota inferior, con lo cual A es acotado superior e inferiormente.

Como subconjunto de (\mathbb{R}, \leq) , A tiene supremo y es $\sqrt{2}$ que no es un elemento de \mathbb{Q} . Supongamos que existe q_0 el supremo de A como subconjunto de (\mathbb{Q}, \leq) . Entonces deberá ser $q_0 > \sqrt{2}$, pues de otra manera q_0 sería una cota superior de A como subconjunto de (\mathbb{R}, \leq) menor que su supremo.

Como \mathbb{Q} es denso en \mathbb{R} , en el intervalo real $(\sqrt{2}, q_0)$ existen infinitos números racionales. En particular existirá $q_1 \in \mathbb{Q}$ tal que $\sqrt{2} < q_1 < q_0$. Pero entonces q_1 es una cota superior de A en (\mathbb{Q}, \leq) menor que el supremo de A , lo que es absurdo.

Concluimos que A es un subconjunto de (\mathbb{Q}, \leq) acotado superiormente que no tiene supremo. ■

Hemos observado que si (A, \preceq) es un conjunto ordenado, entonces (A, \succeq) también lo es, siendo \succeq la relación inversa a \preceq . Existe una relación estrecha entre los elementos destacados de (A, \preceq) (mínimos, ínfimos, máximos, etc.) y los elementos destacados “inversos” de (A, \succeq) denominada **Principio de Dualidad**. Este principio establece que cualquier proposición que involucre cotas inferiores, elementos minimales, mínimos o ínfimos en (A, \preceq) sigue siendo válida en (A, \succeq) cambiando estos elementos por cotas superiores, elementos maximales, máximos o supremos respectivamente (y también cambiando cotas superiores en (A, \preceq) por cotas inferiores en (A, \succeq) , etc.). El Principio de Dualidad se basa en el siguiente resultado, cuya prueba dejamos como **ejercicio**.

Teorema 2.4.10. *Sea (A, \preceq) un conjunto parcialmente ordenado y sea \succeq el orden inverso de \preceq . Entonces*

1. *Si a es un elemento minimal (resp. maximal) de (A, \preceq) , entonces a es un elemento maximal (resp. minimal) de (A, \succeq) .*
2. *Si a es un mínimo (resp. máximo) de (A, \preceq) , entonces a es un máximo (resp. mínimo) de (A, \succeq) .*
3. *Sea $B \subseteq A$. Si a es una cota inferior de B (resp. cota superior) en (A, \preceq) , entonces a es una cota superior de B (resp. cota inferior) en (A, \succeq) .*
4. *Sea $B \subseteq A$. Si a es el ínfimo de B (resp. supremo) en (A, \preceq) , entonces a es el supremo de B (resp. ínfimo) en (A, \succeq) .*

Ejemplo 2.4.11. Consideremos en \mathbb{N} el orden \succeq dado por $a \succeq b$ si a es múltiplo de b . Como a es múltiplo de b si y sólo si b divide a a , resulta que \succeq es la relación inversa de la relación “divide a” en \mathbb{N} . Por lo tanto \succeq tiene un máximo en 1 (dado que 1 es el mínimo de $(\mathbb{N}, |)$). Por otra parte, si restringimos \succeq al conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos obtener el diagrama de Hasse de \succeq invirtiendo el diagrama de Hasse de la relación “divide a” presentado en el Ejemplo 2.1.5:

Diagrama de Hasse de “divide a”

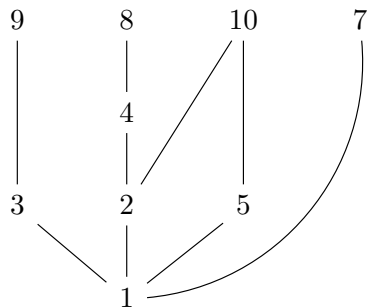
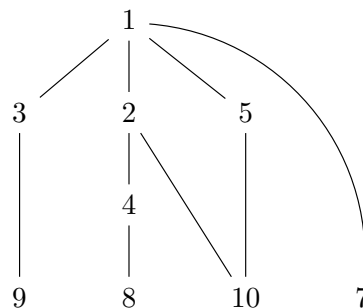


Diagrama de Hasse de \succeq “es múltiplo de”



Observemos que como $(A, |)$ no tiene máximo, (A, \succeq) no tiene mínimo. Como 8, 9, 10 y 7 son elementos maximales de $(A, |)$, estos mismos elementos son minimales en (A, \succeq) .

Si ahora consideramos el subconjunto $B = \{2, 5\} \subset (A, |)$ tenemos que 10 es la única cota superior de B y es su supremo, a la vez que 1 es la única cota inferior de B , y es su ínfimo. Por lo tanto 10 es el ínfimo de B en (A, \succeq) y 1 es su supremo.

Si tomamos $C = \{2, 3, 5\}$, C no tiene supremo en $(A, |)$ y 1 es el ínfimo de C en $(A, |)$. Por lo tanto C no tiene ínfimo en (A, \succeq) y su supremo es 1. ■

Ejemplo 2.4.12. Aplicaciones teóricas del principio de dualidad. El Principio de Dualidad permite “economizar” muchas demostraciones en conjuntos ordenados reduciéndolas a la mitad. De hecho podemos dar por completas las pruebas de los Teoremas 2.2.7, y 2.2.8, el Lema 2.2.10 y el Corolario 2.2.11 aplicando el Principio de Dualidad. En la prueba del Teorema 2.2.7 por ejemplo hemos probado únicamente que un subconjunto finito B de un poset (A, \preceq) tiene un elemento minimal. Pero B es también un subconjunto finito del poset (A, \succeq) con lo cual tiene un elemento minimal en (A, \succeq) que será un elemento maximal en (A, \preceq) .

En el Teorema 2.2.8 probamos que el elemento mínimo de un poset (A, \preceq) , si existe, es único. Como el máximo de (A, \preceq) , si existe, es el mínimo de (A, \succeq) , entonces también debe ser único. Podemos razonar de la misma manera con los demás resultados. ■

2.5. Morfismos de posets

Dados dos conjuntos parcialmente ordenados (A, \preceq_A) y (B, \preceq_B) nos interesa estudiar aquellas funciones $f : A \rightarrow B$ que “preservan” el orden:

Definición 2.5.1. Sean (A, \preceq_A) y (B, \preceq_B) dos posets y sea $f : A \rightarrow B$ una función. Decimos que:

- f es un **morfismo de orden** o **morfismo de posets** si para cada $x, y \in A$ se verifica

$$x \preceq_A y \implies f(x) \preceq_B f(y)$$

- f es un **isomorfismo de posets** de (A, \preceq_A) en (B, \preceq_B) si f es un morfismo de orden biyectivo tal que $f^{-1} : B \rightarrow A$ es un morfismo de posets.

Observación 2.5.2. Muchas veces usaremos la notación $f : (A, \preceq_A) \rightarrow (B, \preceq_B)$ para indicar una función entre conjuntos ordenados, donde nos interese remarcar el orden en A y B . Esta notación es particularmente útil cuando $A = B$ pero los órdenes \preceq_A y \preceq_B son distintos.

Ejemplo 2.5.3. Claramente para cualquier poset (A, \preceq) , la función identidad $\text{Id} : (A, \preceq) \rightarrow (A, \preceq)$ es un isomorfismo de (A, \preceq) en (A, \preceq) .

Esto no es cierto si en A tomamos dos órdenes distintos como quedará claro en el ejemplo siguiente. ■

Ejemplo 2.5.4. Consideremos las funciones $f = \text{Id} : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ y $g = \text{Id} : (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, |)$. Observemos que en términos formales f y g son la misma función. Veremos que tienen comportamientos distintos según los órdenes que consideremos en \mathbb{N} .

Observemos que si $a \mid b$ entonces $f(a) = a \leq b = f(b)$ (pues existe $k \geq 1$ tal que $b = ka$). Luego f es un morfismo de posets. Sin embargo g no es un morfismo de posets. En efecto $2 \leq 3$ y sin embargo $g(2) = 2 \nmid 3 = g(3)$. Como $g = f^{-1}$, f no es un isomorfismo de (\mathbb{N}, \mid) en (\mathbb{N}, \leq) . ■

Teorema 2.5.5. Sean (A, \preceq_A) , (B, \preceq_B) y (C, \preceq_C) posets. Si $f : A \rightarrow B$ y $g : B \rightarrow C$ son morfismos de posets, entonces $g \circ f : A \rightarrow C$ es un morfismo de posets.

Demostración. Sean $x, y \in A$ tales que $x \preceq_A y$. Como f es un morfismo de posets tendremos que $f(x) \preceq_B f(y)$, y como g es un morfismo de posets, resultará entonces $g(f(x)) \preceq_C g(f(y))$. Luego $g \circ f$ es un morfismo de posets. □

Teorema 2.5.6. Sean (A, \preceq_A) y (B, \preceq_B) posets. Si $f : A \rightarrow B$ es un morfismo de posets, entonces f es un isomorfismo de posets si y sólo si f es sobreyectiva y para cada $x, y \in A$ se verifica

$$(2.2) \quad x \preceq_A y \iff f(x) \preceq_B f(y).$$

Demostración. Supongamos primero que f es un isomorfismo de posets de (A, \preceq_A) en (B, \preceq_B) . Entonces f es biyectiva, con lo cual en particular es sobreyectiva, y se verifica que para cada $x, y \in A$,

$$x \preceq_A y \implies f(x) \preceq_B f(y).$$

Debemos entonces probar que si $x, y \in A$ son tales que $f(x) \preceq_B f(y)$ entonces $x \preceq_A y$. Para ello observemos que como f es un isomorfismo, f^{-1} es un morfismo de posets. Luego tendremos:

$$f(x) \preceq_B f(y) \implies f^{-1}(f(x)) \preceq_A f^{-1}(f(y)) \implies x \preceq_A y.$$

Supongamos ahora que f es sobreyectiva y vale la condición (2.2). Veamos primero que f es inyectiva. Sean $x, y \in A$ tales que $f(x) = f(y)$. Entonces tendremos que $f(x) \preceq_B f(y)$ y $f(y) \preceq_B f(x)$. Luego por (2.2), resultará $x \preceq_A y$ y $y \preceq_A x$, con lo cual $x = y$. Concluimos que f es biyectiva.

Veamos ahora que f^{-1} también es un morfismo de posets. Sean $v, w \in B$ tales que $v \preceq_B w$. Como f es biyectiva, existirán únicos $x, y \in A$ tales que $f(x) = v$, $f(y) = w$. Luego $f(x) \preceq_B f(y)$ y de (2.2), resulta $x \preceq_A y$. Pero $x = f^{-1}(v)$ e $y = f^{-1}(w)$, esto es, $f^{-1}(v) \preceq_A f^{-1}(w)$ como queríamos probar. □

Corolario 2.5.7. Sean (A, \preceq_A) y (B, \preceq_B) posets y $f : A \rightarrow B$ un isomorfismo de posets. Si $X \subset A$, entonces $f|_X : X \rightarrow f(X)$ es un isomorfismo de posets de $(X, \preceq_{A|X})$ en $(f(X), \preceq_{B|f(X)})$.

Demostración. Observemos primero que $f|_X : X \rightarrow f(X)$ es biyectiva. Sean $x, x' \in X$. Entonces

$$x \preceq_{A|X} x' \iff x \preceq_A x' \iff f(x) \preceq_B f(x') \iff f|_X(x) \preceq_{B|f(X)} f|_X(x').$$

Sigue del Teorema 2.5.6 que $f|_X : X \rightarrow f(X)$ es un isomorfismo de posets. □

Resumimos en el siguiente resultado las propiedades de los isomorfismos de posets, que son consecuencia inmediata de las propiedades que desarrollamos hasta ahora:

Teorema 2.5.8. Sean (A, \preceq_A) , (B, \preceq_B) y (C, \preceq_C) posets. Entonces

1. $\text{Id} : (A, \preceq_A) \rightarrow (A, \preceq_A)$ es un isomorfismo de posets.
2. f es un isomorfismo de (A, \preceq_A) en (B, \preceq_B) si y sólo si f^{-1} es un isomorfismo de (B, \preceq_B) en (A, \preceq_A) .
3. Si f y g son isomorfismos de posets, entonces $g \circ f$ es un isomorfismo de posets.

Demostración. Los puntos 1 y 2 son inmediatos de la definición de isomorfismo. Dejamos los detalles como **ejercicio**.

Probemos el punto 3. Observemos que por el Teorema 2.5.5 $g \circ f$ es un morfismo de posets, y es biyectivo al ser composición de dos funciones biyectivas. Además tenemos que al ser f y g isomorfismos de posets, del Teorema 2.5.6 para cada $x, y \in A$ resulta

$$x \preceq_A y \Leftrightarrow f(x) \preceq_B f(y) \Leftrightarrow g(f(x)) \preceq_C g(f(y)).$$

Luego se verifica la condición 2.2 y por lo tanto $g \circ f$ es un isomorfismo de posets. \square

El siguiente resultado es inmediato del Teorema 28. Dejamos la prueba como **ejercicio**.

Corolario 2.5.9. Sea Poset el conjunto de todos los conjuntos parcialmente ordenados. Entonces la relación \sim en Poset dada por $(A, \preceq_A) \sim (B, \preceq_B)$ si existe un isomorfismo f de (A, \preceq_A) en (B, \preceq_B) es una relación de equivalencia.

Definición 2.5.10. Dos posets (A, \preceq_A) y (B, \preceq_B) se dicen **posets isomorfos** si existe un isomorfismo de posets $f : A \rightarrow B$ (o equivalentemente, si existe un isomorfismo de posets $g : B \rightarrow A$).

Los posets (A, \preceq_A) y (B, \preceq_B) se dicen **anti-isomorfos** si (A, \preceq_A) es isomorfo a (B, \succeq_B) .

Ejemplo 2.5.11. Sea A un conjunto finito de cardinal n totalmente ordenado. Observemos que como A es finito y todos sus elementos son comparables 2 a 2 podemos escribir $A = \{a_1, a_2, \dots, a_n\}$ donde

$$a_1 \preceq a_2 \preceq \dots \preceq a_n.$$

En particular, resulta $a_i \preceq_A a_j$ si y sólo si $i \leq j$.

Consideremos el conjunto $I_n = \{1, 2, \dots, n\} \subset \mathbb{N}$ con el orden \leq_{I_n} y sea $\Phi : I_n \rightarrow A$ dada por $\Phi(i) = a_i$. Tendremos entonces

$$i \leq j \iff a_i \preceq a_j \iff \Phi(i) \preceq \Phi(j)$$

Resulta del Teorema 2.5.6 que Φ es un isomorfismo de posets.

En consecuencia, todo conjunto finito totalmente ordenado de cardinal n es isomorfo a (I_n, \leq) y por lo tanto dos conjuntos finitos totalmente ordenados son isomorfos si y sólo si tienen el mismo cardinal. \blacksquare

Ejemplo 2.5.12. Sea $X = \{0, 1\}^n = \{0, 1\} \times \{0, 1\} \times \cdots \times \{0, 1\} = \{(\varepsilon_1, \dots, \varepsilon_n) : \varepsilon_i \in \{0, 1\}\}$ con el orden producto usual, esto es, $(\varepsilon_1, \dots, \varepsilon_n) \preceq (\varepsilon'_1, \dots, \varepsilon'_n)$ si $\varepsilon_i \leq \varepsilon'_i$ para cada $i = 1, \dots, n$. Sea $I_n = \{1, \dots, n\} \subset \mathbb{N}$ y consideremos el poset $(\mathcal{P}(I_n), \subseteq)$. Sea $f : \mathcal{P}(I_n) \rightarrow X$ dada por $f(A) = (\varepsilon_1^A, \dots, \varepsilon_n^A)$ donde

$$\varepsilon_n^A = \begin{cases} 1 & \text{si } i \in A \\ 0 & \text{si } i \notin A \end{cases}$$

Observemos que f es sobreyectiva: dado $(\varepsilon_1, \dots, \varepsilon_n) \in X$, sea $A = \{i \in I_n : \varepsilon_i = 1\}$. Entonces es claro que $f(A) = (\varepsilon_1, \dots, \varepsilon_n)$.

Sean $A, B \subseteq I_n$. Supongamos que $A \subseteq B$ y veamos que $(\varepsilon_1^A, \dots, \varepsilon_n^A) \preceq (\varepsilon_1^B, \dots, \varepsilon_n^B)$. Tomemos $j \in 1, \dots, n$ cualquiera. Si $\varepsilon_j^A = 0$, entonces trivialmente $\varepsilon_j^A \leq \varepsilon_j^B$. Si $\varepsilon_j^A = 1$, entonces $j \in A$, y por lo tanto $j \in B$. Luego $\varepsilon_j^A = \varepsilon_j^B = 1$. En cualquier caso, $\varepsilon_j^A \leq \varepsilon_j^B$ como queríamos ver.

Supongamos ahora que $(\varepsilon_1^A, \dots, \varepsilon_n^A) \preceq (\varepsilon_1^B, \dots, \varepsilon_n^B)$ y veamos que $A \subseteq B$. Sea $j \in A$. Entonces $\varepsilon_j^A = 1$, y como $\varepsilon_j^A \leq \varepsilon_j^B$ deberá ser $\varepsilon_j^B = 1$, es decir, $j \in B$.

Concluimos que

$$A \subseteq B \iff f(A) \preceq f(B).$$

Luego del Teorema 2.5.6 f es un isomorfismo de posets. ■

Hemos visto en el Ejemplo 2.5.4 que $\text{Id} : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ no es un isomorfismo de posets. Sin embargo, esto NO implica que estos posets no sean isomorfos, pues podría existir otra función que sí sea un isomorfismo. En general, para probar que dos posets no son isomorfos debemos encontrar alguna propiedad que se preserve por isomorfismos y que tenga uno de ellos pero no tenga el otro. Estas propiedades se denominan **invariantes**. En los resultados siguientes presentamos los invariantes fundamentales por isomorfismos de posets.

Teorema 2.5.13. Sean (A, \preceq_A) , (B, \preceq_B) posets y sea $f : A \rightarrow B$ un isomorfismo de posets. Entonces:

1. A y B tienen el mismo cardinal.
2. A es totalmente ordenado si y sólo si B es totalmente ordenado.

Demostración. El punto 1 es consecuencia del hecho que dos conjuntos tienen el mismo cardinal si y sólo si existe una biyección entre ellos.

Probemos el punto 2. Supongamos primero que A es totalmente ordenado y sean $b_1, b_2 \in B$. Como f es un isomorfismo, existen $a_1, a_2 \in A$ tales que $b_1 = f(a_1)$ y $b_2 = f(a_2)$. Como A es totalmente ordenado, $a_1 \preceq_A a_2$ o $a_2 \preceq_A a_1$. Pero como f es un morfismo de posets, $f(a_1) \preceq_B f(a_2)$ o $f(a_2) \preceq_B f(a_1)$, es decir, $b_1 \preceq_B b_2$ o $b_2 \preceq_B b_1$. Concluimos que B es totalmente ordenado.

Si ahora suponemos que B es totalmente ordenado, como $f^{-1} : B \rightarrow A$ también es un isomorfismo de posets, resulta A totalmente ordenado por el argumento anterior. □

Ejemplo 2.5.14. A partir del Teorema 2.5.13 podemos concluir que los posets $(\mathbb{N}, |)$ y (\mathbb{N}, \leq) no son isomorfos pues (\mathbb{N}, \leq) es totalmente ordenado y $(\mathbb{N}, |)$ no lo es (o sea, no puede existir ninguna otra función entre ellos que sea un isomorfismo de posets). ■

Teorema 2.5.15. Sean (A, \preceq_A) , (B, \preceq_B) posets y sea $f : A \rightarrow B$ un isomorfismo de posets. Entonces:

1. $a \in A$ es un elemento maximal (resp. minimal) de A si y sólo si $f(a)$ es un elemento maximal (resp. minimal) de B .
2. $a \in A$ es un máximo (resp. mínimo) de A si y sólo si $f(a)$ es un máximo (resp. mínimo) de B .
3. Sea $X \subseteq A$. $a \in A$ es una cota superior (resp. inferior) de X si y sólo si $f(a)$ es una cota superior (resp. inferior) de $f(X)$.
4. Sea $X \subseteq A$. $a \in A$ es el supremo (resp. ínfimo) de X si y sólo si $f(a)$ es el supremo (resp. ínfimo) de $f(X)$.

Demostración. Probemos el punto 1. Supongamos que a es un elemento maximal de A y sea $b = f(a)$. Sea $b' \in B$ tal que $b \preceq_B b'$ y $a' \in A$ tal que $f(a') = b'$. Entonces $f(a) \preceq_B f(a')$ y por el Teorema 2.5.6 debe ser $a \preceq_A a'$. Como a es maximal, $a' = a$ y por lo tanto $b = f(a) = f(a') = b'$. Luego b es un elemento maximal de B .

Si ahora suponemos que $b = f(a)$ es un elemento maximal de B , entonces $a = f^{-1}(b)$ es un elemento maximal de A , dado que $f^{-1} : B \rightarrow A$ también es un isomorfismo de posets.

Para probar el punto 2, sea a el máximo de A . Sea $b = f(a)$ y $b' \in B$ cualquiera. Sea $a' \in A$ tal que $f(a') = b'$. Entonces, como a es un máximo, $a' \preceq_A a$, con lo cual $f(a') \preceq_B f(a)$, es decir, $b' \preceq_B b$, y como b' es arbitrario, resulta b el máximo de B .

Si ahora $b = f(a)$ es el máximo de B , entonces $a = f^{-1}(b)$ será el máximo de A por el argumento anterior, dado que $f^{-1} : B \rightarrow A$ es un isomorfismo de posets.

La prueba del punto 1 cuando a es un elemento minimal, así como la prueba del punto 2 cuando a es un mínimo son análogas y las dejamos como **ejercicio**.

A esta altura podemos notar que basta probar una de las implicaciones de cada punto, dado que las recíprocas siguen de aplicar la proposición demostrada para el isomorfismo $f^{-1} : B \rightarrow A$.

Teniendo esto en cuenta, probaremos sólo la primer implicación de los puntos 3 y 4.

Supongamos que a es una cota superior de un subconjunto $X \subset A$. Entonces $x \preceq_A a$ para cada $x \in X$, y por lo tanto $f(x) \preceq_B f(a)$ para cada $x \in X$. Luego $f(a)$ es una cota superior de $f(X)$. El razonamiento si a es una cota inferior es análogo.

Supongamos finalmente que $a = \sup X$. Sea C el conjunto de cotas superiores de X . Entonces $f(C)$ es el conjunto de cotas superiores de $f(X)$ por el punto 3. Por el corolario 2.5.7, $f|_C : C \rightarrow f(C)$ es un isomorfismo de posets. Como $a = \min C$, por el punto 2 resulta $f(a) = \min f(C)$, esto es, $f(a) = \sup f(X)$. La prueba para el ínfimo es análoga. \square

Ejemplo 2.5.16. (\mathbb{N}, \leq) y (\mathbb{N}, \geq) son conjuntos totalmente ordenados no isomorfos, dado que (\mathbb{N}, \leq) tiene mínimo y (\mathbb{N}, \geq) no tiene. Sin embargo son posets obviamente anti-isomorfos (dado que $\text{Id} : (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, \geq)$ es un isomorfismo de posets). Hay infinitos ordenes en \mathbb{N} no isomorfos entre sí. Mostraremos a continuación como construir uno de ellos. Veremos en los ejercicios cómo generalizar este procedimiento.

Consideremos S_0 el conjunto de números naturales pares y S_1 el conjunto de números naturales impares. Observemos que $\{S_0, S_1\}$ es una partición de \mathbb{N} . Definamos la relación \preceq en \mathbb{N} como sigue:

- Si $x \in S_0$ y $y \in S_1$, $x \preceq y$.
- Si $x, y \in S_0$, $x \preceq y$ si y sólo si $x \leq y$.
- Si $x, y \in S_1$, $x \preceq y$ si y sólo si $y \leq x$.

Veamos que \preceq es una relación de orden en \mathbb{N} . Observemos que \preceq es claramente reflexiva, pues un elemento $x \in \mathbb{N}$ está en sólo uno de los subconjuntos S_0 y S_1 y por lo tanto resulta $x \preceq x$ si y sólo si $x \leq x$ (si $x \in S_0$) o $x \geq x$ (si $x \in S_1$). Luego para cada $x \in \mathbb{N}$, $x \preceq x$.

Supongamos ahora que $x, y \in \mathbb{N}$ son tales que $x \preceq y$ y $y \preceq x$. Analizaremos el caso en que $x \in S_0$ y el caso en que $x \in S_1$.

Si $x \in S_0$, como $y \preceq x$, y no puede pertenecer a S_1 , con lo cual $y \in S_0$. Como $\preceq|_{S_0}$ coincide con el orden usual \leq , resulta $x \leq y$ y $y \leq x$ con lo cual $x = y$.

Si ahora $x \in S_1$, como $x \preceq y$, tenemos que y no puede pertenecer a S_0 , y por lo tanto el único caso que debemos analizar es $y \in S_1$. Pero $\preceq|_{S_1}$ coincide con el orden \geq . Tendremos entonces que $x \geq y$ y $y \geq x$ con lo cual nuevamente $x = y$. Concluimos que \preceq es antisimétrica.

Para ver que \preceq es transitiva también debemos proceder por casos. Sean $x, y, z \in \mathbb{N}$ tales que $x \preceq y$ y $y \preceq z$. Supongamos primero que $x \in S_0$:

- Si $z \in S_0$, entonces como $y \preceq z$ deberá ser $y \in S_0$. Por lo tanto tenemos que $x, y, z \in S_0$, y entonces $x \leq y$ e $y \leq z$. Luego $x \leq z$, y como ambos están en S_0 resulta $x \preceq z$.
- Si $z \in S_1$, dado que $x \in S_0$, $x \preceq z$.

Supongamos ahora que $x \in S_1$. En este caso, como $x \preceq y$ deberá ser $y \in S_1$, y como $y \preceq z$, también tendremos $z \in S_1$. Luego $x \geq y$ y $y \geq z$, con lo cual $x \geq z$, o sea, $x \preceq z$.

Luego \preceq es una relación de orden en \mathbb{N} . Observemos que (\mathbb{N}, \preceq) es totalmente ordenado. En efecto, sean $n, m \in \mathbb{N}$. Si $n = m$, n y m son claramente comparables así que supondremos que son distintos. Si $n \in S_0$ y $m \in S_1$, entonces por definición $n \preceq m$. Si $n \in S_1$ y $m \in S_0$, entonces $m \preceq n$. Si $n, m \in S_0$, como $n \leq m$ o $m \leq n$, resulta $n \preceq m$ o $m \preceq n$, y un razonamiento similar prueba que n y m son comparables si ambos están en S_1 .

Veamos finalmente que (\mathbb{N}, \leq) y (\mathbb{N}, \preceq) no son isomorfos. Supongamos que existe un isomorfismo $f : (\mathbb{N}, \leq) \rightarrow (\mathbb{N}, \preceq)$ y sea $A = f^{-1}(S_1)$. Entonces $A \subseteq (\mathbb{N}, \leq)$ es no vacío y por el Teorema 2.3.1, existe $a = \min A$. Luego, por el Teorema 2.5.15, $f(a)$ debe ser un mínimo de S_1 . Sin embargo, si $f(a) \in S_1$, $f(a) + 2$ también es un elemento de S_1 tal que $f(a) + 2 > f(a)$, y por lo tanto $f(a) + 2 \prec f(a)$, lo que contradice la definición de mínimo.

De manera similar puede probarse que no existe un anti-isomorfismo de (\mathbb{N}, \leq) en (\mathbb{N}, \preceq) . ■

2.6. El Axioma de Elección, el Lema de Zorn y el Principio de Buena Ordenación.

Como ya hemos mencionado en la Observación 2.2.12, hasta el momento podemos garantizar la existencia de elementos maximales o minimales sólo en conjuntos finitos. Para generalizar este resultado a conjuntos infinitos necesitamos introducir algunos conceptos más delicados ligados a la teoría axiomática de conjuntos. No desarrollaremos aquí estos temas en profundidad, sólo nos limitaremos a presentar algunos resultados básicos. Para una exposición completa del tema, pueden consultarse [5, 7, 11].

Establecer una teoría formal de conjuntos que evitara las paradojas que se producían a partir de la teoría inicial elaborada por Georg Cantor fue uno de los grandes desafíos de principios del siglo pasado. La teoría logra su formulación completa con los conocidos axiomas de Zermelo-Fraenkel (ZF). Esta teoría logra resolver las paradojas anteriores, pero omite un resultado que resulta crucial en matemática, el denominado *axioma de elección*. El sistema axiomático de Zermelo-Fraenkel junto al axioma de elección se conoce como sistema ZFC (la C hace referencia a la palabra *choice*, elección en inglés). El axioma de elección tiene muchas formulaciones equivalentes, entre ellas, el denominado *Lema de Zorn* y el *Principio de Buena Ordenación*. Las discutiremos a continuación.

Axioma de Elección. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos y disjuntos dos a dos. Entonces existe un conjunto D tal que $A_i \cap D = \{x_i\}$ para cada $i \in I$.

Observación 2.6.1. [5] *Es importante destacar el carácter puramente existencial del Axioma de Elección, pues a pesar de su nombre, no nos da ninguna regla para “elegir” un elemento de cada conjunto de la familia. B. Russell daba el siguiente ejemplo intuitivo para comprender mejor el sentido de este axioma: Supongamos que tuviésemos un conjunto infinito de pares de medias. El axioma nos asegura que existe un conjunto formado por exactamente una media de cada par. Si tuviésemos en cambio una infinidad de pares de zapatos, no necesitaríamos recurrir al Axioma de Elección para formar un conjunto con un zapato de cada par; pues bastaría que eligiéramos como elemento el zapato derecho (o el izquierdo) de cada par.*

Ejemplo 2.6.2. Supongamos que tenemos un conjunto A y $\mathcal{P} = \{A_i\}_{i \in I}$ una partición de A . Sea \sim la relación de equivalencia que se define a partir de \mathcal{P} , esto es, $x \sim y$ si y sólo si $x, y \in A_i$ para algún $i \in I$. El axioma de elección nos permite seleccionar un elemento $x_i \in A_i$ de cada conjunto de la partición. De esta manera, $A/\sim = \mathcal{P} = \{[x_i] : i \in I\}$, es decir, podemos describir la partición \mathcal{P} como clases de equivalencia eligiendo un representante de cada una. ■

Definición 2.6.3. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos. Se denomina una **función selectora** para esta familia es una función

$$f : I \rightarrow \bigcup_{i \in I} A_i$$

tal que $f(i) \in A_i$ para cada $i \in I$.

Lema 2.6.4. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos disjuntos dos a dos. Entonces existe una función selectora para esta familia.

Demostración. Sea D el conjunto cuya existencia garantiza el axioma de elección tal que $D \cap A_i = \{x_i\}$ para cada $i \in I$, y sea $f : I \rightarrow \bigcup_{i \in I} A_i$ tal que $f(i) = x_i$. Entonces f es una función selectora para $\{A_i\}_{i \in I}$. \square

Teorema 2.6.5. *Toda familia no vacía de conjuntos no vacíos admite una función selectora.*

Demostración. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos. Si los conjuntos fuesen disjuntos dos a dos, la existencia de una función selectora para esta familia está garantizada por el Lema 2.6.4.

Supongamos que $\{A_i\}_{i \in I}$ es una familia cualquiera. Para cada $i \in I$ sea

$$B_i = \{i\} \times A_i = \{(i, a) : a \in A_i\}.$$

Observemos que la familia $\{B_i\}_{i \in I}$ es una familia de conjuntos disjuntos dos a dos. En efecto, si existe $(k, a) \in B_i \cap B_j$, entonces $k = i = j$. Es decir, si $i \neq j$, $B_i \cap B_j = \emptyset$.

Por el Lema 2.6.4 existe una función selectora $\tilde{f} : I \rightarrow \bigcup_{i \in I} B_i$ tal que $\tilde{f}(i) \in B_i$, esto es, para cada $i \in I$, existe $x_i \in A_i$ tal que $\tilde{f}(i) = (i, x_i)$. Luego $f : I \rightarrow \bigcup_{i \in I} A_i$, $f(i) = x_i$ es una función selectora para la familia $\{A_i\}_{i \in I}$. \square

Corolario 2.6.6. *Sea A un conjunto no vacío. Entonces existe una función $f : \mathcal{P}(A) - \{\emptyset\} \rightarrow A$ tal que $f(B) \in B$ para cada $B \in \mathcal{P}(A) - \emptyset$.*

Demostración. Sea $I = \mathcal{P}(A) - \{\emptyset\}$ y para cada $B \in I$ (i.e., $B \subseteq A$, $B \neq \emptyset$) pongamos $A_B = B$. Entonces $\{A_B\}_{B \in I}$ es una familia no vacía de conjuntos no vacíos y $\bigcup_{B \in I} A_B = A$. Por el Teorema 2.6.5 existe una función $f : I \rightarrow A$ tal que $f(B) \in A_B = B$. \square

Nos dedicaremos ahora a probar el Lema de Zorn, que generaliza el Teorema 2.2.7 para conjuntos que no necesariamente son finitos.

Definición 2.6.7. *Sea (A, \preceq) un poset. Un subconjunto $X \subseteq A$ se dice una **cadena** si $(X, \preceq|_X)$ es un conjunto totalmente ordenado.*

Ejemplo 2.6.8. Para cualquier poset (A, \preceq) , \emptyset es una cadena (por vacuidad en la definición) y cualquier singulete $\{x\}$ es una cadena. Si (A, \preceq) está totalmente ordenado, cualquier subconjunto de A es una cadena. En particular, cualquier subconjunto de una cadena es una cadena. \blacksquare

Ejemplo 2.6.9. En $(\mathbb{N}, |)$ (que no es totalmente ordenado) el conjunto de las potencias de 2,

$$B = \{2^k : k \in \mathbb{N}_0\}$$

es una cadena. En efecto, dados $j, k \in \mathbb{N}_0$, se verifica $j \leq k$ o $k < j$. En el primer caso, $2^j \mid 2^k$ y en el segundo $2^k \mid 2^j$. Luego dos elementos cualesquiera de B son comparables, y por lo tanto B es totalmente ordenado. \blacksquare

Ejemplo 2.6.10. Consideremos el poset $(\mathcal{P}(\mathbb{N}), \subseteq)$ y para cada $n \in \mathbb{N}$ sea $I_n = \{1, 2, \dots, n\}$. Entonces $X = \{I_n : n \in \mathbb{N}\}$ es una cadena, dado que si $j \leq k$, entonces $I_j \subseteq I_k$. Más aún, se verifica que

$$I_1 \subset I_2 \subset \dots \subset I_n \subset I_{n+1} \subset \dots$$

Más generalmente, sea A un conjunto cualquiera y sea $\{A_n\}_{n \in \mathbb{N}}$ una familia de subconjuntos. Para cada $n \in \mathbb{N}$ sea $B_n = \bigcup_{i \leq n} A_i$. Entonces claramente $X = \{B_i : i \in \mathbb{N}\}$ es una cadena en $(\mathcal{P}(A), \subseteq)$. ■

Definición 2.6.11. Sea (A, \preceq) un poset y sea \mathcal{C} el conjunto de cadenas de A . Una cadena M de A se dice una cadena maximal si M es un elemento maximal del poset (\mathcal{C}, \subseteq) .

Ejemplo 2.6.12. Si (A, \preceq) es un conjunto totalmente ordenado, entonces el conjunto de cadenas de A es $\mathcal{C} = \mathcal{P}(A)$, y la única cadena maximal de A es $M = A$ (pues A es el único elemento maximal, y por lo tanto el máximo, de $(\mathcal{P}(A), \subseteq)$). ■

Lema 2.6.13. Sea (A, \preceq) un poset. Una cadena M de A es una cadena maximal si y sólo si para cada $x \in A - M$, $M \cup \{x\}$ no es una cadena.

Demostración. Si M es una cadena maximal de A , trivialmente $M \cup \{x\}$ no puede ser una cadena, pues $M \subsetneq M \cup \{x\}$. Supongamos entonces que M es una cadena de A tal que para cada $x \in A - M$, $M \cup \{x\}$ no es una cadena.

Sea X una cadena de A tal que $M \subseteq X$. Si $X \neq A$, entonces existe un elemento $x \in X - M \subset A - M$. Luego $M \cup \{x\}$ es un subconjunto de la cadena X , y por lo tanto es una cadena lo cual contradice la hipótesis. Concluimos que $X = M$ y por lo tanto M es maximal. □

Ejemplo 2.6.14. Consideremos la cadena $B = \{2^k : k \in \mathbb{N}\}$ de $(\mathbb{N}, |)$ dada en el Ejemplo 2.6.9. Veamos que B es una cadena maximal.

Sea $n \in \mathbb{N} - B$ cualquiera y supongamos que $B \cup \{n\}$ es una cadena. Sea $k \in \mathbb{N}$, entonces n y 2^k deben ser comparables. Supongamos que $n \mid 2^k$. Entonces m. c. d. $(n, 2^k) = n$, y por el Corolario 2.3.15 n debe ser una potencia de 2. Esto es $n \in B$, lo que no puede ocurrir. Luego deberá ser $2^k \mid n$. Sea k_0 el mayor natural tal que $2^{k_0} \mid n$ (observemos que k_0 siempre existe por el Teorema 2.2.11, dado que $K = \{k \in \mathbb{N} : 2^k \mid n\}$ es un subconjunto finito de (\mathbb{N}, \leq)). Luego $2^{k_0+1} \nmid n$, y por lo tanto deberá ser $n \mid 2^{k_0+1}$. Pero con el mismo razonamiento que antes, tendríamos que $n \in B$.

Luego $B \cup \{n\}$ no es una cadena, y por lo tanto B es maximal. ■

Teorema 2.6.15 (Principio de maximalidad de Hausdorff). *En todo poset (A, \preceq) existe una cadena maximal.*

Demostración. Sea \mathcal{C} el conjunto de cadenas de A . Para cada $X \in \mathcal{C}$, sea

$$X^* = \{x \in A - X : A \cup \{x\} \in \mathcal{C}\}$$

Observemos que por el Lema 2.6.13, X es una cadena maximal de A si y sólo si $X^* = \emptyset$.

Por el Corolario 2.6.6, existe una función $f : \mathcal{P}(A) - \{\emptyset\} \rightarrow A$ tal que $f(B) \in B$ para cada $B \subseteq A$, $B \neq \emptyset$. Definamos una nueva función $F : \mathcal{C} \rightarrow \mathcal{C}$ dada por

$$F(X) = \begin{cases} X \cup \{f(X^*)\} & \text{si } X^* \neq \emptyset \\ X & \text{si } X^* = \emptyset \end{cases}$$

Observemos que F está bien definida, pues si $X^* \neq \emptyset$, $f(X^*) \in X^*$, y por lo tanto $X \cup \{f(X^*)\}$ es una cadena de A . Es decir, F asigna a cada cadena X en A una nueva cadena $F(X)$ tal que $X \subsetneq F(X)$ si X no es maximal, y deja X invariante si X es una cadena maximal.

Una f -torre es un subconjunto $\mathcal{T} \subseteq \mathcal{C}$ (es decir, \mathcal{T} es un conjunto de cadenas de A) tal que:

- $\emptyset \in \mathcal{T}$,
- Si $X \in \mathcal{T}$, entonces $F(X) \in \mathcal{T}$,
- Si \mathcal{K} es una cadena en el poset (\mathcal{T}, \subseteq) , entonces $\bigcup_{K \in \mathcal{K}} K \in \mathcal{T}$.

Aclaremos este último punto: si \mathcal{K} es una colección de cadenas de A en \mathcal{T} tales que para cada $X, Y \in \mathcal{K}$, $X \subseteq Y$ o $Y \subseteq X$, entonces $\bigcup_{K \in \mathcal{K}} K$ es una cadena en A que pertenece a \mathcal{T} .

Sea \mathfrak{T} el conjunto de f -torres, ordenado por la relación de inclusión \subseteq y definamos

$$\mathcal{T}_0 = \bigcap_{\mathcal{T} \in \mathfrak{T}} \mathcal{T} = \bigcap \{\mathcal{T} \subseteq \mathcal{C} : \mathcal{T} \text{ es una } f\text{-torre}\}.$$

Es inmediato verificar (y lo dejamos como **ejercicio**) que \mathcal{T}_0 es una f -torre. Es decir, $\mathcal{T}_0 \in \mathfrak{T}$ y en consecuencia \mathcal{T}_0 es el mínimo de $(\mathfrak{T}, \subseteq)$ (observemos que $\mathcal{T}_0 \neq \emptyset$ pues $\emptyset \in \mathcal{T}_0$).

Mostraremos que $(\mathcal{T}_0, \subseteq)$ es un conjunto totalmente ordenado. Posterguemos la prueba por un momento, y veamos cómo concluir la tesis del teorema a partir de este hecho. Una vez que hayamos probado esto, tendremos que $(\mathcal{T}_0, \subseteq)$ es una cadena, y como $\mathcal{T}_0 \subseteq \mathcal{C}$ y \mathcal{T}_0 es una f -torre, entonces

$$M = \bigcup_{X \in \mathcal{T}_0} X \in \mathcal{T}_0.$$

Es decir, M es el elemento máximo de $(\mathcal{T}_0, \subseteq)$.

Por otra parte, M es una cadena de (A, \preceq) , pues $\mathcal{T}_0 \subseteq \mathcal{C}$. Supongamos que $M^* \neq \emptyset$. Entonces $M \subsetneq F(M)$, y como \mathcal{T}_0 es una f -torre, $F(M) \in \mathcal{T}_0$. Pero esto es absurdo, pues M es el máximo de $(\mathcal{T}_0, \subseteq)$. Concluimos que debe ser $M^* = \emptyset$ y por lo tanto M es una cadena maximal de (A, \preceq) .

Veamos entonces que $(\mathcal{T}_0, \subseteq)$ es totalmente ordenado. Sea $X \in \mathcal{T}_0$. Diremos que X es *comparable* si para cada $Y \in \mathcal{T}_0$, $X \subseteq Y$ o $Y \subseteq X$. Consideremos el conjunto \mathcal{F} de elementos comparables de \mathcal{T}_0 .

Para $X \in \mathcal{F}$, sea

$$\mathcal{T}_X = \underbrace{\{Y \in \mathcal{T}_0 : Y \subsetneq X\}}_{\mathcal{X}_1} \cup \{X\} \cup \underbrace{\{Y \in \mathcal{T}_0 : F(X) \subseteq Y\}}_{\mathcal{X}_2}.$$

Probaremos que \mathcal{T}_X es una f -torre. Trivialmente $\emptyset \in \mathcal{T}_X$, pues $\emptyset \in \mathcal{T}_0$ y $X = \emptyset$ o $\emptyset \subsetneq X$.

Sea $Y \in \mathcal{T}_X$ y veamos que $F(Y) \in \mathcal{T}_X$. Observemos que como $\mathcal{T}_X \subset \mathcal{T}_0$ y \mathcal{T}_0 es una f -torre, entonces $F(Y) \in \mathcal{T}_0$.

- Si $Y = X$, $F(X) = F(Y)$, o sea $F(Y) \in \mathcal{X}_2$.
- Si $Y \in \mathcal{X}_2$, entonces $F(X) \subseteq Y \subseteq F(Y)$, con lo cual $F(Y) \in \mathcal{X}_2$.
- Si $Y \in \mathcal{X}_1$, entonces existe $x_0 \in X$ tal que $x_0 \notin Y$. Como X es comparable, será $F(Y) \subseteq X$ o $X \subsetneq F(Y)$. En el primer caso, $F(Y) \in \mathcal{X}_1 \cup \{X\}$. Observemos que el segundo no puede ocurrir. En efecto, supongamos que $X \subsetneq F(Y)$. Como $Y \subsetneq X$, $F(Y) \neq Y$. Luego $Y^* \neq \emptyset$ y $F(Y) = Y \cup \{f(Y^*)\}$. Como $x_0 \in X$ y $x_0 \notin Y$, deberá ser $x_0 = f(Y^*)$, pero entonces $F(Y) \subseteq X$ en contra de lo que estamos suponiendo.

En cualquiera de los casos, concluimos que $F(Y) \in \mathcal{T}_X$.

Lo último que debemos probar para ver que \mathcal{T}_X es una f -torre es que si \mathcal{K} es una cadena en $(\mathcal{T}_X, \subseteq)$, entonces $Y = \bigcup_{K \in \mathcal{K}} K \in \mathcal{T}_X$. Para cada $K \in \mathcal{K}$ tendremos que $K \in \mathcal{X}_1 \cup \{X\}$, es decir, $K \subseteq X$, o $K \in \mathcal{X}_2$, es decir $F(X) \subseteq K$.

- Si $K \subseteq X$ para cada $K \in \mathcal{K}$, entonces $Y \subseteq X$ y por lo tanto $Y \in \mathcal{X}_1 \cup \{X\} \subseteq \mathcal{T}_X$.
- Supongamos entonces que existe $K_0 \in \mathcal{K}$ tal que $F(X) \subseteq K_0$. Entonces $f(X) \subseteq Y$ con lo cual $Y \in \mathcal{X}_2$.

Concluimos que $\mathcal{T}_X \in \mathfrak{T}$ y $\mathcal{T}_X \subset \mathcal{T}_0$. Como \mathcal{T}_0 es el mínimo de $(\mathfrak{T}, \subseteq)$ deberá ser $\mathcal{T}_X = \mathcal{T}_0$. En particular, tenemos que para cada $Y \in \mathcal{T}_0$, $Y \subseteq X \subseteq F(X)$ o $F(X) \subseteq Y$, con lo cual si $X \in \mathcal{F}$, entonces $F(X) \in \mathcal{F}$.

Veamos finalmente que \mathcal{F} es una f -torre. Claramente \emptyset es un elemento comparable de \mathcal{T}_0 , y hemos visto que si $X \in \mathcal{F}$, $F(X) \in \mathcal{F}$. Consideremos entonces una cadena \mathcal{K} en (\mathcal{F}, \subseteq) y sea $Y = \bigcup_{K \in \mathcal{K}} K$. Recordemos que todos los elementos de \mathcal{K} son elementos comparables de \mathcal{T}_0 . Sea $Z \in \mathcal{T}_0$ cualquiera.

- Si $K \subset Z$ para cada $K \in \mathcal{K}$, entonces $Y \subseteq Z$.
- Supongamos que existe $K_0 \in \mathcal{K}$ tal que $Z \subseteq K_0$, entonces trivialmente $Z \subseteq Y$.

Concluimos que $Y \in \mathcal{F}$ y por lo tanto \mathcal{F} es una f -torre. Como $\mathcal{F} \subseteq \mathcal{T}_0$ y \mathcal{T}_0 es el mínimo de $(\mathfrak{T}, \subseteq)$ debe ser $\mathcal{F} = \mathcal{T}_0$. Luego todos los elementos de \mathcal{T}_0 son comparables, y por lo tanto $(\mathcal{T}_0, \subseteq)$ es totalmente ordenado, como queríamos probar. \square

Teorema 2.6.16 (Lema de Zorn). *Sea (A, \preceq) un poset no vacío. Si toda cadena en A tiene una cota superior, entonces A tiene al menos un elemento maximal.*

Demostración. Por el Teorema 2.6.15 existe en (A, \preceq) una cadena maximal M . Por hipótesis, además, M tiene una cota superior, digamos $m \in A$. Es decir, $x \preceq m$ para cada $x \in M$. Observemos que entonces $M \cup \{m\}$ es una cadena. En efecto, si $x, y \in M$, entonces x e y son comparables, y si $x \in M$ y $y = m$, entonces $x \preceq y$. Como M es maximal, del Lema 2.6.13 deberá ser $m \in M$ y por lo tanto m es el máximo de M . Es decir, M tiene una única cota superior que es su máximo.

Si ahora $z \in A$ verifica $m \preceq z$, entonces para cada $x \in M$, $x \preceq m \preceq z$. Luego z es una cota superior de M y por lo tanto $z = m$. Concluimos que m es un elemento maximal de (A, \preceq) . \square

Para finalizar este capítulo el último de los resultados clásicos de la teoría de conjuntos ordenados, el *Principio de buena ordenación*.

Definición 2.6.17. Un poset no vacío (A, \preceq) se dice un **conjunto bien ordenado** si todo subconjunto no vacío B de A tiene un mínimo (denominado **primer elemento**). La relación \preceq se dice en este caso un **buen orden** en A .

Observación 2.6.18. Si $A \neq \emptyset$ y (A, \preceq) es un conjunto bien ordenado, entonces A debe tener un mínimo, dado que A es un subconjunto no vacío de sí mismo.

Ejemplo 2.6.19.

1. (\mathbb{R}, \leq) no es un conjunto bien ordenado. En efecto, basta considerar cualquier intervalo abierto (a, b) , que con el orden restringido no tiene un mínimo.
2. Por el Corolario 2.2.11, todo conjunto finito totalmente ordenado es bien ordenado.
3. Por el Principio del Buen Orden (Teorema 2.3.1), (\mathbb{N}, \leq) es bien ordenado.
4. $(\mathbb{N}, |)$ no es bien ordenado. Por ejemplo $B = \{2, 3\}$ no tiene mínimo, dado que el único elemento $x \in \mathbb{N}$ tal que $x \mid 2$ y $x \mid 3$ es $x = 1$ que no pertenece a B .
5. (\mathbb{N}, \preceq) , donde \preceq es el orden del Ejemplo 2.5.16, no es bien ordenado (hemos probado allí que el subconjunto S_1 de números impares no tiene mínimo). ■

Lema 2.6.20. Si (A, \preceq) es un conjunto bien ordenado, entonces \preceq es un orden total.

Demostración. Sean $x, y \in A$. Entonces $B = \{x, y\}$ es no vacío y por lo tanto tendrá un mínimo, que deberá ser x o y . Se debe verificar entonces $x \preceq y$ o $y \preceq x$, con lo cual x e y son comparables. □

Teorema 2.6.21 (Principio de buena ordenación). *Todo conjunto no vacío A admite una relación de orden \preceq tal que (A, \preceq) es un conjunto bien ordenado.*

Demostración. Supongamos primero que A es un conjunto finito. Entonces si $n = |A|$, existe una biyección $f : \{1, \dots, n\} \rightarrow A$. Definamos la relación \preceq en A por

$$a \preceq b \text{ si y sólo si } f^{-1}(a) \leq f^{-1}(b),$$

donde \leq es el orden usual en \mathbb{N} . Dejamos como **ejercicio** verificar que \preceq es una relación de orden en A , y por el Lema 2.5.6 f^{-1} , y por lo tanto f , es un isomorfismo de posets. Como $(\{1, \dots, n\}, \leq)$ es totalmente ordenado, del Teorema 2.5.13 resulta (A, \preceq) totalmente ordenado. Luego cualquier subconjunto no vacío de (A, \preceq) es finito y totalmente ordenado y por el Corolario 2.2.11 tiene un mínimo. Concluimos que (A, \preceq) es bien ordenado.

Supongamos ahora que A es un conjunto cualquiera y consideremos el conjunto

$$\mathcal{W} = \{(X, \mathcal{R}_X) : X \in \mathcal{P}(A), \mathcal{R}_X \subset X \times X \text{ es un buen orden en } X\}.$$

El conjunto \mathcal{W} es no vacío dado que, por lo que acabamos de ver, todo subconjunto finito de X puede ser bien ordenado. Definimos la relación \preceq en \mathcal{W} poniendo

$$(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y) \iff \begin{cases} X \subseteq Y \\ (\mathcal{R}_Y)_{|X} = \mathcal{R}_X \\ \text{si } x \in X, y \in Y - X, \text{ entonces } x \mathcal{R}_Y y. \end{cases}$$

Veamos que \preceq es una relación de orden en \mathcal{W} . \preceq es trivialmente reflexiva. Veamos que es antisimétrica. Supongamos que $(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y)$ y que $(Y, \mathcal{R}_Y) \preceq (X, \mathcal{R}_X)$. Entonces $X = Y$ (dado que $X \subseteq Y$ y $Y \subseteq X$) y por lo tanto

$$\mathcal{R}_Y = (\mathcal{R}_Y)_{|Y} = (\mathcal{R}_Y)_{|X} = \mathcal{R}_X.$$

Concluimos que $(X, \mathcal{R}_X) = (Y, \mathcal{R}_Y)$.

Vamos finalmente que \preceq es transitiva. Sean $(X, \mathcal{R}_X), (Y, \mathcal{R}_Y), (Z, \mathcal{R}_Z) \in \mathcal{W}$ tales que

$$(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y) \text{ y } (Y, \mathcal{R}_Y) \preceq (Z, \mathcal{R}_Z).$$

Entonces en primer lugar tendremos que $X \subseteq Y$ y $Y \subseteq Z$, de donde $X \subseteq Z$. Además, $(\mathcal{R}_Z)_{|Y} = \mathcal{R}_Y$ y $(\mathcal{R}_Y)_{|X} = \mathcal{R}_X$. Luego, del Ejercicio 9 del Capítulo 1, resulta

$$(\mathcal{R}_Z)_{|X} = ((\mathcal{R}_Z)_{|Y})_{|X} = (\mathcal{R}_Y)_{|X} = \mathcal{R}_X.$$

Finalmente, sean $x \in X$ y $z \in Z - X$. Como $X \subseteq Y \subseteq Z$, en particular $x \in Y$ y existen dos opciones, $z \in Y$ o $z \in Z - Y$. Si $z \in Y$, entonces $x \in X$ y $z \in Y - X$ con lo cual $x \mathcal{R}_Y z$. Pero como $\mathcal{R}_Y = (\mathcal{R}_Z)_{|Y}$, tendremos $x \mathcal{R}_Z z$. Si $z \in Z - Y$, entonces $x \in Y$ y $z \in Z - Y$ de donde $x \mathcal{R}_Z z$. Concluimos entonces que $(X, \mathcal{R}_X) \preceq (Z, \mathcal{R}_Z)$.

Sea \mathcal{X} una cadena en (\mathcal{W}, \preceq) y veamos que \mathcal{X} es acotado superiormente. Pongamos

$$U = \bigcup_{(X, \mathcal{R}_X) \in \mathcal{X}} X$$

y definamos la relación \mathcal{R}_U en U como sigue: dados $s, t \in U$,

$$s \mathcal{R}_U t \iff \text{existe } (X, \mathcal{R}_X) \in \mathcal{X} \text{ tal que } s, t \in X \text{ y } s \mathcal{R}_X t.$$

Observemos que \mathcal{R}_U está bien definida. Esto es, si existen $(X, \mathcal{R}_X) \in \mathcal{X}$ y $(Y, \mathcal{R}_Y) \in \mathcal{X}$ tales que $s, t \in X \cap Y$, entonces

$$s \mathcal{R}_X t \iff s \mathcal{R}_Y t.$$

En efecto, supongamos que $s, y \in X \cap Y$ y $s \mathcal{R}_X t$. Como \mathcal{X} es una cadena, tendremos que $(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y)$ o $(Y, \mathcal{R}_Y) \preceq (X, \mathcal{R}_X)$. En el primer caso, $X \subseteq Y$ y $\mathcal{R}_X = (\mathcal{R}_Y)_{|X}$. Luego $s (\mathcal{R}_Y)_{|X} t$, con lo cual $s \mathcal{R}_Y t$. En el segundo caso, $Y \subseteq X$ y $\mathcal{R}_Y = (\mathcal{R}_X)_{|Y}$. Como $s, y \in Y$ y $s \mathcal{R}_X t$, resulta trivialmente $s \mathcal{R}_Y t$. La otra implicación es análoga.

Luego \mathcal{R}_U es una relación bien definida en U , y al ser \mathcal{X} una cadena no es difícil ver que \mathcal{R}_U es una relación de orden en U (dejamos los detalles como **ejercicio**).

Veamos finalmente que $(U, \mathcal{R}_U) \in \mathcal{W}$, es decir, \mathcal{R}_U es un buen orden en U . Sea $T \subset U$ un subconjunto no vacío. Tomemos $t \in T$ cualquiera, y sea $(X, \mathcal{R}_X) \in \mathcal{X}$ tal que $t \in X$. Entonces en particular $T \cap X$ es un subconjunto no vacío de (X, \mathcal{R}_X) y por lo tanto tiene un mínimo, digamos m_X .

Supongamos que ahora $(Y, \mathcal{R}_Y) \in \mathcal{X}$ es tal que $T \cap Y$ es no vacío y sea m_Y el mínimo de $T \cap Y$ para la relación \mathcal{R}_Y .

Nuevamente, como \mathcal{X} es una cadena, (X, \mathcal{R}_X) e (Y, \mathcal{R}_Y) son comparables. Supongamos sin pérdida de generalidad que $(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y)$. Entonces $X \subseteq Y$, $\mathcal{R}_X = (\mathcal{R}_Y)|_X$ y para cada $x \in X$ e $y \in Y - X$ resulta $x \mathcal{R}_Y y$. En particular, $T \cap X \subseteq T \cap Y$, y Ejercicio 9 del Capítulo 1, tenemos

$$(\mathcal{R}_X)|_{T \cap X} = ((\mathcal{R}_Y)|_X)|_{T \cap X} = (\mathcal{R}_Y)|_{T \cap X}$$

y por lo tanto, del Ejercicio 5 de este capítulo resulta

$$m_Y \mathcal{R}_Y m_X.$$

Si $m_Y \in T \cap X$, deberá ser $m_Y = m_X$, pues $m_X = \min T \cap X$. Si $m_Y \notin T \cap X$, como $m_Y \in T \cap Y$, tendremos que $m_X \in X$ y $m_Y \in Y - X$, con lo cual debe ser $m_X \mathcal{R}_Y m_Y$. Pero esto es absurdo, pues entonces $m_X = m_Y$ y $m_Y \in X$ en contra de lo que estamos suponiendo.

En conclusión, si (X, \mathcal{R}_X) e (Y, \mathcal{R}_Y) son elementos de \mathcal{X} tales que $T \cap X \neq \emptyset$ y $T \cap Y \neq \emptyset$, entonces

$$m_X = \min(T \cap X, \mathcal{R}_X) = \min(T \cap Y, \mathcal{R}_Y) = m_Y.$$

Pongamos entonces m este mínimo común de $(T \cap X, \mathcal{R}_X)$ cualquiera sea $(X, \mathcal{R}_X) \in \mathcal{X}$. Si ahora $s \in T \subseteq U$ es un elemento cualquiera, existirá Z tal que $(Z, \mathcal{R}_Z) \in \mathcal{X}$ y $s \in Z$. Luego $m, s \in Z$ y como $m = \min(T \cap Z, \mathcal{R}_Z)$, resulta $m \mathcal{R}_Z s$, con lo cual $m \mathcal{R}_U s$. Concluimos que $m = \min(T, (\mathcal{R}_U)|_T)$. Como T es un subconjunto no vacío arbitrario de U resulta que (U, \mathcal{R}_U) es bien ordenado, es decir, $(U, \mathcal{R}_U) \in \mathcal{X}$ como queríamos ver.

Ahora bien, si (X, \mathcal{R}_X) es un elemento cualquiera de \mathcal{X} , claramente $X \subseteq U$ y por cómo está definida \mathcal{R}_U se tiene $(\mathcal{R}_U)|_X = \mathcal{R}_X$. Supongamos que $x \in X$ e $y \in U - X$. Sea $(Y, \mathcal{R}_Y) \in \mathcal{X}$ tal que $y \in Y$. Como (X, \mathcal{R}_X) e (Y, \mathcal{R}_Y) son comparables, pero $y \in Y - X$, deberá ser $(X, \mathcal{R}_X) \preceq (Y, \mathcal{R}_Y)$. Luego $x \in X$, $y \in Y - X$, entonces $x, y \in Y$ y $x \mathcal{R}_Y y$. Por lo tanto $x \mathcal{R}_U y$, de donde $(X, \mathcal{R}_X) \preceq (U, \mathcal{R}_U)$. Concluimos entonces que (U, \mathcal{R}_U) es una cota superior de \mathcal{X} .

Hemos probado hasta aquí que toda cadena \mathcal{X} en (\mathcal{W}, \preceq) tiene una cota superior. Aplicando el Lema de Zorn (Teorema 2.6.16) resulta que (\mathcal{W}, \preceq) tiene un elemento maximal, digamos (M, \mathcal{R}_M) . Supongamos que $M \subsetneq A$ y sea entonces $a \in A$ tal que $a \notin M$.

Pongamos $\tilde{M} = M \cup \{a\}$ y $\mathcal{R}_{\tilde{M}}$ la relación en \tilde{M} tal que $(\mathcal{R}_{\tilde{M}})|_M = \mathcal{R}_M$ y $x \mathcal{R}_{\tilde{M}} a$ para cada $x \in M$. Como \mathcal{R}_M es un buen orden en M , es inmediato que $\mathcal{R}_{\tilde{M}}$ es un buen orden en \tilde{M} . Luego $(\tilde{M}, \mathcal{R}_{\tilde{M}}) \in \mathcal{W}$, pero por cómo definimos $\mathcal{R}_{\tilde{M}}$, resulta $(M, \mathcal{R}_M) \preceq (\tilde{M}, \mathcal{R}_{\tilde{M}})$ lo que contradice la maximalidad de (M, \mathcal{R}_M) .

Luego debe ser $M = A$ y por lo tanto \mathcal{R}_M es un buen orden en A . \square

Hasta aquí hemos enunciado una serie de resultados que resumimos a continuación:

- (**AE**) Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos y disjuntos dos a dos. Entonces existe un conjunto D tal que $A_i \cap D = \{x_i\}$ para cada $i \in I$.
- (**AE'**) Toda familia no vacía de conjuntos no vacíos admite una función selectora.
- (**AE''**) Sea A un conjunto no vacío. Entonces existe una función $f : \mathcal{P}(A) - \{\emptyset\} \rightarrow A$ tal que $f(B) \in B$ para cada $B \in \mathcal{P}(A) - \emptyset$.
- (**PMH**) En todo poset (A, \preceq) existe una cadena maximal.
- (**LZ**) Sea (A, \preceq) un poset no vacío. Si toda cadena en A tiene una cota superior, entonces A tiene al menos un elemento maximal.
- (**PBO**) Todo conjunto no vacío A admite una relación de orden \preceq tal que (A, \preceq) es un conjunto bien ordenado.

Si analizamos las demostraciones de los siguientes resultados, podemos observar que para probar cada uno de ellos hemos utilizado sólo el resultado anterior. Es decir, probamos que:

$$(\mathbf{AE}) \implies (\mathbf{AE}') \implies (\mathbf{AE}'') \implies (\mathbf{PMH}) \implies (\mathbf{LZ}) \implies (\mathbf{PBO}).$$

Como hemos adelantado en la introducción a esta sección, probaremos a continuación que todos estos enunciados son equivalentes dos a dos. Es decir, el axioma de elección puede ser substituido por cualquiera de ellos en la Teoría Axiomática ZFC. Para ello sólo debemos “cerrar el círculo”, probando que (**PBO**) implica (**AE**)

Teorema 2.6.22. *El Principio de Buena Ordenación implica el Axioma de Elección.*

Demostración. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos no vacíos y disjuntos dos a dos y sea $A = \bigcup_{i \in I} A_i$. Por el Teorema 2.6.21, existe un buen orden \preceq en A . Como cada A_i es un subconjunto no vacío de A , existe $m_i = \min(A_i, \preceq)$ para cada $i \in I$. Sea $D = \{m_i\}_{i \in I}$. Observemos que si $i \neq j$, $m_i \in A_i$ pero $m_i \notin A_j$, dado que $A_i \cap A_j = \emptyset$. Por lo tanto $D \cap A_i = \{m_i\}$ como queríamos probar. \square

El Axioma de Elección, o cualquiera de sus formulaciones equivalentes, resultan fundamentales para probar resultados profundos en matemática. Por ejemplo, a partir del Lema de Zorn puede probarse que un espacio vectorial siempre tiene una base. Muchas de estas aplicaciones pueden consultarse en [21]. Para finalizar este capítulo presentaremos sólo una de estas aplicaciones, el *Principio de Inducción Transfinita*.

Definición 2.6.23. *Sea (A, \preceq) un poset y sea $a \in A$. Se denomina **sección inicial** determinada por a al conjunto*

$$A_a = \{x \in A : x \prec a\}.$$

Teorema 2.6.24 (Principio de Inducción Transfinita). Sea (A, \preceq) un conjunto bien ordenado. Si $B \subseteq A$ es un subconjunto de A que satisface la siguiente propiedad:

$$(P) \quad \text{Para todo } x \in A, \text{ si } A_x \subseteq B \text{ entonces } x \in B$$

entonces $B = A$.

Demostración. Supongamos por el absurdo que existe $B \subseteq A$ que satisface (P) pero $B \neq A$. Entonces $S = A - B \neq \emptyset$ y como (A, \preceq) es bien ordenado, S tiene un mínimo m . Vemos que $A_m \subseteq B$. En efecto, si $m = \min A$, entonces $A_m = \emptyset \subset B$. Supongamos entonces que $m \neq \min A$, y por lo tanto $A_m \neq \emptyset$. Sea $x \in A_m$, es decir, $x \prec m$. Luego $x \notin S$, pues de lo contrario x sería un elemento de S tal que $x \prec m = \min S$. Luego $x \in A - S = B$. Como $x \in A_m$ es arbitrario, concluimos que $A_m \subseteq B$.

Como B satisface (P), deberá ser $m \in B$. Pero esto es absurdo pues $m \in S = A - B$. El absurdo proviene de suponer que $B \neq A$, y por lo tanto $B = A$. \square

2.7. Ejercicios

1. Sea (A, \preceq) un conjunto ordenado y sean $a_1, a_2, a_3 \in A$ tales que $a_1 \preceq a_2$ y $a_2 \prec a_3$. Probar que entonces $a_1 \prec a_3$. Probar que vale un resultado análogo si $a_1 \prec a_2$ y $a_2 \preceq a_3$, o si $a_1 \prec a_2$ y $a_2 \prec a_3$.
2. Probar que si (A, \preceq_A) y (B, \preceq_B) son conjuntos parcialmente ordenados, entonces $(A \times B, \preceq_{lex})$ es un conjunto parcialmente ordenado. Probar que si A y B son totalmente ordenados, entonces \preceq_{lex} es un orden total en $A \times B$.
3. Sean $(\{0, 1\}, \leq)$ y $(\mathcal{P}(\{0, 1\}), \subseteq)$. Hallar los diagramas de Hasse del orden producto y del orden lexicográfico para estos conjuntos ordenados.
4. Sean (A, \preceq_1) y (A, \preceq_2) posets. Determinar si las siguientes relaciones determinan un orden parcial en A :

$$a) \preceq_1 \cup \preceq_2.$$

$$b) \preceq_1 \cap \preceq_2.$$

$$c) \preceq_1 \circ \preceq_2$$

5. Sea (A, \preceq) un poset y sean $X \subseteq Y \subseteq A$. Supongamos que existen $m_X = \min X$, $m_Y = \min Y$, $M_X = \max X$ y $M_Y = \max Y$.
 - a) Probar que $m_Y \preceq m_X$ y $M_X \preceq M_Y$.
 - b) Si X tiene elementos maximales o minimales, ¿Existe alguna relación entre estos y los elementos correspondientes de Y ?
6. Sea (A, \preceq) un poset. Un subconjunto $B \subset A$ se denomina una **anticadena** si para cada $x, y \in B$ se verifica que

$$x \preceq y \implies x = y.$$

Probar que el conjunto de todos los elementos maximales (resp. minimales) de un conjunto ordenado, es una anticadena.

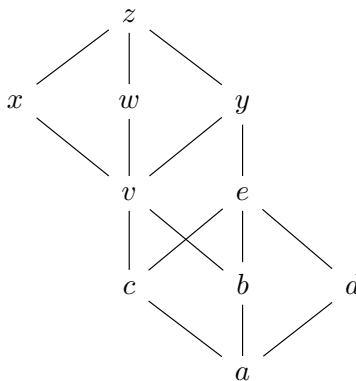
7. Demostrar el Corolario 2.2.11.

8. Si $a \in \mathbb{N}$ y $b \in \mathbb{Z}$, pongamos $r_a(b)$ el resto de dividir b por a . Sean $x_1, \dots, x_n \in \mathbb{Z}$ y $r_i = r_a(x_i)$ para cada $i = 1, \dots, n$. Probar que
- $r_a(x_1 + x_2 + \dots + x_n) = r_a(r_1 + r_2 + \dots + r_n)$. En particular, si y_1, \dots, y_n son enteros tales que $r_a(x_j) = r_a(y_j)$ para cada $j = 1, \dots, n$, entonces $r_a(\sum_{j=1}^n x_j) = r_a(\sum_{j=1}^n y_j)$.
 - $r_a(x_1 x_2 \dots x_n) = r_a(r_1 r_2 \dots r_n)$. En particular, si y_1, \dots, y_n son enteros tales que $r_a(x_j) = r_a(y_j)$ para cada $j = 1, \dots, n$, entonces $r_a(x_1 \dots x_n) = r_a(y_1 \dots y_n)$.
 - $r_a(x_1^n) = r_a(r_1^n)$ para cada $n \in \mathbb{N}$.
9. Sean b_1, b_2, \dots, b_n números enteros. Una *combinación lineal entera* de b_1, \dots, b_n es un número entero b para el cual existen enteros x_1, \dots, x_n tales que

$$b = b_1 x_1 + b_2 x_2 + \dots + b_n x_n.$$

Sean $a \in \mathbb{N}$, $b_1, b_2, \dots, b_n \in \mathbb{Z}$ con $a \neq 0$. Probar que si a divide a los enteros b_1, \dots, b_n , entonces a divide a cualquier combinación lineal entera de ellos.

10. Si $x, y \in \mathbb{N}$ pongamos $c_x(y)$ al cociente de dividir y por x . Sean $a, b, c \in \mathbb{N}$. Probar que
- Si $d = \text{m.c.d.}(a, b)$, entonces $c_d(a)$ y $c_d(b)$ son coprimos.
 - Si a y b son coprimos y $a \mid bc$, entonces $a \mid c$.
 - Si $a, b \in \text{Div}(n)$ para algún número natural n entonces $c_{\text{m.c.m.}(a,b)}(n) = \text{m.c.d.}(c_a(n), c_b(n))$ y $c_{\text{m.c.d.}(a,b)}(n) = \text{m.c.m.}(c_a(n), c_b(n))$.
11. Probar que 3515625 y 369754 son coprimos y escribir a 1 como combinación lineal entera de ellos.
12. Sean p y q números primos distintos. Probar que para cada $j, k \in \mathbb{N}$, p^j y q^k son coprimos.
13. Sean $a, b \in \mathbb{N}$. Probar que $ab = \text{m.c.m.}(a, b) \text{m.c.d.}(a, b)$.
14. Sea $A = \{a, b, c, d, e, v, w, x, y, z\}$ y sea \preceq el orden parcial en A cuyo diagrama de Hasse es el siguiente:



Determinar, si existen,

- | | | | |
|-------------------|-------------------|-------------------|-------------------|
| a) $\inf\{b, c\}$ | c) $\inf\{e, x\}$ | e) $\sup\{c, b\}$ | g) $\sup\{c, e\}$ |
| b) $\inf\{b, w\}$ | d) $\inf\{b, e\}$ | f) $\sup\{d, x\}$ | h) $\sup\{a, v\}$ |

15. Decimos que un poset (A, \preceq) satisface el **axioma del supremo** si todo subconjunto no vacío de A acotado superiormente tiene un supremo.
- a) Mostrar que $(\mathcal{P}(X), \subseteq)$ satisface el axioma del supremo.
- b) ¿El axioma del supremo es una propiedad hereditaria? Es decir, si (A, \preceq) es un poset que satisface el axioma del supremo y $B \subseteq A$, ¿ $(B, \preceq|_{B \times B})$ también lo satisface?
- c) Decimos que un poset (A, \preceq) satisface el **axioma del ínfimo** si todo subconjunto no vacío de A acotado inferiormente tiene ínfimo. Probar que (A, \preceq) satisface el axioma del supremo si y solo si (A, \preceq) satisface el axioma del ínfimo.
16. Demostrar el Teorema 2.4.10.
17. Probar que $(\mathcal{P}(\{0\}) \times \mathcal{P}(\{1, \dots, n\}), \preceq_{\text{prod}})$ y $(\mathcal{P}(\{0, \dots, n\}), \subseteq)$ son posets isomorfos.
18. Demostrar el Corolario 2.5.9.
19. Sea (A, \preceq) poset. Para todo $a \in A$ se define:

$$A_a := \{x \in A : x \leq a\}$$

Sea $\mathcal{A} = \{A_a : a \in A\}$, mostrar que $(\mathcal{A}, \subseteq) \simeq (A, \preceq)$.

20. Sean (X, \preceq_X) y (Y, \preceq_Y) posets. Una conexión de Galois es un par de funciones (f, g) con $f : X \rightarrow Y$ y $g : Y \rightarrow X$ tales que:

$$f(x) \preceq_Y y \iff x \preceq_X g(y) \quad \forall x \in X, y \in Y.$$

- a) Probar que todo isomorfismo de orden f induce una conexión de Galois (f, f^{-1}) .
- b) Dada una función $f : A \rightarrow B$, probar que se puede construir una conexión de Galois entre $\mathcal{P}(A)$ y $\mathcal{P}(B)$ utilizando los operadores que calculan la imagen de f sobre un subconjunto de A y la imagen inversa de f sobre un subconjunto de B .
- c) Encontrar una conexión de Galois (i, g) entre (\mathbb{N}, \leq) y (\mathbb{Q}_0^+, \leq) , donde i es la inclusión.
- d) Dada una conexión de Galois (f, g) entre (X, \preceq_X) y (Y, \preceq_Y) , probar que
- $$x \preceq_X g(f(x)) \quad \text{y} \quad f(g(y)) \preceq_Y y$$
- para todo $x \in X, y \in Y$.
- e) Dada una conexión de Galois (f, g) entre (X, \preceq_X) y (Y, \preceq_Y) , probar que f y g son morfismos de orden.
21. Sean $X = \{3^k : k \in \mathbb{N}\}$ y $Y = \{10^k : k \in \mathbb{N}\}$. Probar que X es una cadena maximal de $(\mathbb{N}, |)$ pero Y no lo es. ¿Para qué números naturales $m \in \mathbb{N}$ se verifica que $X_m = \{m^k : k \in \mathbb{N}\}$ es una cadena maximal de $(\mathbb{N}, |)$?

22. Sea (A, \preceq) un poset. Probar que si toda cadena en A está acotada inferiormente, entonces A posee al menos un elemento minimal.
23. Probar el Teorema 2.2.7 aplicando el Lema de Zorn.
24. Sean (A, \preceq_A) y (B, \preceq_B) posets y $f : A \rightarrow B$ un isomorfismo de posets. Probar que:
- a) $X \subseteq A$ es una cadena si y sólo si $f(X) \subseteq B$ es una cadena.

- b) (A, \preceq_A) es bien ordenado si y sólo si (B, \preceq_B) es bien ordenado.
25. Probar sin usar el Axioma de Elección o sus enunciados equivalentes que todo conjunto numerable admite un buen orden (recordar que X es numerable si X es finito o existe una función biyectiva $f : \mathbb{N} \rightarrow X$).
26. Sea (A, \preceq) un conjunto bien ordenado. Dado $x \in A$, se define el *sucesor* de x (si existe) por $s(x) = \min\{y \in A : x \prec y\}$.
- a) Probar que para cada $x \in A$ tal que $x \neq \max A$ (en caso que este último existiese), existe $s(x)$.
- b) Probar que para cada $x, y \in A$, si $s(x) = s(y)$ entonces $x = y$.
27. Sea (A, \preceq) un conjunto bien ordenado y $\phi(x)$ un predicado definido sobre A . Supongamos que ϕ verifica que para cada $x \in A$,
- (I) si $\phi(y)$ es verdadero para cada $y \prec x$, entonces $\phi(x)$ es verdadero.
- Probar que $\phi(x)$ es verdadera para cada $x \in A$.

Retículos

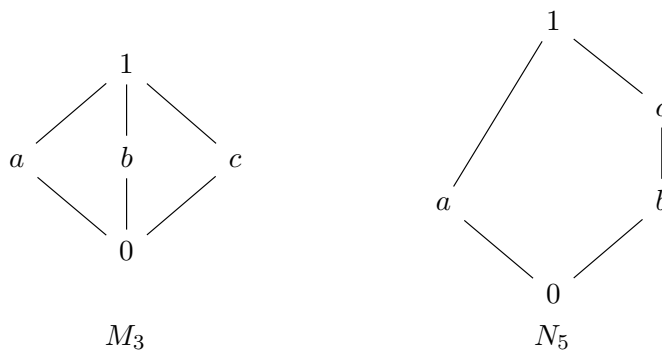
3.1. Definición y primeros ejemplos

En este capítulo estudiaremos un tipo particular de conjuntos ordenados, denominados *retículos*. La mayoría de los temas que presentaremos aquí pueden ampliarse consultando [6]

Definición 3.1.1. Un conjunto parcialmente ordenado (L, \preceq) se denomina un **retículo** (también llamado **reticulado** o **lattice**) si para cada $x, y \in L$, el conjunto $\{x, y\}$ posee ínfimo y supremo.

Ejemplo 3.1.2. Si (A, \preceq) es un conjunto totalmente ordenado. Entonces (A, \preceq) es trivialmente un retículo dado que el ínfimo y el supremo de $\{x, y\}$ son x o y y son además mínimo y máximo de $\{x, y\}$. En particular, cualquier subconjunto de \mathbb{R} con las relaciones \leq o \geq es un retículo.

Ejemplo 3.1.3. Retículos M_3 y N_5 . Consideremos los posets M_3 y N_5 cuyos diagramas de Hasse son los siguientes:



En M_3 , tenemos

$$\inf\{0, x\} = 0, \quad \sup\{0, x\} = x, \quad \inf\{1, x\} = x, \quad \sup\{1, x\} = 1$$

cualquiera sea $x \in M_3$ y además

$$\inf\{a, b\} = \inf\{a, c\} = \inf\{b, c\} = 0, \quad \sup\{a, b\} = \sup\{a, c\} = \sup\{b, c\} = 1.$$

En N_5 , resulta

$$\inf\{0, x\} = 0, \quad \sup\{0, x\} = x, \quad \inf\{1, x\} = x, \quad \sup\{1, x\} = 1$$

cualquiera sea $x \in N_5$ y además

$$\inf\{a, b\} = \inf\{a, c\} = 0, \quad \inf\{b, c\} = b, \quad \sup\{a, b\} = \sup\{a, c\} = 1, \quad \sup\{b, c\} = c.$$

Estos retículos son particularmente importantes, como veremos más adelante. ■

Ejemplo 3.1.4. Sea $X \neq \emptyset$. Entonces $(\mathcal{P}(X), \subseteq)$ es un retículo. En efecto, sean $C, D \subseteq X$ y sea $I = C \cap D$. Entonces I es una cota inferior de $\{C, D\}$ (pues $I \subseteq C$ y $I \subseteq D$) y si $B \subset X$ es una cota inferior de $\{C, D\}$, entonces $B \subseteq C$ y $B \subseteq D$, con lo cual $B \subseteq C \cap D = I$. Luego $I = \inf\{C, D\}$. De manera similar se prueba que $U = C \cup D = \sup\{C, D\}$. ■

Ejemplo 3.1.5. Consideremos el poset $(\mathbb{N}, |)$. Vimos en el Ejemplo 2.4.7 del Capítulo 2 que todo subconjunto finito no vacío de $(\mathbb{N}, |)$ tiene un ínfimo y un supremo, el máximo común divisor y el mínimo común múltiplo de sus elementos respectivamente. Por lo tanto $(\mathbb{N}, |)$ es un retículo. ■

Observación 3.1.6. *Observemos que **NO todo subconjunto de un retículo (con el orden restringido) es un retículo.** Por ejemplo si tomamos el subconjunto $P \subseteq \mathbb{N}$ de los números primos entonces $(P, |)$ no es un retículo. Más aún ningún subconjunto $\{x, y\} \subseteq P$ con $x \neq y$ tiene ínfimo ni supremo.*

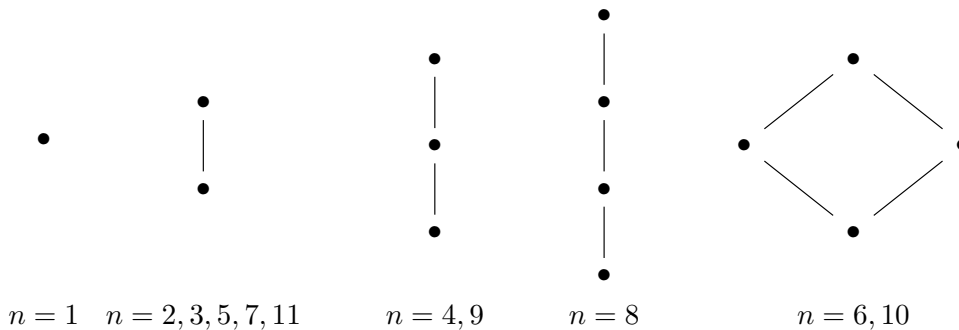
Ejemplo 3.1.7. El retículo D_n de divisores de n Fijemos $n \in \mathbb{N}$ y sea D_n el conjunto de divisores de n , esto es,

$$D_n = \{m \in \mathbb{N} : m \mid n\}.$$

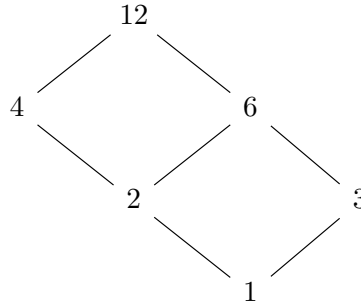
Observemos que si $m \in D_n$ y $k \in \mathbb{N}$ divide a m , entonces $k \mid n$. Luego $k \in D_n$. Por lo tanto si $m_1, m_2 \in D_n$, como $\text{mcd}(m_1, m_2)$ (donde mcd representa el máximo común divisor) divide a ambos, $\text{mcd}(m_1, m_2) \in D_n$ y por lo tanto existe (en D_n) el ínfimo $\inf\{m_1, m_2\} = \text{mcd}(m_1, m_2)$.

Por otra parte, si $m_1, m_2 \in D_n$, entonces n es un múltiplo común de m_1 y m_2 . Luego n es divisible por el mínimo común múltiplo de ambos (que denotamos $\text{mcm}(m_1, m_2)$). Es decir, $\text{mcm}(m_1, m_2) \in D_n$ y por lo tanto existe (en D_n) el supremo $\sup\{m_1, m_2\} = \text{mcm}(m_1, m_2)$. Concluimos que $(D_n, |)$ es un retículo.

Para los primeros 11 números naturales, los diagramas de Hasse de $(D_n, |)$ tienen alguna de las siguientes formas:

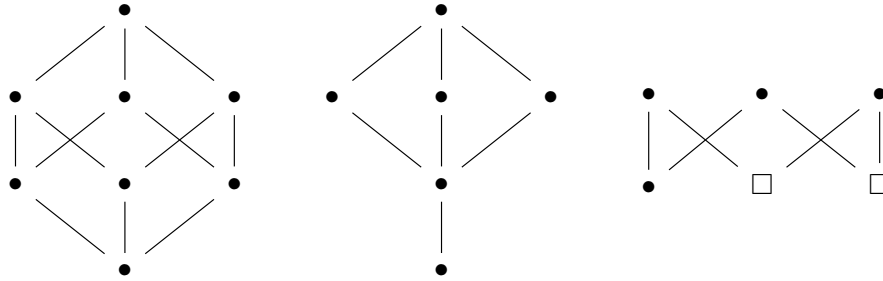


Observemos que el segundo diagrama (de izquierda a derecha) representa $(D_p, |)$ para cualquier número primo p . El diagrama de Hasse para D_{12} es



■

Ejemplo 3.1.8. Es fácil comprobar que los siguientes diagramas de Hasse, los dos primeros corresponden a retículos (¿Qué posets representan?).



El tercero no corresponde a un retículo, pues por ejemplo el conjunto formado por los elementos cuyos nodos están representados por cuadrados tiene supremo pero no tiene ínfimo. ■

El siguiente resultado es inmediato del Principio de Dualidad que presentamos en el Capítulo 2 (cf. Teorema 2.4.10). Dejamos los detalles de la prueba como **ejercicio**.

Lema 3.1.9. Sea (L, \preceq) un poset. Entonces (L, \preceq) es un retículo si y sólo si (L, \succeq) es un retículo.

Definición 3.1.10. Si (L, \preceq) es un retículo, entonces (L, \succeq) se denomina **retículo dual** de (L, \preceq) . Cuando la relación se da por conocida y denotamos al retículo directamente por L , su dual suele denotarse por L^* .

Lema 3.1.11 (Retículo producto). Sean (L, \preceq) y (L', \preceq') retículos. Entonces el poset $(L \times L', \preceq_{\text{prod}})$ con el orden producto es un retículo.

Demostración. Sean (x, x') y (y, y') en $L \times L'$ y sean $a = \sup\{x, y\}$ y $a' = \sup\{x', y'\}$. Entonces es claro que $(x, x') \preceq_{\text{prod}} (a, a')$ y $(y, y') \preceq_{\text{prod}} (a, a')$, con lo cual (a, a') es una cota superior de $\{(x, x'), (y, y')\}$. Si (c, c') es otra cota superior de $\{(x, x'), (y, y')\}$ entonces

$$(x, x') \preceq_{\text{prod}} (c, c') \implies x \preceq c, x' \preceq' c'.$$

De manera análoga, $y \preceq c$ y $y' \preceq' c'$, con lo cual c es una cota superior de $\{x, y\}$ en L y c' es una cota superior de $\{x', y'\}$ en L' . Luego $a \preceq c$ y $a' \preceq' c'$ y entonces $(a, a') \preceq_{\text{prod}} (c, c')$. Concluimos que (a, a') es el mínimo del conjunto de cotas superiores y entonces $(c, c') = \sup\{(x, x'), (y, y')\}$.

Análogamente se muestra que si $b = \inf\{x, y\}$ y $b' = \inf\{x', y'\}$ entonces $(b, b') = \inf\{(x, x'), (y, y')\}$. \square

3.2. Las operaciones “join” y “meet”

La existencia de supremo e ínfimo para los conjuntos de dos elementos permite definir dos operaciones binarias en un retículo (L, \preceq) (trataremos este tema formalmente en el próximo capítulo). Es decir:

Definición 3.2.1. Sea (L, \preceq) un retículo. Entonces están bien definidas dos funciones (operaciones)

$$\vee : L \times L \rightarrow L, \quad \vee(x, y) = \sup\{x, y\},$$

$$\wedge : L \times L \rightarrow L, \quad \wedge(x, y) = \inf\{x, y\}.$$

\vee se denomina **join** del retículo (L, \preceq) y \wedge se denomina **meet** de (L, \preceq) . Se denota $x \vee y := \vee(x, y)$ y $x \wedge y := \wedge(x, y)$

Ejemplo 3.2.2. Si $X \neq \emptyset$, las operaciones join y meet para el retículo (X, \subseteq) (ver Ejemplo 3.1.4) son la unión y la intersección de conjuntos respectivamente. Esto es, si $A, B \subseteq X$, entonces $A \vee B = A \cup B$ y $A \wedge B = A \cap B$. \blacksquare

Ejemplo 3.2.3. Para el retículo $(\mathbb{N}, |)$ (ver Ejemplo 3.1.5) las operaciones join y meet son el mínimo común múltiplo y el máximo común divisor respectivamente. Esto es, para cada $x, y \in \mathbb{N}$, $x \wedge y = \text{m. c. m.}(x, y)$ y $x \vee y = \text{m. c. d.}(x, y)$. \blacksquare

Teorema 3.2.4. Sea (L, \preceq) un retículo. Entonces para cada $x, y, z \in L$ se verifica:

1. $x \preceq x \vee y$.
2. $x \wedge y \preceq x$.
3. $x \preceq y \iff x = x \wedge y \iff y = x \vee y$.
4. \vee y \wedge son asociativas, esto es,

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

5. \vee y \wedge son conmutativas, esto es,

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

6. Cada elemento es idempotente, esto es, $x \vee x = x$ y $x \wedge x = x$.

7. $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ (propiedad de absorción).

8. \vee y \wedge son compatibles con el orden \preceq , esto es,

$$\left. \begin{array}{l} x \preceq y \\ x' \preceq y' \end{array} \right\} \implies x \vee x' \preceq y \vee y', \quad \left. \begin{array}{l} x \preceq y \\ x' \preceq y' \end{array} \right\} \implies x \wedge x' \preceq y \wedge y'$$

Demostración. La prueba de los puntos 1, 2, 3, 5 y 6 son inmediatas y las dejamos como **ejercicio**.

Probemos 4. Sean $x, y, z \in L$ y consideremos

$$a = x \wedge y = \inf\{x, y\}, \quad a' = y \wedge z = \inf\{y, z\}.$$

Sean $b = \inf\{a, z\}$. Debemos probar que $b = \inf\{x, a'\}$.

Veamos primero que b es una cota inferior de $\{x, a'\}$. Como $b \preceq a$ y $a \preceq x$, resulta

$$(3.1) \quad b \preceq x.$$

Con el mismo argumento, $b \preceq y$ y por definición de b , $b \preceq z$. Luego

$$(3.2) \quad b \preceq \inf\{y, z\} = a'.$$

De (3.1) y (3.2), b resulta una cota inferior de $\{x, a'\}$.

Veamos ahora que para cualquier cota inferior c de $\{x, a'\}$, $c \preceq b$.

En efecto, si c es cota inferior de $\{x, a'\}$ entonces $c \preceq x$ y $c \preceq a' = \inf\{y, z\}$. De esto último obtenemos que $c \preceq y$ y $c \preceq z$. Tenemos entonces que

$$c \preceq x, \quad c \preceq y, \quad c \preceq z.$$

En particular, c es una cota inferior de $\{x, y\}$ y por lo tanto $c \preceq a = \inf\{x, y\}$. Luego c es una cota inferior de $\{a, z\}$ y por lo tanto $c \preceq b$ como queríamos probar.

La prueba de la asociatividad de \vee es análoga y la dejamos como ejercicio.

Probemos 6. Por el punto 2, $x \wedge y \preceq x$. Luego por el ítem 3, $x = (x \wedge y) \vee x = x \vee (x \wedge y)$, donde la última igualdad vale por la conmutatividad de \vee (ítem 5). La otra propiedad de absorción es análoga y la dejamos como ejercicio.

Probemos finalmente la compatibilidad de estas operaciones con el orden \preceq (ítem 8). Supongamos que $x \preceq y$ y $x' \preceq y'$. Sea $a = y \vee y'$. Entonces $y \preceq a$ y $y' \preceq a$, con lo cual $x \preceq a$ y $x' \preceq a$. Luego a es una cota superior de $\{x, x'\}$ y entonces $\sup\{x, x'\} \preceq a$. Es decir $x \vee x' \preceq y \vee y'$. La compatibilidad de \wedge con \preceq es análoga y la dejamos como ejercicio. \square

Las operaciones \wedge y \vee caracterizan completamente los retículos, en el sentido que cualquier conjunto con dos operaciones que satisfagan los ítem 4 a 7 admite un orden para el cual es un retículo:

Teorema 3.2.5. *Sea L un conjunto no vacío con dos operaciones, $\vee : L \times L \rightarrow L$ y $\wedge : L \times L \rightarrow L$ tales que:*

1. \vee y \wedge son asociativas: para cada $x, y, z \in L$,

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

2. \vee y \wedge son conmutativas: para cada $x, y \in L$,

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

3. Cada elemento es idempotente, esto es, $x \vee x = x$ y $x \wedge x = x$ para cada $x \in L$.

4. Valen las propiedades de absorción: para cada $x, y \in L$,

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

Entonces la relación \preceq en L definida por

$$(3.3) \quad x \preceq y \iff x \vee y = y$$

es un orden parcial en L que además verifica

$$(3.4) \quad x \preceq y \iff x \wedge y = x.$$

Más aún, (L, \preceq) es un retículo tal que para cada $x, y \in L$, $\inf\{x, y\} = x \wedge y$ y $\sup\{x, y\} = x \vee y$, esto es, \wedge y \vee son el meet y el join para (L, \preceq) respectivamente.

Demostración. Comencemos probando que la relación \preceq definida por (3.3) es un orden parcial en L .

Sea $x \in L$. Como x es idempotente para \vee , resulta $x = x \vee x$ y por lo tanto $x \preceq x$. Luego \preceq es reflexiva.

Sean $x, y \in L$ tales que $x \preceq y$ y $y \preceq x$. Entonces $x \vee y = y$ y $y \vee x = x$. Como \vee es conmutativa, resulta $x \vee y = y \vee x$ y por lo tanto $x = y$. Luego \preceq es antisimétrica.

Veamos finalmente que \preceq es transitiva. Sean $x, y, z \in L$ tales que $x \preceq y$ y $y \preceq z$. Entonces $x \vee y = y$ y $y \vee z = z$. Por lo tanto, como \vee es asociativa tendremos

$$x \vee z = x \vee (y \vee z) = (x \vee y) \vee z = y \vee z = z \implies x \preceq z.$$

Probaremos ahora que la relación \preceq verifica (3.4). En efecto, si $x \preceq y$ entonces $x \vee y = y$ y por lo tanto, de las propiedades de absorción resulta

$$x \wedge y = x \wedge (x \vee y) \stackrel{4}{=} x.$$

Recíprocamente, si $x \wedge y = x$, entonces $x \vee y = (x \wedge y) \vee y \stackrel{2}{=} y \vee (y \wedge x) \stackrel{4}{=} y$, y por lo tanto $x \preceq y$.

Veamos ahora que para cada $x, y \in L$, existen $\inf\{x, y\} = x \wedge y$ y $\sup\{x, y\} = x \vee y$.

Sean $x, y \in L$ cualesquiera y sea $w = x \vee y$. Entonces tendremos que

$$x \vee w = x \vee (x \vee y) \stackrel{1}{=} (x \vee x) \vee y \stackrel{3}{=} x \vee y = w \implies x \preceq w$$

y de manera análoga $y \preceq w$. Luego w es una cota superior de $\{x, y\}$.

Sea ahora z una cota superior cualquiera de $\{x, y\}$. Entonces $x \preceq z$ y $y \preceq z$, de donde $x \vee z = z$ y $y \vee z = z$. Luego

$$w \vee z = (x \vee y) \vee z \stackrel{1}{=} x \vee (y \vee z) = x \vee z = z \implies w \preceq z.$$

Concluimos que $w = x \vee y$ es un mínimo en el conjunto de cotas superiores de $\{x, y\}$ y por lo tanto $x \vee y = \sup\{x, y\}$.

A partir de (3.4) la prueba de que $\inf\{x, y\} = x \wedge y$ es similar y la dejamos como **ejercicio**. \square

Definición 3.2.6. Sea L un conjunto no vacío y \vee y \wedge dos operaciones en L que satisfacen las hipótesis del Teorema 3.2.5. La relación de orden \preceq en L definida por (3.3) o por 3.4 se denomina **orden inducido por \vee y \wedge** . Esta manera de definir un retículo L se denomina **definición algebraica** de L . Denotamos un retículo definido algebraicamente por (L, \vee, \wedge) .

Usaremos la notación $(L, \preceq) = (L, \vee, \wedge)$ para indicar que \preceq es el orden inducido por \vee y \wedge , o que \vee y \wedge son el join y el meet para el orden \preceq .

Ejemplo 3.2.7. Definición algebraica del retículo producto. Consideremos dos retículos (L, \vee_L, \wedge_L) y $(L', \vee_{L'}, \wedge_{L'})$ definidos algebraicamente. En $L \times L'$ consideremos las funciones \vee_{prod} y \wedge_{prod} de la siguiente manera:

$$(x, x') \vee_{prod} (y, y') = (x \vee_L x', y \vee_{L'} y'), \quad (x, x') \wedge_{prod} (y, y') = (x \wedge_L x', y \wedge_{L'} y').$$

Es fácil verificar que \vee_{prod} y \wedge_{prod} satisfacen las hipótesis del Teorema 3.2.5 y por lo tanto definen un retículo $(L \times L', \preceq)$ cuyo orden está dado por

$$(x, x') \preceq (y, y') \iff (x, x') \vee_{prod} (y, y') = (y, y').$$

Pongamos \preceq_L y $\preceq_{L'}$ los ordenes inducidos por \vee_L y \wedge_L , y por $\vee_{L'}$ y $\wedge_{L'}$ respectivamente. Tenemos entonces

$$\begin{aligned} (x, x') \preceq (y, y') &\iff (x, x') \vee_{prod} (y, y') = (y, y') \iff x \vee_L y = y, \quad x' \vee_{L'} y' = y' \\ &\iff x \preceq_L y, \quad x' \preceq_{L'} y' \iff (x, x') \preceq_{prod} (y, y'). \end{aligned}$$

Es decir, \preceq es el orden producto de los órdenes \preceq_L y $\preceq_{L'}$. ■

Ejemplo 3.2.8. Definición algebraica del retículo dual. Sea (L, \vee, \wedge) un retículo definido algebraicamente. Definamos en L las operaciones $\vee^* = \wedge$ y $\wedge^* = \vee$. Es inmediato verificar que \vee^* y \wedge^* satisfacen las hipótesis del Teorema 3.2.5 y por lo tanto (L, \vee^*, \wedge^*) es un retículo definido algebraicamente. Si \preceq es el orden asociado a (L, \vee, \wedge) y \preceq^* es el orden asociado a (L, \vee^*, \wedge^*) , entonces para cada $x, y \in L$ tenemos

$$x \preceq y \iff x \vee y = y \iff x \wedge^* y = y \iff y \preceq^* x.$$

Es decir, el orden inducido por \vee^* y \wedge^* en L es el orden inverso al que inducen \vee y \wedge . ■

Ejemplo 3.2.9. El retículo 2^n . Consideremos el conjunto $\mathbf{2} = \{0, 1\}$ y pongamos $\vee = \oplus$ y $\wedge = \odot$ suma y el producto booleanos dados en la Definición 1.4.12. Es decir, \vee y \wedge están dados por las siguientes tablas:

\vee	0	1
0	0	1
1	1	1

,

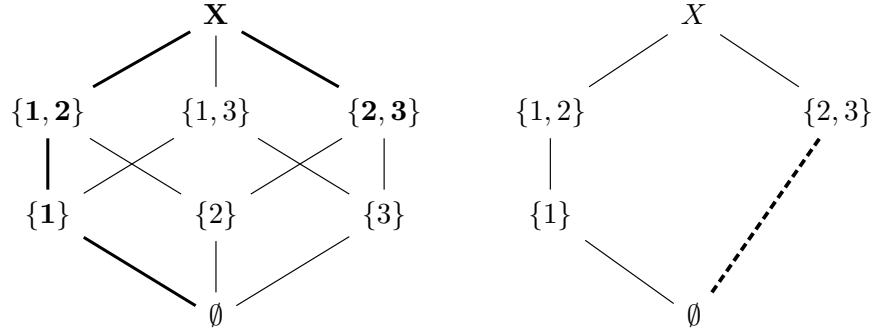
\wedge	0	1
0	0	0
1	0	1

Es inmediato (aunque un poco trabajoso) verificar que \vee y \wedge verifican las hipótesis del Teorema 3.2.5 y por lo tanto $(\mathbf{2}, \vee, \wedge)$ es un retículo definido algebraicamente. Observemos que el orden inducido por \vee y \wedge es el orden usual en $\{0, 1\}$. Por 2^n denotaremos el retículo producto definido inductivamente como $2^1 = \mathbf{2}$, $2^{n+1} = \mathbf{2} \times 2^n$. ■

3.3. Subretículos

Si (A, \preceq) es un poset, entonces $(A, \preceq|_A)$ es un poset. Sin embargo, vimos en la Observación 3.1.6 que esto es falso si reemplazamos “poset” por “retículo”. Es decir, un subconjunto de un retículo con el orden restringido no necesariamente es un retículo. Incluso si esto ocurre, podría suceder que las operaciones \vee y \wedge no se restrinjan adecuadamente a L' , como veremos en el ejemplo siguiente.

Ejemplo 3.3.1. Consideremos $X = \{1, 2, 3\}$ y el retículo $L = (\mathcal{P}(X), \subseteq)$. Sea $L' = \{\emptyset, \{1\}, \{1, 2\}, \{2, 3\}, X\}$. Entonces $(L', \subseteq|_{L'})$ es un retículo (las líneas punteadas indicaran aristas que no forman parte del diagrama de Hasse original):



Observemos que en L , $\vee = \cup$ y $\wedge = \cap$, pero en L' , $\{1, 2\} \wedge' \{2, 3\} = \emptyset \neq \{1, 2\} \cap \{2, 3\}$. Esto último se debe a que $\{1, 2\} \cap \{2, 3\} \notin L'$, es decir, \wedge no es una operación cerrada en L' . ■

Lema 3.3.2. Sea $(L, \vee, \wedge) = (L, \preceq)$ un retículo y sea $L' \subseteq L$. Si $\vee(L' \times L') \subseteq L'$ y $\wedge(L' \times L') \subseteq L'$, entonces $(L', \preceq|_{L'})$ es un retículo tal que su join y meet son respectivamente $\vee_{L'} : L' \times L' \rightarrow L'$ y $\wedge_{L'} : L' \times L' \rightarrow L'$ definidas por

$$x \vee_{L'} y = x \vee y, \quad x \wedge_{L'} y = x \wedge y$$

para cada $x, y \in L'$

Demostración. Supongamos $\vee(L' \times L') \subseteq L'$ y $\wedge(L' \times L') \subseteq L'$. Quedan entonces bien definidas las operaciones

$$\vee_{L'} : L' \times L' \rightarrow L' \rightarrow L', \quad \wedge_{L'} : L' \times L' \rightarrow L'$$

por $\vee_{L'}(x, y) = x \vee y \in L'$ y $\wedge_{L'}(x, y) = x \wedge y \in L'$. Es inmediato verificar que $\vee_{L'}$ y $\wedge_{L'}$ satisfacen las hipótesis del Teorema 3.2.5 y por lo tanto existe un orden \preceq' en L' tal que (L', \preceq') es un retículo cuyos join y meet son $\vee_{L'}$ y $\wedge_{L'}$ respectivamente.

Si ahora $x, y \in L'$, entonces

$$x \preceq' y \xLeftrightarrow{\text{Teo. 3.2.5}} x \vee_{L'} y = y \iff x \vee y = y \xLeftrightarrow{\text{Teo. 3.2.4}} x \preceq y$$

Concluimos que para cada $x, y \in L'$, $x \preceq' y$ si y sólo si $x \preceq y$, con lo cual $\preceq' = \preceq|_{L'}$. □

Observación 3.3.3. Como hemos observado en el Ejemplo 3.3.1, puede ocurrir que si (L, \preceq) es un retículo y L' es un subconjunto de L , entonces $(L', \preceq|_{L'})$ sea un retículo aunque $\vee(L' \times L') \not\subseteq L'$ o $\wedge(L' \times L') \not\subseteq L'$.

En vistas del Lema 3.3.2 y de la Observación 3.3.3 nos interesa distinguir aquellos subconjuntos L' de un retículo (L, \preceq) tales que $(L', \preceq|_{L'})$ es un retículo cuyos join y el meet son el join y el meet de L restringido a L' , y aquellos que no verifican esta propiedad:

Definición 3.3.4. Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Un subconjunto $L' \subseteq L$ es un **subretículo** de L si para cada $x, y \in L'$, $x \vee y \in L'$ y $x \wedge y \in L'$. En ese caso, si $\vee_{L'}$ y $\wedge_{L'}$ están definidas como en el Lema 3.3.2, $(L', \preceq|_{L'})$ es un retículo definido algebraicamente por $(L, \vee_{L'}, \wedge_{L'})$

Observación 3.3.5. Sea L un retículo y $L' \subseteq L$. Dado que para cada $x \in L'$, $x \vee x = x \wedge x = x \in L'$ y si $x, y \in L'$ verifican $x \preceq y$, $x \vee y = y \in L'$ y $x \wedge y = x \in L'$, para verificar si L' es un subretículo de L basta comprobar que $x \vee y \in L'$ y $x \wedge y \in L'$ para x e y elementos no comparables de L' .

Lema 3.3.6. Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Entonces:

1. Si L' y L'' son subretículos de L , entonces $L' \cap L''$ es un subretículo de L .
2. Si L' y L'' son subretículos de L y $L'' \subseteq L'$ entonces L'' es un subretículo de L' .
3. Si L' es un subretículo de L y L'' es un subretículo de L' , entonces L'' es un subretículo de L .

Demostración. Probemos el punto 1. Sean $x, y \in L' \cap L''$. Como L' es subretículo de L , $x \vee y \in L'$ y $x \wedge y \in L'$. Pero L'' también es subretículo de L , con lo cual $x \vee y \in L''$ y $x \wedge y \in L''$. Concluimos que $x \vee y \in L' \cap L''$ y $x \wedge y \in L' \cap L''$, con lo cual $L' \cap L''$ es un subretículo de L .

Veamos ahora el punto 2. Pongamos $\vee_{L'}$ y $\wedge_{L'}$ el join y el meet del subretículo $(L', \preceq|_{L'})$. Como L' es subretículo de L , para cada $x, y \in L'$, $x \vee_{L'} y = x \vee y$ y $x \wedge_{L'} y = x \wedge y$. Por otra parte, como L'' es subretículo de L , tenemos que si $x, y \in L''$, entonces $x \vee y \in L''$ y $x \wedge y \in L''$. Luego para cada $x, y \in L''$,

$$x \vee_{L'} y = x \vee y \in L'', \quad x \wedge_{L'} y = x \wedge y \in L''$$

con lo cual L'' es un subretículo de L' .

Veamos finalmente el punto 3. Pongamos nuevamente $\vee_{L'}$ y $\wedge_{L'}$ el join y el meet del subretículo $(L', \preceq|_{L'})$. Como L'' es subretículo de L' , para cada $x, y \in L''$, $x \vee_{L'} y \in L''$ y $x \wedge_{L'} y \in L''$. Pero por cómo están definidas $\vee_{L'}$ y $\wedge_{L'}$, dados $x, y \in L'' \subseteq L'$ se tiene

$$x \vee y = x \vee_{L'} y \in L'', \quad x \wedge y = x \wedge_{L'} y \in L''$$

con lo cual L'' es un subretículo de L . □

Ejemplo 3.3.7. Continuando con el ejemplo 3.3.1, tenemos que si $L' = \{\emptyset, \{1\}, \{1, 2\}, \{2, 3\}, X\}$, entonces (L', \subseteq) es un retículo que no es un subretículo de $(\mathcal{P}(X), \subseteq)$, con $X = \{1, 2, 3\}$.

Consideremos ahora $L'' = \{\emptyset, \{1\}, \{1, 2\}, X\}$. Entonces en $(\mathcal{P}(X), \subseteq) = (\mathcal{P}(X), \cup, \cap)$,

$$\emptyset \cup X = \{1\} \cup X = \{1, 2\} \cup X = X \in L'', \quad \emptyset \cup \{1, 2\} = \{1\} \cup \{1, 2\} = \{1, 2\} \in L'', \quad \emptyset \cup \{1\} = \{1\} \in L''$$

$$\emptyset \cap \{1\} = \emptyset \cap \{1, 2\} = \emptyset \cap X = \emptyset \in L''; \quad \{1\} \cap \{1, 2\} = \{1\} \cap X = \{1\} \in L'', \quad \{1, 2\} \cap X = \{1, 2\} \in L''$$

con lo cual L'' es un subretículo de $(\mathcal{P}(X), \subseteq)$. Observemos que L'' también es un subretículo de (L', \subseteq) , aunque este último no sea un subretículo de $\mathcal{P}(X)$. ■

Ejemplo 3.3.8. El caso de L'' del ejemplo anterior puede generalizarse de la siguiente manera: Si $(L, \preceq) = (L, \vee, \wedge)$ es un retículo y L' es una cadena en L , entonces L' es un subretículo de L .

En efecto, al ser L' una cadena, $(L', \preceq_{|L'})$ es totalmente ordenado. Luego dados $x, y \in L'$, se tiene que $x \vee y = y$ y $x \wedge y = x$, si $x \preceq y$, o bien $x \vee y = x$ y $x \wedge y = y$ si $y \preceq x$. En cualquier caso resulta $x \vee y \in L'$ y $x \wedge y \in L'$. ■

Ejemplo 3.3.9. Los retículos $(D_n, |)$ son subretículos de $(\mathbb{N}, |)$ para cada $n \in \mathbb{N}$, puesto que en ambos casos $\vee = \text{m. c. m.}$ y $\wedge = \text{m. c. d.}$. Además, si $n | m$, entonces todos los divisores de n son también divisores de m . Por lo tanto $D_n \subseteq D_m$, y entonces $(D_n, |)$ es un subretículo de $(D_m, |)$. ■

3.4. Morfismos de retículos

Recordemos que una función $f : (L, \preceq) \rightarrow (L', \preceq')$ es un morfismo de orden si se verifica que para cada $x, y \in L$,

$$x \preceq y \implies f(x) \preceq' f(y)$$

y que f es un isomorfismo entre L y L' si f es un morfismo de orden biyectivo tal que su inversa es un morfismo de orden, o equivalentemente (ver Teorema 2.5.6), si f es sobreyectiva y para cada $x, y \in L$

$$x \preceq y \iff f(x) \preceq' f(y).$$

A su vez, f es un anti-isomorfismo si es un isomorfismo de (L, \preceq) en (L', \succeq) .

Recordemos además que un morfismo de orden biyectivo no es necesariamente un isomorfismo de orden (ver Ejemplo 2.5.4).

Definiremos a continuación qué entendemos por *morfismo de retículos*. Un retículo es, en particular, un poset. Por lo tanto un morfismo de retículos debe ser en primer lugar un morfismo de posets. Pero además deberá preservar las operaciones que definen a los retículos, esto es, el join y el meet. Como veremos en el ejemplo siguiente, esto no necesariamente sucede con un morfismo de posets entre dos retículos:

Ejemplo 3.4.1. Consideremos el morfismo de posets $\text{Id} : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ (ver Ejemplo 2.5.4). Pongamos $\vee_1, \wedge_1, \vee_\leq, \wedge_\leq$ el join y el meet en $(\mathbb{N}, |)$ y en (\mathbb{N}, \leq) respectivamente. En $(\mathbb{N}, |)$ tenemos que

$$x \vee_1 y = \text{m. c. m.}(x, y), \quad x \wedge_1 y = \text{m. c. d.}(x, y)$$

y en (\mathbb{N}, \leq) tenemos

$$x \vee_\leq y = \min(x, y), \quad x \wedge_\leq y = \max(x, y)$$

donde \min y \max son el mínimo y el máximo para el orden \leq . Entonces no es cierto en general que

$$\text{Id}(x \vee_1 y) = \text{Id}(x) \vee_\leq \text{Id}(y), \quad \text{y} \quad \text{Id}(x \wedge_1 y) = \text{Id}(x) \wedge_\leq \text{Id}(y).$$

En efecto, basta tomar $x = 2, y = 3$ y tendremos que $2 \vee_1 3 = 6$ y $\text{Id}(2) \vee_\leq \text{Id}(3) = 2 \vee_\leq 3 = 3 \neq \text{Id}(6)$. ■

En cualquier estructura, un morfismo de esa estructura debe preservar los elementos que la definen. En este caso, definimos:

Definición 3.4.2. Sean $(L, \preceq) = (L, \vee, \wedge)$ y $(L', \preceq') = (L', \tilde{\vee}, \tilde{\wedge})$ retículos. Una función $f : L \rightarrow L'$ es un **morfismo de retículos** si f es un morfismo de posets tal que para cada $x, y \in L$,

$$f(x \vee y) = f(x) \tilde{\vee} f(y), \quad f(x \wedge y) = f(x) \tilde{\wedge} f(y)$$

Ya hemos observado que un morfismo de posets entre dos retículos no necesariamente es un morfismo de retículos. Veremos a continuación que basta que una función preserve el join y el meet para que sea un morfismo de retículos.

Lema 3.4.3. Sean $(L, \preceq) = (L, \vee, \wedge)$ y $(L', \preceq') = (L', \tilde{\vee}, \tilde{\wedge})$ retículos y sea $f : L \rightarrow L'$. Entonces f es un morfismo de retículos si y sólo si para cada $x, y \in L$ se verifican

$$(3.5) \quad f(x \vee y) = f(x) \tilde{\vee} f(y), \quad f(x \wedge y) = f(x) \tilde{\wedge} f(y).$$

Demostración. Claramente, si f es un morfismo de retículos se verifican las propiedades (3.5). Por lo tanto sólo debemos ver que una función $f : L \rightarrow L'$ que verifique (3.5) es un morfismo de orden. Sean $x, y \in L$ tales que $x \preceq y$. Entonces $x \vee y = y$ y por (3.5) $f(x) \tilde{\vee} f(y) = f(y)$. Luego $f(x) \preceq' f(y)$. \square

Ejemplo 3.4.4. Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo y $S \subset L$ un subconjunto de L .

Supongamos que $(S, \preceq|_S) = (S, \vee_S, \wedge_S)$ es un subretículo de L y consideremos la inclusión $i : S \rightarrow L$, $i(x) = x$ para cada $x \in S$. Entonces por el Lema 3.3.2 tenemos que para cada $x, y \in S$,

$$i(x \vee_S y) = i(x \vee y) = x \vee y = i(x) \vee i(y)$$

y de manera análoga $i(x \wedge_S y) = i(x \wedge y) = x \wedge y = i(x) \wedge i(y)$. Concluimos que i es un morfismo de retículos. Puede probarse que también vale la recíproca (ver el Ejercicio 12 de este capítulo). \blacksquare

Lema 3.4.5. Sean $(L, \preceq) = (L, \vee, \wedge)$, $(L', \preceq') = (L', \vee', \wedge')$ y $(L'', \preceq'') = (L'', \vee'', \wedge'')$ retículos y $f : L \rightarrow L'$, $g : L' \rightarrow L''$ morfismos de retículos. Entonces $g \circ f : L \rightarrow L''$ es un morfismo de retículos.

Demostración. Sean $x, y \in L$. Entonces

$$\begin{aligned} (g \circ f)(x \vee y) &= g(f(x \vee y)) = g(f(x) \vee' f(y)) = g(f(x)) \vee'' g(f(y)) \\ &= (g \circ f)(x) \vee'' (g \circ f)(y) \end{aligned}$$

De manera análoga se prueba que $(g \circ f)(x \wedge y) = (g \circ f)(x) \wedge'' (g \circ f)(y)$. Luego del Lema 3.4.3 resulta $g \circ f$ un morfismo de retículos. \square

Definición 3.4.6. Sean L y L' retículos y $f : L \rightarrow L'$ una función. Decimos que f es un **isomorfismo de retículos** si f es biyectiva y f y f^{-1} son morfismos de retículos. f es un **anti-isomorfismo de retículos** de L en L' si f es un isomorfismo de retículos de (L, \preceq) en (L', \succeq) .

Ejemplo 3.4.7. Sea (L, \preceq) un retículo. Entonces es inmediato que $\text{Id} : (L, \preceq) \rightarrow (L, \preceq)$ es un isomorfismo de retículos y $\text{Id} : (L, \preceq) \rightarrow (L, \succeq)$ es un anti-isomorfismo de retículos. ■

Lema 3.4.8. Sean $(L, \preceq) = (L, \vee, \wedge)$ y $(L', \preceq') = (L', \tilde{\vee}, \tilde{\wedge})$ retículos y sea $f : L \rightarrow L'$. Entonces f es un isomorfismo de retículos si y sólo si f es un morfismo de retículos biyectivo. Esto es: f es un isomorfismo de retículos si y sólo si

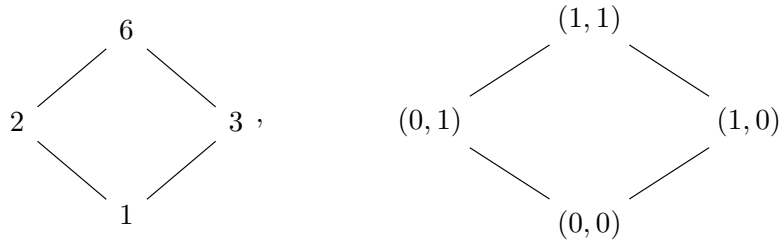
- f es biyectiva;
- Para cada $x, y \in L$, $f(x \vee y) = f(x) \tilde{\vee} f(y)$ y $f(x \wedge y) = f(x) \tilde{\wedge} f(y)$.

Demostración. Por definición, si f es un isomorfismo de retículos entonces f es un morfismo de retículos biyectivo. Por lo tanto, debemos ver que todo morfismo de retículos biyectivo es un isomorfismo de retículos, y para ello solo nos queda probar que f^{-1} es un morfismo de retículos. Sean entonces $v, w \in L'$ y sean $x = f^{-1}(v)$, $y = f^{-1}(w)$. Entonces

$$f(x \vee y) = f(x) \tilde{\vee} f(y) = v \tilde{\vee} w \implies x \vee y = f^{-1}(v \tilde{\vee} w).$$

Por lo tanto tendremos $f^{-1}(v \tilde{\vee} w) = x \vee y = f^{-1}(v) \vee f^{-1}(w)$ como queríamos probar. La demostración de que $f^{-1}(v \tilde{\wedge} w) = f^{-1}(v) \wedge f^{-1}(w)$ es análoga. □

Ejemplo 3.4.9. Consideremos el retículo $L = (D_6, |)$ y el retículo $L' = (\{0, 1\} \times \{0, 1\}, \leq_{\text{prod}})$, donde en $\{0, 1\}$ tomamos el orden usual. Observemos que ambos diagramas de Hasse de L y L' son iguales, lo único que cambia es la etiqueta de los vértices:



Definamos $f : L \rightarrow L'$ poniendo

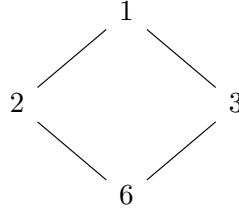
$$f(1) = (0, 0), \quad f(2) = (0, 1), \quad f(3) = (1, 0), \quad f(6) = (1, 1).$$

Es claro que f es biyectiva, y además si \vee, \wedge y $\tilde{\vee}, \tilde{\wedge}$ son el join y el meet de L y L' respectivamente, entonces:

$$\begin{aligned} f(1 \vee 2) &= f(2) = (0, 1) = (0, 0) \tilde{\vee} (0, 1) = f(1) \tilde{\vee} f(2) \\ f(1 \vee 3) &= f(3) = (1, 0) = (0, 0) \tilde{\vee} (1, 0) = f(1) \tilde{\vee} f(3) \\ f(1 \vee 6) &= f(6) = (1, 1) = (0, 0) \tilde{\vee} (1, 1) = f(1) \tilde{\vee} f(6) \\ f(2 \vee 3) &= f(6) = (1, 1) = (0, 1) \tilde{\vee} (1, 0) = f(2) \tilde{\vee} f(3) \\ f(2 \vee 6) &= f(6) = (1, 1) = (0, 1) \tilde{\vee} (1, 1) = f(2) \tilde{\vee} f(6) \\ f(3 \vee 6) &= f(6) = (1, 1) = (1, 0) \tilde{\vee} (1, 1) = f(3) \tilde{\vee} f(6) \end{aligned}$$

esto es, $f(x \vee y) = f(x) \tilde{\vee} f(y)$ para cada $x, y \in L$. De manera análoga se prueba que $f(x \wedge y) = f(x) \tilde{\wedge} f(y)$ para cada $x, y \in L$, con lo cual f es un isomorfismo de retículos.

Si ahora consideramos el retículo dual L^* , su diagrama de Hasse es el siguiente:



Nuevamente se trata de un diagrama idéntico al de L , salvo por la etiqueta de los nodos. Con el mismo razonamiento que para f , puede probarse que $g : L \rightarrow L^*$ tal que $g(1) = 6$, $g(2) = 2$, $g(3) = 3$, $g(6) = 1$ es un isomorfismo de retículos, o equivalentemente, $g : L \rightarrow L$ es un anti-isomorfismo de retículos. ■

Como ya hemos notado, un morfismo de posets entre dos retículos no tiene por qué ser un morfismo de retículos. Esto cambia en el caso de un isomorfismo de posets. Observemos que todo isomorfismo de retículos es en particular un isomorfismo de posets. La recíproca también es válida, más aún tenemos:

Teorema 3.4.10. Sean $(L, \preceq) = (L, \vee, \wedge)$ un retículo y (L', \preceq') un poset. Si $f : L \rightarrow L'$ es un isomorfismo de posets entonces:

1. (L', \preceq') es un retículo.
2. f es un isomorfismo de retículos.

Demostración. Veamos primero que (L', \preceq') es un retículo. Sean $x', y' \in L'$ y sean $x, y \in L$ (los únicos elementos) tales que $f(x) = x'$, $f(y) = y'$. Del Teorema 2.5.15 resulta que existen $\sup_L \{x, y\}$ y $\inf_L \{x, y\}$ y verifican

$$\sup_{L'} \{x', y'\} = f(\sup_L \{x, y\}) = f(x \vee y), \quad \inf_{L'} \{x', y'\} = f(\inf_L \{x, y\}) = f(x \wedge y).$$

Por lo tanto (L', \preceq') es un retículo, y si \vee', \wedge' son el join y el meet de L' respectivamente,

$$f(x \vee y) = f(x) \vee' f(y), \quad f(x \wedge y) = f(x) \wedge' f(y).$$

Como f es un isomorfismo de orden, en particular f es biyectiva. Luego del Lema 3.4.8, f es un isomorfismo de retículos. □

A partir del Teorema 3.4.10 podemos aplicar a los retículos los resultados del Teorema 28 y el Corolario 2.5.9 del Capítulo 2:

Corolario 3.4.11. Sean L , L' y L'' retículos y $f : L \rightarrow L'$, $g : L' \rightarrow L''$ isomorfismos de retículos. Entonces:

1. $\text{Id} : L \rightarrow L$ es un isomorfismo de retículos
2. $f^{-1} : L' \rightarrow L$ es un isomorfismo de retículos.
3. $g \circ f : L \rightarrow L''$ es un isomorfismo de retículos.

Corolario 3.4.12. Sea Ret el conjunto de todos los retículos. Entonces la relación \sim en Ret definida por $L \sim L'$ si existe un isomorfismo de retículos $f : L \rightarrow L'$ es una relación de equivalencia.

Definición 3.4.13. Sean L y L' retículos. Si existe un isomorfismo $f : L \rightarrow L'$ (y por lo tanto también existe un isomorfismo $g = f^{-1} : L' \rightarrow L$) L y L' se dicen **retículos isomorfos**.

Si un retículo L es isomorfo a su dual L^* (es decir, si existe un anti-isomorfismo de L en L), L se denomina un retículo **autodual**.

Ejemplo 3.4.14. Consideremos los retículos $L = \mathbf{2}^n = \{0, 1\}^n$ con el orden producto (ver Ejemplo 3.2.9) y $L' = (\mathcal{P}(\{1, \dots, n\}), \subseteq)$. Vimos en el Ejemplo 2.5.12 que la función $f : L' \rightarrow L$ tal que $f(A) = (\varepsilon_1^A, \dots, \varepsilon_n^A)$, con

$$\varepsilon_n^A = \begin{cases} 1 & \text{si } i \in A \\ 0 & \text{si } i \notin A \end{cases}$$

es un isomorfismo de orden. Luego por el Teorema 3.4.10, f es un isomorfismo de retículos. ■

Ejemplo 3.4.15. Vimos en el Ejemplo 3.1.2 que un conjunto totalmente ordenado es un retículo. Por otra parte, vimos en el Ejemplo 2.5.11 del Capítulo 2, si $(A = \{a_1, \dots, a_n\}, \preceq)$ es un conjunto totalmente ordenado de cardinal n , podemos ordenar los elementos de A de modo que $a_i \preceq a_j$ si y sólo si $i \leq j$, y

$$\Phi : (I_n, \leq) \rightarrow A, \quad \Phi(i) = a_i$$

es un isomorfismo de posets, donde $I_n = \{1, \dots, n\}$. Del Teorema 3.4.10 resulta que Φ es un isomorfismo de retículos.

Concluimos que (A, \preceq) es un retículo isomorfo a (I_n, \preceq) , y en función del Corolario 3.4.12, que todos los conjuntos totalmente ordenados de cardinal n son retículos isomorfos entre sí.

Consideremos ahora la función $\varphi : I_n \rightarrow I_n$ dada por

$$\varphi(i) = (n+1) - i.$$

Tenemos en este caso que

$$i \leq j \iff (n+1) - j \leq (n+1) - i \iff \varphi(i) \geq \varphi(j)$$

Por lo tanto $\varphi : (I_n, \leq) \rightarrow (I_n, \geq)$ es un isomorfismo de orden, y por lo tanto es un isomorfismo de retículos. Luego I_n es un retículo autodual. Veremos en el Ejercicio 16 de este capítulo que si dos retículos son isomorfos, entonces sus duales también lo son. Luego cualquier conjunto finito totalmente ordenado es un retículo autodual. ■

Ejemplo 3.4.16. Vimos en el Ejemplo 3.4.9 que $(D_6, |)$ es un retículo autodual. Veremos que no se trata de un caso aislado, sino que todos los retículos $(D_n, |)$ son autoduales. Si $m \in \mathbb{N}$, consideremos la función $c_m : \mathbb{N} \rightarrow \mathbb{N}$ tal que $c_m(k)$ es el cociente de la división de k por m (esto es, $k = c_m(k)m + r_m(k)$, donde $r_m(k)$ es el resto de dividir k por m , ver el Teorema 2.3.2). Observemos que dados $m, n \in \mathbb{N}$,

$$m \mid n \iff n = c_m(n)m \iff r_m(n) = 0.$$

Por lo tanto si $m \in D_n$, entonces $n = mc_m(n)$ con lo cual $c_m(n)$ también es un divisor de n y $c_{c_m(n)}(n) = m$. Es decir, $c_m(n) \in D_n$ para cada $m \in D_n$ y podemos considerar entonces la función

$$f : D_n \rightarrow D_n^*, \quad f(m) = c_m(n)$$

Observemos que

$$f \circ f(m) = f(f(m)) = f(c_m(n)) = c_{c_m(n)}(n) = m.$$

O sea $f \circ f = Id$, y entonces f es biyectiva. Veamos que f es un isomorfismo de retículos. Por el Teorema 3.4.10 sólo debemos probar que es un isomorfismo de orden.

Para ello debemos ver que f verifica que $m \mid k$ si y sólo si $f(k) \mid f(m)$.

En efecto, si $m \mid k$, entonces $k = c_m(k)m$ y como a su vez $k \mid n$, tendremos:

$$n = c_k(n)k = c_k(n)c_m(k)m \quad \text{y} \quad n = c_m(n)m$$

De la unicidad del cociente (ver Teorema 2.3.2) resulta

$$c_m(n) = c_k(n)c_m(k) \implies f(m) = f(k)c_m(k)$$

de donde $f(k) \mid f(m)$.

Si ahora suponemos que $f(k) \mid f(m)$, entonces existe $\lambda \in \mathbb{N}$ tal que $f(m) = \lambda f(k)$. Ahora

$$n = f(k)k \quad \text{y} \quad n = f(m)m = \lambda f(k)m \implies f(k)k = \lambda f(k)m \implies k = \lambda m$$

y por lo tanto $m \mid k$ como queríamos ver. Observemos que si $a, b \in \text{Div}(n)$ para algún número natural n entonces

$$c_{\text{m.c.m.}(a,b)}(n) = f(a \vee b) = f(a) \vee^* f(b) = \text{m.c.d.}(c_a(n), c_b(n))$$

$$c_{\text{m.c.d.}(a,b)}(n) = f(a \wedge b) = f(a) \wedge^* f(b) = \text{m.c.m.}(c_a(n), c_b(n))$$

(comparar este resultado con el Ejercicio 10 del Capítulo 2). ■

Ejemplo 3.4.17. Recordemos que (\mathbb{N}, \leq) no es isomorfo a (\mathbb{N}, \geq) y por lo tanto no es auto-dual. Sin embargo (\mathbb{R}, \leq) sí lo es. En efecto, consideremos la función $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = -x$. Tenemos que

$$x \leq y \iff -y \leq -x \iff f(x) \geq f(y)$$

de donde $f : (\mathbb{R}, \leq) \rightarrow (\mathbb{R}, \geq)$ es un isomorfismo de orden y por el Teorema 3.4.10 f es un isomorfismo de retículos. ■

Finalizamos esta sección con un resultado que establece como obtener subretículos de un retículo dado a partir de un morfismo de retículos. Dejamos la prueba como ejercicio:

Teorema 3.4.18. Sean $(L, \preceq_L) = (L, \vee, \wedge)$ y $(S, \preceq_S) = (S, \tilde{\vee}, \tilde{\wedge})$ dos retículos y sea $f : L \rightarrow S$ un morfismo de retículos. Entonces:

1. Si L' es un subretículo de L , entonces $f(L')$ es un subretículo de S .
2. Si S' es un subretículo de S entonces $f^{-1}(S')$ es un subretículo de L .

Demostración. Probaremos solo el primer punto, dejamos el segundo como **ejercicio**.

Sean $x', y' \in f(L')$ y sean $x, y \in L'$ tales que $x' = f(x)$, $y' = f(y)$. Entonces, como L' es un subretículo de L , $x \vee y \in L'$ y $x \wedge y \in L'$. Como f es un morfismo de retículos tenemos:

$$x' \tilde{\vee} y' = f(x) \tilde{\vee} f(y) = f(x \vee y) \in f(L')$$

y de manera análoga $x' \tilde{\wedge} y' \in f(L')$. Luego $f(L')$ es un subretículo de S . □

3.5. Retículos acotados y complementados

Definición 3.5.1. Un retículo $(L, \preceq) = (L, \vee, \wedge)$ se dice **acotado** si como conjunto ordenado tiene máximo y mínimo. El máximo de L suele denotarse por \top o por 1 (y suele denominarse **top**) y el mínimo de L por \perp o 0 (y suele denominarse **bottom**). Denotaremos $(L, \preceq, 1, 0) = (L, \vee, \wedge, 1, 0)$ o $(L, \preceq, \top, \perp) = (L, \vee, \wedge, \top, \perp)$ a un retículo acotado con máximo 1 o \top y mínimo 0 o \perp .

Usualmente suelen reservarse los símbolos \top y \perp cuando tratamos con el orden de L y 1 y 0 cuando tratamos con su estructura algebraica, pero estos símbolos son intercambiables, y muchas veces es útil utilizar los primeros incluso cuando lidiamos con las operaciones \vee y \wedge para evitar confundir los elementos 1 y 0 (definidos en abstracto) con los números 1 y 0 que podrían estar presentes en el conjunto L sin ser su máximo o su mínimo.

En términos generales, tendremos que (L, \preceq) es un retículo acotado si existen $\top, \perp \in L$ tales que

$$\perp \preceq x, \quad x \preceq \top, \quad \forall x \in L$$

En términos de las operaciones \vee y \wedge , (L, \vee, \wedge) es un retículo acotado si existen $0, 1 \in L$ tales que

$$0 \wedge x = 0, \quad x \vee 1 = 1, \quad \forall x \in L$$

Ejemplo 3.5.2. Para cualquier conjunto X , $(\mathcal{P}(X), \subseteq) = (\mathcal{P}(X), \cup, \cap)$ es un retículo acotado con $1 = \top = X$ y $0 = \perp = \emptyset$. ■

Ejemplo 3.5.3. Para cada $n \in \mathbb{N}$, $(D_n, |)$ es un retículo acotado con $1 = \top = n$, $0 = \perp = 1$ (en este caso, por ejemplo, es preferible usar las notaciones \top y \perp , pues 1 adquiere dos significados distintos). Observemos que $(\mathbb{N}, |)$ no es un retículo acotado, aunque tiene mínimo $\perp = 1$. Como $x \mid 0$ para cualquier $x \in \mathbb{N}$, muchas veces en la bibliografía suele usarse la convención de que $0 \mid 0$. En este caso, el retículo $(\mathbb{N}_0, |)$ sí resulta acotado, siendo $\top = 0$. ■

Observación 3.5.4. Por el principio de dualidad resulta claro que L es un retículo acotado si y sólo si L^* es un retículo acotado, y valen $\top = \perp^*$, $\perp = \top^*$, o sea, $0^* = 1$ y $1^* = 0$. ■

El siguiente resultado es inmediato (ver Ejemplo 2.2.6):

Lema 3.5.5. Sean L y L' retículos acotados. Entonces $(L \times L', \preceq_{\text{prod}})$ es acotado. Más aún, $1_{L \times L'} = (1_L, 1_{L'})$ y $0_{L \times L'} = (0_L, 0_{L'})$, donde $1_L, 1_{L'}, 1_{L \times L'}$ y $0_L, 0_{L'}, 0_{L \times L'}$ son el máximo y el mínimo de L , L' y $L \times L'$ respectivamente.

Definición 3.5.6. Sea L un retículo acotado. Dado $a \in L$, un elemento $b \in L$ se denomina un **complemento** de a , o se dice que a está **complementado por** b , si

$$a \vee b = \top \quad y \quad a \wedge b = \perp.$$

Denotamos por $\text{comp}(a) = \{b \in L : b \text{ es un complemento de } a\}$

Un retículo acotado se dice un **retículo complementado** si existe una función

$$(\cdot)^c : L \rightarrow L, \quad a \mapsto a^c$$

tal que para cada $a \in L$, a^c es un complemento de a .

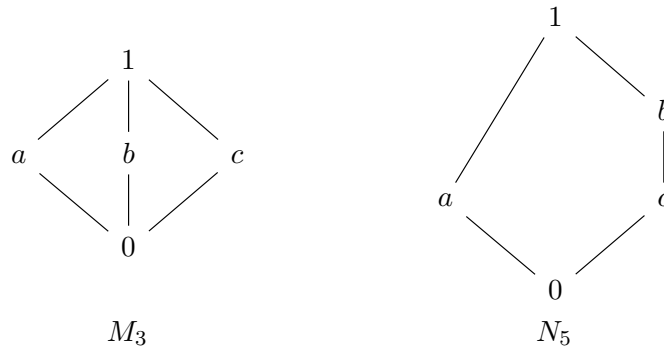
Observación 3.5.7. A partir del Axioma de Elección, un retículo es complementado si y sólo si todo elemento admite al menos un complemento, esto es, $\text{comp}(a) \neq \emptyset$ para cada $a \in L$.

En efecto, claramente si L es un retículo complementado, entonces $a^c \in \text{comp}(a)$ para cada $a \in L$, con lo cual $\text{comp}(a) \neq \emptyset$. Recíprocamente, supongamos que $\text{comp}(a) \neq \emptyset$ para cada $a \in L$ y consideremos la familia $\mathcal{F} = \{\text{comp}(a)\}_{a \in L}$ y la función $g : L \rightarrow \mathcal{F}$, $g(a) = \text{comp}(a)$. Por hipótesis \mathcal{F} es una familia no vacía de subconjuntos no vacíos de L . Luego, por el Teorema 2.6.5 existe una función selectora $f : \mathcal{F} \rightarrow L$ para la familia \mathcal{F} , es decir, tal que $f(\text{comp}(a)) \in \text{comp}(a)$ para cada $a \in L$. Entonces $(\cdot)^c = f \circ g : L \rightarrow L$ verifica que $a^c = f(g(a)) \in \text{comp}(a)$ para cada $a \in L$.

Observación 3.5.8. Es inmediato de la conmutatividad de \vee y \wedge que para cada $a \in L$, b es un complemento de a si y sólo si a es un complemento de b .

Además es claro que \top y \perp (o 1 y 0) son complementos uno del otro.

Ejemplo 3.5.9. Consideremos los retículos M_3 y N_5 introducidos en el Ejemplo 3.1.3, cuyos diagramas de Hasse son



Ambos retículos son claramente acotados. Observemos que en M_3 tenemos

$$\text{comp}(0) = \{1\}, \quad \text{comp}(1) = \{0\}, \quad \text{comp}(a) = \{b, c\}, \quad \text{comp}(b) = \{a, c\}, \quad \text{comp}(c) = \{a, b\}$$

y en N_5

$$\text{comp}(0) = \{1\}, \quad \text{comp}(1) = \{0\}, \quad \text{comp}(a) = \{b, c\}, \quad \text{comp}(b) = \{a\}, \quad \text{comp}(c) = \{a\}.$$

Por lo tanto M_3 y N_5 son retículos complementados. ■

Ejemplo 3.5.10. Sea $X \neq \emptyset$. El retículo acotado $(\mathcal{P}(X), \cup, \cap, X, \emptyset)$ es complementado. En efecto, dado $B \in \mathcal{P}(X)$, $B^c = X - B$ verifica $B \cup B^c = X (= 1)$ y $B \cap B^c = \emptyset (= 0)$.

Observemos que existen muchos subconjuntos de X que verifican estas dos condiciones por separado, pero B^c es el único que las satisface simultáneamente. La función $(\cdot)^c$ que a cada subconjunto de X le asocia su complemento es en este caso la única que hace de $(\mathcal{P}(X), \subseteq)$ un retículo complementado. ■

Lema 3.5.11. Sean $(L, \preceq_L) = (L, \vee_L, \wedge_L)$ y $(L', \preceq_{L'}) = (L', \vee_{L'}, \wedge_{L'})$ retículos complementados. Entonces:

1. El retículo dual L^* es complementado. Más aún, dado $a \in L$ resulta que b es un complemento de a en L si y sólo si b es un complemento de a en L^* .
2. $(L \times L', \preceq_{\text{prod}}) = (L \times L', \vee_{\text{prod}}, \wedge_{\text{prod}})$ es complementado.

Demostración. El punto 1 es inmediato y dejamos los detalles como **ejercicio**.

Probemos el punto 2. Observemos que, al ser complementados, L y L' son retículos acotados. Denotemos por 1_L y $1_{L'}$ los máximos de L y L' respectivamente, y por 0_L y $0_{L'}$ los mínimos de L y L' respectivamente. Por el Lema 3.5.5, $L \times L'$ es un retículo acotado con máximo $1_{L \times L'} = (1_L, 1_{L'})$ y mínimo $0_{L \times L'} = (0_L, 0_{L'})$.

Sea $(a, b) \in L \times L'$ y sean a^c y b^c un complemento de a y b en L y L' respectivamente. Entonces (ver Ejemplo 3.2.7)

$$(a, b) \vee_{\text{prod}} (a^c, b^c) = (a \vee_L a^c, b \vee_{L'} b^c) = (1_L, 1_{L'}) = 1_{L \times L'}$$

y de manera análoga $(a, b) \wedge_{\text{prod}} (a^c, b^c) = 0_{L \times L'}$. Luego (a^c, b^c) es un complemento de (a, b) en $L \times L'$, y por lo tanto $L \times L'$ es complementado. □

Ejemplo 3.5.12. Consideremos el retículo $\mathbf{2}^n$ definido en el Ejemplo 3.2.9. Entonces como $\mathbf{2}$ es claramente acotado y complementado (sus dos únicos elementos son el mínimo y el máximo), $\mathbf{2}^n$ resulta un retículo acotado y complementado, de modo tal que $0_{\mathbf{2}^n} = (0, \dots, 0)$, $1_{\mathbf{2}^n} = (1, \dots, 1)$ y si ponemos

$$\bar{\varepsilon} = \begin{cases} 1 & \text{si } \varepsilon = 0 \\ 0 & \text{si } \varepsilon = 1 \end{cases}$$

para cada $\varepsilon \in \mathbf{2}$, entonces

$$(\varepsilon_1, \dots, \varepsilon_n)^c = (\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n).$$

■

Teorema 3.5.13. Sean $(L, \preceq_L) = (L, \vee, \wedge)$ y $(S, \preceq_S) = (S, \tilde{\vee}, \tilde{\wedge})$ retículos y $f : L \rightarrow S$ un isomorfismo de retículos. Entonces:

1. L es un retículo acotado si y sólo si S es un retículo acotado. En ese caso, si $1_L, 0_L, 1_S, 0_S$ son el máximo y el mínimo de L y S respectivamente, entonces debe ser $0_S = f(0_L)$ y $1_S = f(1_L)$.
2. Para cada $x \in L$, $\text{comp}(f(x)) = f(\text{comp}(x))$.
3. L es un retículo complementado si y sólo si S es un retículo complementado.

Demostración. El punto 1 es inmediato del Teorema 2.5.15.

Veamos el punto 2. Sea $x \in L$ y sea $y \in \text{comp}(x)$. Entonces $x \vee y = 1_L$ y $x \wedge y = 0_L$, y como f es un isomorfismo de retículos resulta

$$f(x) \tilde{\vee} f(y) = f(x \vee y) = f(1_L) = 1_S, \quad y \quad f(x) \tilde{\wedge} f(y) = f(x \wedge y) = f(0_L) = 0_S.$$

Concluimos que $f(y) \in \text{comp}(f(x))$, y por lo tanto $f(\text{comp}(x)) \subseteq \text{comp}(f(x))$.

Si ahora $w \in \text{comp}(f(x))$, sea $z \in L$ el único elemento tal que $f(z) = w$. Entonces

$$f(z \vee x) = f(z) \tilde{\vee} f(x) = w \tilde{\vee} f(x) = 1_S = f(1_L)$$

y como f es biyectiva, debe ser $z \vee x = 1_L$. De manera análoga se prueba que $z \wedge x = 0_L$, y por lo tanto $z \in \text{comp}(x)$. Como $w = f(z)$, resulta $w \in f(\text{comp}(x))$, de donde $\text{comp}(f(x)) \subseteq f(\text{comp}(x))$ lo que concluye la prueba de 2.

El punto 3 es inmediato del punto 2 y de la Observación 3.5.7. □

Observación 3.5.14. Si L y S son retículos acotados y $f : L \rightarrow S$ es un morfismo de retículos, no necesariamente $f(0_L) = 0_S$ y $f(1_L) = 1_S$. Consideremos por ejemplo $X = \{1, 2, 3\}$ y $f : (\mathcal{P}(X), \subseteq) \rightarrow (\mathcal{P}(X), \subseteq)$ tal que $f(A) = \{1\}$ para cada $A \in \mathcal{P}(X)$. Es inmediato verificar que f es un morfismo de retículos, pero el top y el bottom del codominio ni siquiera pertenecen a la imagen de f .

Cuando $f : L \rightarrow S$ es un morfismo entre retículos acotados tal que sí vale que $f(0_L) = 0_S$ y $f(1_L) = 1_S$, f suele denominarse un **morfismo**- $\{0, 1\}$.

Ejemplo 3.5.15. Consideremos para $n \in \mathbb{N}$ fijo, el retículo acotado $(D_n, |)$, donde $\top = n$ y $\perp = 1$. Supongamos que $n = p_1 p_2 \cdots p_l$ con p_i números primos distintos dos a dos. Por el Ejercicio 14 de este capítulo, $(D_n, |)$ es isomorfo a $(\mathcal{P}(I_l), \subseteq)$, donde $I_l = \{1, 2, \dots, l\}$. Luego por el Teorema 3.5.13, $(D_n, |)$ es un retículo complementado.

Analicemos ahora qué ocurre para el resto de los D_n . Por el Teorema Fundamental de la Aritmética (Teorema podemos descomponer a n en factores primos. Supongamos que

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

es una descomposición en factores primos de n , y es tal que $n_j \geq 2$ para al menos un $j \in \{1, \dots, k\}$. Entonces cualquier elemento de D_n puede tener en su descomposición en factores primos sólo a los primos p_1, \dots, p_l , elevados a potencias menores o iguales a los respectivos n_i . Sea

$$x = p_1 p_2 \cdots p_k.$$

Entonces $x \in D_n$ y $x \neq n$. Observemos que como x ya tiene en su descomposición todos los factores primos posibles que conforman los elementos de D_n , no existe ningún $y \neq 1$ tal que $\text{m.c.d.}(x, y) = 1$ (pues si $y \neq 1$ es divisor de n , debe compartir al menos un factor primo con x). Es decir, el único elemento y tal que $x \wedge y = 1$ es $y = 1$. Pero en este caso, $x \vee y = x \neq n$, con lo cual x no tiene ningún complemento en D_n . Concluimos que D_n no es un retículo complementado. ■

3.6. Retículos distributivos y modulares

Definición 3.6.1. Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Decimos que L es un **retículo distributivo** si para cada $x, y, z \in L$ se verifican:

$$(3.6) \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$(3.7) \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

Observación 3.6.2. Cuando dos operaciones en un conjunto verifican propiedades como 3.6 o 3.7 se dice que una es distributiva respecto de la otra. Por ejemplo, en \mathbb{R} , el producto es distributivo respecto de la suma, dado que si en 3.6 reemplazamos \vee por \cdot y \wedge por $+$, entonces la ecuación sigue valiendo, esto es $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$. Observemos que para estos reemplazos, 3.7 no vale, es decir, la suma no es distributiva respecto del producto. De estas consideraciones, un retículo es distributivo si y sólo si \vee es distributiva respecto de \wedge y \wedge es distributiva respecto de \vee .

Observación 3.6.3. Observemos que en un retículo cualquiera se verifican

$$(3.8) \quad x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z), \quad (x \wedge y) \vee (x \wedge z) \preceq x \wedge (y \vee z)$$

cualesquiera sean $x, y, z \in L$.

En efecto, $x \preceq x \vee y$ y $x \preceq x \vee z$, con lo cual x es una cota inferior de $\{x \vee y, x \vee z\}$ y por lo tanto $x \preceq (x \vee y) \wedge (x \vee z)$.

De la misma manera, $y \wedge z \preceq y \preceq x \vee y$, $y \wedge z \preceq z \preceq x \vee z$. Luego $y \wedge z$ también es una cota inferior de $\{x \vee y, x \vee z\}$ y entonces $y \wedge z \preceq (x \vee y) \wedge (x \vee z)$.

Pero entonces $(x \vee y) \wedge (x \vee z)$ es una cota superior de $\{x, y \wedge z\}$, con lo cual $x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z)$.

La prueba de la otra comparación es similar y se deja como **ejercicio**. Luego L es un retículo distributivo cuando en 3.8 vale la igualdad en ambas condiciones.

La prueba del siguiente resultado es inmediata de la definición 3.6.1 y del principio de inducción. Dejamos los detalles como **ejercicio**.

Lema 3.6.4. Sea L un retículo distributivo y sean $x_1, \dots, x_n, y \in L$. Entonces:

$$y \vee (x_1 \wedge x_2 \wedge \dots \wedge x_n) = (y \vee x_1) \wedge (y \vee x_2) \wedge \dots \wedge (y \vee x_n)$$

$$y \wedge (x_1 \vee x_2 \vee \dots \vee x_n) = (x_1 \wedge y) \vee (x_2 \wedge y) \vee \dots \vee (x_n \wedge y).$$

Ejemplo 3.6.5. Si $X \neq \emptyset$, $(\mathcal{P}(X), \cup, \cap)$ es un retículo distributivo, pues las operaciones \cup y \cap verifican las propiedades (3.6) y (3.7). ■

Observación 3.6.6. Si (L, \vee, \wedge) es un retículo distributivo, es inmediato que su dual $L^* = (L, \wedge, \vee)$ es un retículo distributivo. En efecto, la propiedad (3.6) para L se transforma en la propiedad (3.7) para L^* , y la propiedad (3.7) para L se transforma en la propiedad (3.6) para L^* . ■

Teorema 3.6.7. *Si un retículo L satisface una de las propiedades (3.6) o (3.7) entonces satisface la otra, y por lo tanto es distributivo.*

Demostración. Supongamos primero que L satisface la ecuación (3.7) y veamos que entonces debe satisfacer (3.6). En efecto,

$$\begin{aligned}
 (x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) && [\text{por (3.7)}] \\
 &= x \vee (z \wedge (x \vee y)) && [\text{Teo. 3.2.4: conmutatividad de } \wedge, \text{ absorción}] \\
 &= x \vee ((z \wedge x) \vee (z \wedge y)) && [\text{por (3.7)}] \\
 &= (x \vee (z \wedge x)) \vee (z \wedge y) && [\text{Teo 3.2.4: asociatividad de } \vee] \\
 &= x \vee (y \wedge z) && [\text{Teo 3.2.4: abosorsción, conmutatividad de } \wedge]
 \end{aligned}$$

Observemos que en el dual L^* las ecuaciones (3.6) y (3.7) se intercambian. Luego, como el dual de un retículo distributivo es distributivo, la prueba anterior aplicada a L^* prueba que (3.6) implica (3.7). \square

Ejemplo 3.6.8. Todo conjunto totalmente ordenado es un retículo distributivo. En efecto, si (L, \preceq) es totalmente ordenado,

$$x \wedge y = \max\{x, y\} = \begin{cases} x & \text{si } y \preceq x \\ y & \text{si } x \preceq y \end{cases}, \quad x \vee y = \min\{x, y\} = \begin{cases} x & \text{si } x \preceq y \\ y & \text{si } y \preceq x \end{cases}$$

Para ver que L es un retículo distributivo, por el Teorema 3.6.7 basta probar que se verifica la ecuación (3.6), que en este caso es

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}$$

Si $x, y, z \in L$, son comparables dos a dos así que necesariamente debe verificarse $x \preceq y \preceq z$ o alguna de sus permutaciones. Supondremos que valen estas relaciones y dejamos las otras como ejercicio (hay que analizar 9 casos). Tenemos entonces:

$$\max\{x, \min\{y, z\}\} = \max\{x, y\} = y, \quad \min\{\max\{x, y\}, \max\{x, z\}\} = \min\{y, z\} = y$$

como queríamos probar.

En particular, los conjuntos numéricos \mathbb{N} , \mathbb{Z} , \mathbb{Q} y \mathbb{R} con la relación \leq son retículos distributivos y los retículos $(D_n, |)$ con $n = p^k$, p primo, $k \in \mathbb{N}$, son distributivos. \blacksquare

El siguiente resultado es inmediato. Dejamos los detalles de la prueba como **ejercicio**.

Lema 3.6.9. *Sean L y L' retículos y sea S un subretículo de L . Entonces:*

1. *Si L es distributivo entonces S es distributivo.*
2. *Si L y L' son distributivos, entonces $L \times L'$ son distributivos.*

Ejemplo 3.6.10. El retículo $(\mathbf{2}, \oplus, \odot)$ del Ejemplo 3.2.9 es trivialmente distributivo. Por lo tanto $\mathbf{2}^n$ es un retículo distributivo. \blacksquare

Teorema 3.6.11. Sean L y S retículos y sea $f : L \rightarrow S$ un homomorfismo de retículos. Entonces:

1. Si L es un retículo distributivo, entonces $f(L)$ es un retículo distributivo.
2. Si f es un isomorfismo, L es distributivo si y sólo si S es un retículo distributivo.

Demostración. Sea $f : L \rightarrow S$ un homomorfismo de retículos y supongamos que L es distributivo. Vimos en el Teorema 3.4.18 que $f(L)$ es un subretículo de S , y por lo tanto es en particular un retículo cuyo join y meet coinciden con el join y el meet de S .

Sean $u, v, w \in f(L)$ y sean $x, y, z \in L$ tales que $f(x) = u$, $f(y) = v$ y $f(z) = w$. Entonces

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

por lo tanto $f(L)$ es distributivo.

Si ahora f es un isomorfismo, si L es distributivo, $S = f(L)$ es distributivo. Y si S es distributivo, como $f^{-1} : S \rightarrow L$ también es un isomorfismo, entonces $L = f^{-1}(S)$ es distributivo. \square

Ejemplo 3.6.12. Consideremos el retículo $(D_n, |)$ para $n = p_1 p_2 \cdots p_l$ con $p_1, \dots, p_l \in \mathbb{N}$ números primos distintos dos a dos. Entonces si $I_l = \{1, \dots, l\}$, $(D_n, |)$ es un retículo isomorfo a $(\mathcal{P}(I_l), \subseteq)$ (ver Ejercicio 14 de este capítulo). Como este último es distributivo, resulta del Teorema 3.6.11 que $(D_n, |)$ es distributivo.

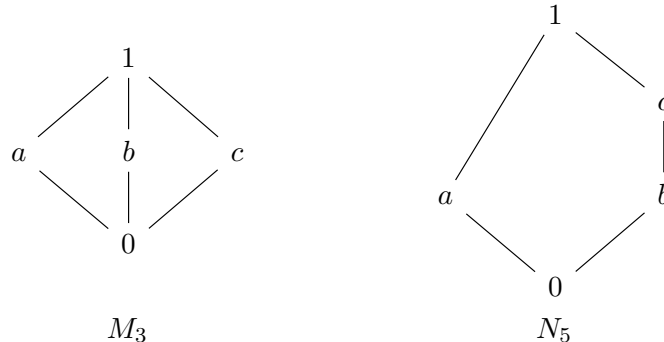
Dejamos como ejercicio (intentar) probar que en realidad todos los retículos $(D_n, |)$ son distributivos. Observemos que para ello debemos probar que dados $x, y, z \in D_n$,

$$\text{m. c. m.}(x, \text{m. c. d.}(y, z)) = \text{m. c. d.}(\text{m. c. m.}(x, y), \text{m. c. m.}(x, z))$$

$$\text{m. c. d.}(x, \text{m. c. m.}(y, z)) = \text{m. c. m.}(\text{m. c. d.}(x, y), \text{m. c. d.}(x, z)).$$

Resulta evidente que esta prueba es más complicada que apelar al isomorfismo anterior, pero hasta el momento no hemos visto que D_n sea isomorfo a ningún retículo distributivo para un n genérico. Veremos más adelante un criterio general que nos permitirá dar una prueba relativamente simple para todos los casos. \blacksquare

Ejemplo 3.6.13. Consideremos los retículos M_3 y N_5 (ver Ejemplo 3.1.3) cuyos diagramas de Hasse son los siguientes:



En M_3 tenemos por ejemplo

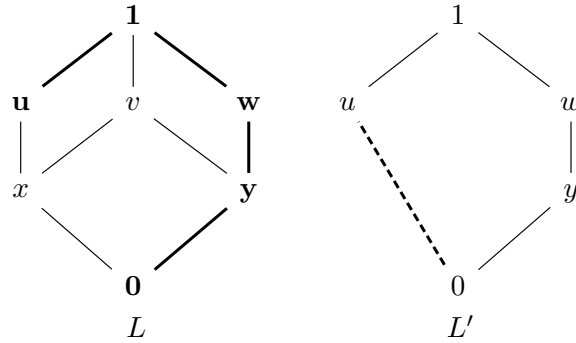
$$a \wedge (b \vee c) = a \wedge 1 = a, \quad (a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$$

y en N_5 ,

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

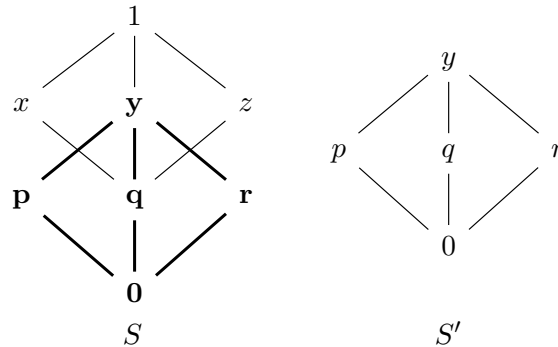
Por lo tanto ninguno de los dos retículos es distributivo. ■

Ejemplo 3.6.14. Consideremos $L = \{0, x, y, u, v, w, 1\}$ con el orden \preceq cuyo diagrama de Hasse es



y sea $L' = \{0, u, y, w, 1\} \subseteq L$. Entonces es fácil ver que L' es un subretículo de L , isomorfo a N_5 . Luego, por el Teorema 3.6.11, L' no es distributivo. Como por el Teorema 3.6.9 todo subretículo de un retículo distributivo es distributivo, concluimos que L no puede ser distributivo.

Consideremos ahora el retículo $S = \{0, p, q, r, x, y, z, 1\}$ cuyo diagrama de Hasse es el siguiente



Es fácil verificar que $S' = \{0, p, q, r, y\}$ es un subretículo de S , claramente isomorfo a M_3 . Con el mismo argumento de antes, si S fuese distributivo, todo subretículo de S debería ser distributivo, lo que no puede ocurrir, pues S tiene un subretículo isomorfo a M_3 . Luego S no es distributivo. ■

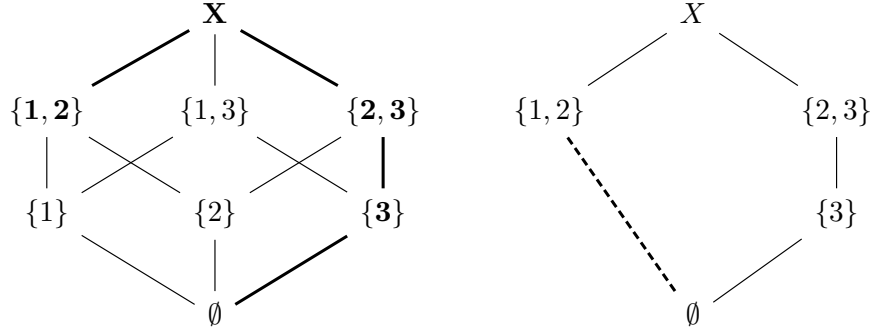
Los argumentos del Ejemplo 3.6.14 pueden generalizarse para probar el siguiente resultado. Dejamos los detalles de la prueba como **ejercicio**.

youtube

Lema 3.6.15. Sea L un retículo. Si L es distributivo, entonces L no contiene ningún subretículo isomorfo a M_3 o N_5 .

La recíproca del Lema 3.6.15 también es cierta y constituye un resultado muy importante, denominado *Teorema $M_3 - N_5$* . Lo probaremos más adelante.

Ejemplo 3.6.16. Consideremos $X = \{1, 2, 3\}$ y el retículo $L = (\mathcal{P}(X), \subseteq)$. Sea $L' = \{\emptyset, \{3\}, \{1, 2\}, \{2, 3\}, X\}$.



L es un retículo distributivo, y L' es un retículo isomorfo a M_5 , contenido en L . ¿Por qué este ejemplo no contradice el Lema 3.6.15? Simplemente porque L' NO es un subretículo de L . ■

Teorema 3.6.17. *Sea L un retículo distributivo y acotado. Entonces todo elemento de L tiene a lo sumo un elemento complementario.*

Demostración. Sea $x \in L$ y supongamos que x tiene dos elementos complementarios y, y' . Esto es, existen $y, y' \in L$ tales que

$$x \vee y = x \vee y' = 1, \quad x \wedge y = x \wedge y' = 0.$$

Además, para cada $z \in L$ se verifican $z \vee 1 = 1$, $z \wedge 1 = z$, $z \wedge 0 = 0$, $z \vee 0 = z$. Luego, como L es distributivo,

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

de donde $y \preceq y'$. Con el mismo argumento, $y' = y' \wedge y$ y por lo tanto $y' \preceq y$. Luego $y = y'$. □

Corolario 3.6.18. *Sea L un retículo complementado y distributivo. Entonces el complemento de cada elemento de L es único.*

Ejemplo 3.6.19. Aplicando el Corolario 3.6.18 podemos dar una prueba alternativa sencilla de que M_3 y N_5 no son distributivos. En efecto, vimos en el Ejemplo 3.5.9 que M_3 y N_5 son complementados, pero en ambos casos hay elementos que tienen más de un complemento. Por lo tanto no pueden ser retículos distributivos. ■

Dedicaremos el resto de esta sección a demostrar la recíproca del Lema 3.6.15. Para ello debemos introducir previamente una condición más relajada que la noción de distributividad de un retículo:

Definición 3.6.20. *Un retículo $(L, \preceq) = (L, \vee, \wedge)$ se dice **modular** si para cada $a, b, c \in L$ se verifica:*

$$(3.9) \quad a \preceq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c.$$

Observación 3.6.21. *Observemos que por la propiedad de absorción, la condición (3.9) se verifica trivialmente para cualquier retículo si $a = c$. Luego para probar que un retículo es modular bastará demostrar que vale (3.9) cuando $a \prec c$.*

Observación 3.6.22. *Observemos que en un retículo L cualquiera, si $a \preceq c$, entonces para cada $b \in L$ se verifica*

$$(3.10) \quad a \vee (b \wedge c) \preceq (a \vee b) \wedge c.$$

En efecto, como $a \preceq c$ y $a \preceq a \vee b$, resulta que a es una cota inferior de $\{a \vee b, c\}$ y por lo tanto

$$a \preceq \inf\{a \vee b, c\} = (a \vee b) \wedge c.$$

Por otra parte, $b \wedge c \preceq b \preceq a \vee b$ y $b \wedge c \preceq c$, con lo cual $b \wedge c$ es una cota inferior de $\{a \vee b, c\}$ y entonces

$$b \wedge c \preceq \inf\{a \vee b, c\} = (a \vee b) \wedge c.$$

Pero entonces $(a \vee b) \wedge c$ es una cota superior de $\{a, b \wedge c\}$ y por lo tanto

$$a \vee (b \wedge c) = \sup\{a, b \wedge c\} \preceq (a \vee b) \wedge c$$

como queríamos ver.

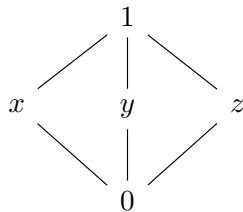
Un retículo es modular cuando en (3.10) (que se verifica en cualquier retículo) vale la igualdad.

Nuevamente, de las definiciones de modularidad y de homomorfismos de retículos, los siguientes resultados son inmediatos. Dejamos la prueba como **ejercicio**.

Teorema 3.6.23. *Sean L y S retículos y $f : L \rightarrow S$ un homomorfismo de retículos. Entonces:*

1. *Si L es modular, entonces $f(L)$ es un retículo modular.*
2. *Si f es un isomorfismo, entonces L es modular si y sólo si S es modular.*
3. *Si L es un retículo modular, cualquier subretículo de L es modular.*
4. *Si L es modular, entonces su dual L^* es modular.*

Ejemplo 3.6.24. Consideremos el retículo M_3 ,



Supongamos que $c = 1$. Para cualquier $m \in M_3$, $m \wedge c = m$, luego se verifica trivialmente la condición

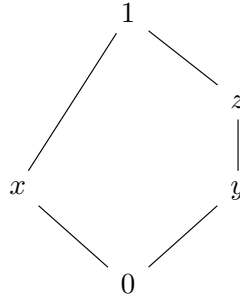
$$a \vee (b \wedge c) = a \vee b = (a \vee b) \wedge c$$

De manera análoga, si $a = 0$, para cualquier $m \in M_3$ $a \vee m = m$, con lo cual

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

Si ahora elegimos $a, c \in M_3$ tales que $a \prec c$, tendremos necesariamente que $c = 1$ o $a = 0$. Luego M_3 es modular. ■

Ejemplo 3.6.25. Consideremos ahora el retículo N_5 :



En este caso, tomando $a = y$, $c = z$ tenemos que $a \prec c$ y si tomamos $b = x$ tendremos que

$$(a \vee b) \wedge c = (y \vee x) \wedge z = 1 \wedge z = z, \quad a \vee (b \wedge c) = y \vee (x \wedge z) = y \vee 0 = y \neq z$$

luego N_5 no es modular. ■

Teorema 3.6.26. *Todo retículo distributivo es modular.*

Demostración. Sea L un retículo distributivo y sean $a, b, c \in L$ tales que $a \preceq c$. Como L es distributivo,

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

Pero como $a \preceq c$, $a \vee c = c$, con lo cual

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

como queríamos ver. □

Observación 3.6.27. *Observemos que M_5 es un retículo modular que no es distributivo. Luego la recíproca del Teorema 3.6.26 es falsa.*

Teorema 3.6.28. *Sea L un retículo. L es modular si y sólo si no tiene ningún subretículo isomorfo a N_5 .*

Demostración. Probaremos la siguiente proposición equivalente: L es un retículo no modular si y sólo si L tiene un subretículo isomorfo a N_5 .

Ya hemos visto en el Ejemplo 3.6.25 que N_5 no es modular. Supongamos que L es un retículo que tiene un subretículo L' isomorfo a N_5 . Si L fuese modular, por el Teorema 3.6.23 L' debería ser modular. Pero por ese mismo resultado, como L' es isomorfo a N_5 , N_5 debería ser modular, lo que no ocurre. Luego L no es modular.

Probaremos ahora que si L no es modular, L debe tener un subretículo isomorfo a N_5 .

Sea entonces L un retículo que no es modular, es decir, existen $a, b, c \in L$ tales que $a \preceq c$ pero $a \vee (b \wedge c) \neq (a \vee b) \wedge c$. Pongamos

$$u = a \vee (b \wedge c), \quad v = (a \vee b) \wedge c$$

Vimos en la Observación 3.6.22 que en cualquier retículo $u \preceq v$. Luego si $u \neq v$, debe verificarse

$$(3.11) \quad u \prec v.$$

Observemos ahora que b no es comparable con u ni con v . En efecto,

$$(3.12) \quad b \vee u = b \vee (a \vee (b \wedge c)) = (b \vee a) \vee (b \wedge c) = b \vee a$$

$$(3.13) \quad v \wedge b = ((a \vee b) \wedge c) \wedge b = (a \vee b) \wedge (b \wedge c) = b \wedge c$$

dado que $b \wedge c \preceq b \preceq b \vee a$.

Supongamos que b es comparable con u . Si $b \preceq u$, entonces $b \vee u = u$. Luego de (3.12), $u = b \vee a$ y

$$v = (a \vee b) \wedge c \preceq a \vee b = u$$

lo que contradice (3.11). Si fuese $u \preceq b$, entonces $b \vee u = b$. Luego de (3.12) $b = b \vee a$, de donde $a \preceq b$. Recordemos que además $a \preceq c$ por hipótesis, con lo cual a es una cota inferior de $\{b, c\}$ y por lo tanto $a \preceq b \wedge c$. Luego

$$u = a \vee (b \wedge c) = b \wedge c \stackrel{(3.13)}{=} v$$

lo que también contradice 3.11.

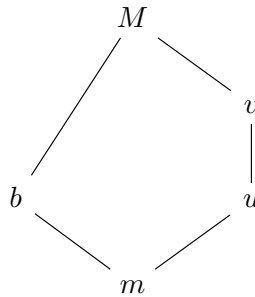
Concluimos que u y b no son comparables. Con un razonamiento similar puede probarse que b y v no son comparables (dejamos los detalles como **ejercicio**).

Veremos que b, u y v son los nodos “intermedios” de un subretículo de L isomorfo a N_5 .

Pongamos

$$m = b \wedge u \quad \text{y} \quad M = b \vee v.$$

Como b no es comparable con u , resulta $m \prec b$ y $m \prec u$. Como además $u \prec v$, resulta $m \prec v$. Con el mismo argumento, tendremos $b \prec M$, $u \prec M$, $v \prec M$ y por lo tanto $m \prec M$. Luego si $L' = \{m, b, u, v, M\}$, el diagrama de Hasse de $(L', \preceq_{|L'})$ es



Observemos que $(L', \preceq_{|L'})$ es trivialmente un retículo isomorfo a N_5 y $L' \subseteq L$, pero no hemos probado aún que L' sea un subretículo de L .

A partir de las definiciones de m, b, u, v y M es inmediato observar que si $s, t \in L'$ entonces $s \wedge t \in L'$ y $s \vee t \in L'$ para casi todos los posibles valores de s y t , a excepción de $b \wedge v$ y $b \vee u$. Luego lo único que nos resta probar para ver que L' es un subretículo de L es que

$$b \wedge v = m \in L' \quad \text{y} \quad b \vee u = M \in L'$$

Ahora bien, como $u \prec v$, del Teorema 3.2.4 tenemos que

$$(3.14) \quad m = u \wedge b \preceq v \wedge b$$

Por otra parte,

$$(3.15) \quad b \wedge v \stackrel{(3.13)}{=} b \wedge c = b \wedge (b \wedge c) \stackrel{(*)}{\preceq} b \wedge (a \vee (b \wedge c)) = b \wedge u = m,$$

donde $(*)$ vale por el Teorema 3.2.4, dado que $b \wedge c \preceq a \vee (b \wedge c)$.

De (3.14) y (3.15) tenemos que $v \wedge b = m$ como queríamos ver. De manera similar se prueba que $b \vee u = M$. Dejamos los detalles como **ejercicio**. \square

Teorema 3.6.29 (Teorema M_3 - N_5). *Sea L un retículo. Entonces L es distributivo si y sólo si L no contiene ningún subretículo isomorfo a M_3 o a N_5 .*

Demostración. Ya vimos en el Lema 3.6.15 que si L es distributivo, entonces L no tiene ningún subretículo isomorfo a M_3 o a N_5 .

Supongamos ahora que L no tiene ningún subretículo isomorfo a M_3 o N_5 . Entonces por el Teorema 3.6.28 L es modular. Supongamos que L no es distributivo. Por la observación 3.6.3 y el Teorema 3.6.7 deben existir $d, e, f \in L$ tales que

$$(3.16) \quad (d \wedge e) \vee (d \wedge f) \prec d \wedge (e \vee f).$$

Construiremos con estos elementos un subretículo de L isomorfo a M_3 , lo que nos conducirá a un absurdo. Pongamos

$$\begin{aligned} p &:= (d \wedge e) \vee (e \wedge f) \vee (f \wedge d), \\ q &:= (d \vee e) \wedge (e \vee f) \wedge (f \vee d), \\ u &:= (d \wedge q) \vee p, \\ v &:= (e \wedge q) \vee p, \\ w &:= (f \wedge q) \vee p. \end{aligned}$$

Sea $L' = \{p, q, u, v, w\}$. Observemos que por la propiedad de absorción (Teorema 3.2.4) resulta

$$p = u \wedge p = v \wedge p = w \wedge p$$

y en particular, $p \preceq u$, $p \preceq v$, $p \preceq w$. Además, del Ejercicio 6 de este capítulo, resulta $p \preceq q$. Luego del Teorema 3.2.4, tenemos

$$u = (d \wedge q) \vee p \preceq (d \wedge q) \vee q = q.$$

y de manera análoga, $v \preceq q$, $w \preceq q$.

Probaremos que L' es un subretículo de L isomorfo a M_3 . Como L es modular, dados $a, b, c \in L$ vale (3.9), condición que a lo largo de esta prueba denotaremos por (M). Es decir, si $a \preceq c$ entonces

$$(M) \quad a \vee (b \wedge c) = (a \vee b) \wedge c$$

Aplicaremos reiteradamente esta propiedad, indicando en cada caso qué elementos juegan el rol de a , b y c . Aplicaremos también repetidamente las propiedades asociativa y conmutativa de $\vee \wedge$ sin mencionarlas. Finalmente, indicaremos con “abs” cada vez que apliquemos alguna de las propiedades de absorción del Teorema 3.2.4.

Veamos primero que $p \prec q$. Observemos que $d \wedge e \preceq d$ y $f \wedge d \preceq d$, con lo cual $(d \wedge e) \vee (f \wedge d) \preceq d$. Luego:

$$\begin{aligned}
 p \wedge d &= \underbrace{((d \wedge e) \vee (f \wedge d))}_a \vee \underbrace{(e \wedge f)}_b \wedge \underbrace{d}_c \\
 &\stackrel{(M)}{=} ((d \wedge e) \vee (f \wedge d)) \vee ((e \wedge f) \wedge d) \\
 &= (f \wedge d) \vee ((d \wedge e) \vee ((d \wedge e) \wedge f)) \\
 &\stackrel{abs}{=} (f \wedge d) \vee (d \wedge e) \\
 &\stackrel{(3.16)}{\prec} d \wedge (e \vee f)
 \end{aligned}$$

Por otra parte

$$\begin{aligned}
 q \wedge d &= (d \vee e) \wedge (e \vee f) \wedge ((f \vee d) \wedge d) \\
 &\stackrel{abs}{=} (d \vee e) \wedge (e \vee f) \wedge d \\
 &= ((d \vee e) \wedge d) \wedge (e \vee f) \\
 &\stackrel{abs}{=} d \wedge (e \vee f).
 \end{aligned}$$

Por lo tanto $p \wedge d \neq q \wedge d$ y entonces $p \neq q$. Luego deberá ser $p \prec q$ como queríamos ver.

Veamos ahora que $u \wedge v = p$. En efecto:

$$u \wedge v = \underbrace{p}_a \vee \underbrace{(d \wedge q)}_b \wedge \underbrace{((e \wedge q) \vee p)}_c \stackrel{(M)}{=} p \vee ((d \wedge q) \wedge ((e \wedge q) \vee p))$$

Por otro lado

$$\begin{aligned}
 (d \wedge q) \wedge ((\underbrace{e}_b \wedge \underbrace{q}_c) \vee \underbrace{p}_a) &\stackrel{(M)}{=} (d \wedge q) \wedge ((e \vee p) \wedge q) \\
 &= \underbrace{((d \wedge q) \wedge q)}_{\preceq q} \wedge (e \vee p) \\
 &= (d \wedge q) \wedge (e \vee p)
 \end{aligned}$$

Por lo tanto

$$(3.17) \quad u \wedge v = p \vee ((d \wedge q) \wedge (e \vee p))$$

Ya vimos que $d \wedge q = d \wedge (e \vee f)$. Ahora

$$\begin{aligned} e \vee p &= e \vee (d \wedge e) \vee (e \wedge f) \vee (f \wedge d) \\ &\stackrel{abs}{=} e \vee (e \wedge f) \vee (f \wedge d) \stackrel{abs}{=} e \vee (f \wedge d) \end{aligned}$$

Luego

$$\begin{aligned} (d \wedge q) \wedge (e \vee p) &= (d \wedge (e \vee f)) \wedge (e \vee (f \wedge d)) \\ &= d \wedge (\underbrace{(e \vee f)}_c \wedge (\underbrace{e}_a \vee \underbrace{(f \wedge d)}_b)) \\ &\stackrel{(M)}{=} d \wedge (e \vee ((e \vee f) \wedge (f \wedge d))) \\ &\stackrel{abs}{=} \underbrace{d}_c \wedge (\underbrace{e}_b \vee \underbrace{(f \wedge d)}_a) \\ &\stackrel{(M)}{=} (f \wedge e) \vee (f \wedge d) \end{aligned}$$

Reemplazando en (3.17), resulta

$$u \wedge v = p \vee ((f \wedge e) \vee (f \wedge d))$$

Pero $(f \wedge e) \vee (f \wedge d) \preceq (f \wedge e) \vee (f \wedge d) \vee (d \wedge e) = p$ de donde

$$u \wedge v = p$$

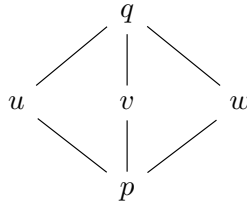
como queríamos ver. De manera completamente análoga se prueba que $u \wedge w = v \wedge w = p$ y de manera similar, que $u \vee v = u \vee w = v \vee w = q$.

Veamos ahora que u, v, w no son comparables dos a dos. Supongamos que $u \preceq v$ (los demás casos son análogos y se dejan como **ejercicio**). Entonces $u \wedge v = u$ y $u \vee v = v$. Luego debe ser $p = u$ y $q = v$. Pero por otro lado $u = p = u \wedge w$, de donde $u \preceq w$ y por lo tanto $u \vee w = w = q$. Luego $w = v = q$. Finalmente, como $v \wedge w = p$, si $v = w = q$ debería ser $p = q$, lo cual es absurdo.

Como u, v y w no son comparables, deberá ser además

$$p \prec u, p \prec v, p \prec w, u \prec q, v \prec q, w \prec q$$

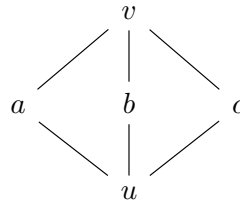
y el diagrama de Hasse de L' es



Como además $x \wedge y \in L'$ y $x \vee y \in L'$ para cada $x, y \in L'$, resulta L' un subretículo de L isomorfo a M_3 , lo que lleva a un absurdo. El absurdo proviene de suponer que L no es distributivo. Luego L es un retículo distributivo. \square

Ejemplo 3.6.30. A partir del Teorema $M_3 - N_5$ podemos probar de manera sencilla que los conjuntos totalmente ordenados son retículos distributivos (ver Ejemplo 3.6.8). En efecto, si L es totalmente ordenado y L' es un subretículo de L , entonces L' es totalmente ordenado. Como ni M_3 ni N_5 son totalmente ordenados, no pueden ser isomorfos a L' . Luego L no tiene ningún subretículo isomorfo a M_3 o N_5 y por lo tanto es distributivo. ■

Ejemplo 3.6.31. Veremos ahora que $(\mathbb{N}, |)$ es un retículo distributivo. Supongamos que $(\mathbb{N}, |)$ tiene un subretículo isomorfo a M_3 . Deberán existir entonces $a, b, c, u, v \in \mathbb{N}$ tales que si $L' = \{a, b, c, u, v\}$, el diagrama de Hasse de $(L', |)$ es



En este caso tendremos que

$$\text{m. c. d.}(a, b) = \text{m. c. d.}(a, c) = \text{m. c. d.}(b, c) = u, \quad \text{m. c. m.}(a, b) = \text{m. c. m.}(a, c) = \text{m. c. m.}(b, c) = v$$

En particular, existirán $k_1, k_2, k_3 \in \mathbb{N}$ tales que

$$a = k_1 u, \quad b = k_2 u, \quad c = k_3 u.$$

Por otra parte, del Ejercicio 13 del Capítulo 2, $ab = \text{m. c. m.}(a, b) \text{ m. c. d.}(a, b)$. Luego

$$k_1 k_2 u^2 = uv \implies v = k_1 k_2 u.$$

De manera análoga, tendremos que $v = k_1 k_3 u, v = k_2 k_3 u$. Pero entonces

$$k_1 k_2 u = k_1 k_3 u \implies k_2 = k_3 \implies b = c$$

lo cual es absurdo. Concluimos que $(\mathbb{N}, |)$ no puede tener ningún subretículo isomorfo a M_3 . De manera similar (lo dejamos como ejercicio), $(\mathbb{N}, |)$ no puede tener ningún subretículo isomorfo a N_5 , y por lo tanto $(\mathbb{N}, |)$ es distributivo.

Como cada $(D_n, |)$ es un subretículo de $(\mathbb{N}, |)$, todos estos retículos resultan distributivos. ■

3.7. Álgebras de Boole

Introduciremos en esta última sección la última de las estructuras ordenadas que estudiaremos: las *álgebras de Boole*. Haremos una presentación elemental del tema. Más detalles pueden encontrarse en [8].

Definición 3.7.1. Un retículo se denomina **un álgebra de Boole** si es complementado y distributivo.

Observación 3.7.2. Por el Teorema 3.6.17, todo elemento de un álgebra de Boole tiene un único complemento, y por lo tanto hay una única función complemento $(\cdot)^c : B \rightarrow B$ bien definida.

Notación 3.7.3. Si $(B, \preceq) = (B, \vee, \wedge)$ es un álgebra de Boole con máximo 1 y mínimo 0, usualmente la denotamos $(B, \vee, \wedge, 1, 0)$. El (único) complemento de un elemento $x \in B$ se denotará siempre por x^c .

Ejemplo 3.7.4. Consideremos el retículo $(\mathbf{2}, \oplus, \odot)$ definido en el Ejemplo 3.2.9. Entonces $\mathbf{2}^n$ es un retículo complementado (Ejemplo 3.5.12) y distributivo (Ejemplo 3.6.10), con lo cual $\mathbf{2}^n$ es un álgebra de Boole. $\mathbf{2}$ es el álgebra de Boole más pequeña (para la cual $0 \neq 1$). ■

Ejemplo 3.7.5. Hemos visto en el Ejemplo 3.6.31 que los retículos $(D_n, |)$ son todos distributivos. Sin embargo, los únicos que son complementados son los que tienen n de la forma $n = p_1 \cdots p_l$, con p_i números primos distintos dos a dos (ver Ejemplo 3.5.15). Luego $(D_n, |)$ es un álgebra de Boole si y sólo si $n = p_1 \cdots p_l$, con p_i números primos distintos dos a dos. En ese caso, $\top = n$, $\perp = 1$ y el complemento de $q = \prod_{j \in J} p_j$, con $J \subseteq \{1, \dots, l\}$ es $q^c = \prod_{j \notin J} p_j$. ■

Ejemplo 3.7.6. Si $X \neq \emptyset$, $(\mathcal{P}(X), \subseteq)$ es un álgebra de Boole (con mínimo $0 = \emptyset$, máximo $1 = X$ y $(\cdot)^c$ la función que a cada $A \subset X$ le asigna su complemento). ■

Como consecuencia de los resultados estudiados en las secciones anteriores (ver el Lema 3.5.11, la Observación 3.6.6 y el Lema 3.6.9), el siguiente resultado es inmediato:

Lema 3.7.7. Sean B y B' dos álgebras de Boole y sea B^* el retículo dual de B . Entonces:

1. B^* es un álgebra de Boole.
2. $(B \times B', \preceq_{\text{prod}})$ es un álgebra de Boole.

En el siguiente resultado reunimos las propiedades básicas de un álgebra de Boole:

Teorema 3.7.8. Sea B un álgebra de Boole con mínimo 0, máximo 1 y función complemento $(\cdot)^c$. Entonces:

1. $0^c = 1$ y $1^c = 0$;
2. para cada $x \in B$, $(x^c)^c = x$;
3. valen las **leyes de De Morgan**, esto es, para cada $x, y, z \in B$,

$$(3.18) \quad (x \vee y)^c = x^c \wedge y^c$$

$$(3.19) \quad (x \wedge y)^c = x^c \vee y^c.$$

Demostración. Las propiedades 1 y 2 son triviales, y son comunes a todos los retículos complementados donde el complemento de cada elemento sea único.

Veamos ahora que vale 3. Probaremos sólo la propiedad (3.18)

Para ver que el complemento de $x \vee y$ es $x^c \wedge y^c$, debemos probar que $(x \vee y) \vee (x^c \wedge y^c) = 1$ y que $(x \vee y) \wedge (x^c \wedge y^c) = 0$. Ahora:

$$\begin{aligned}
 (x \vee y) \vee (x^c \wedge y^c) &= ((x \vee y) \vee x^c) \wedge ((x \vee y) \vee y^c) && [\text{por ser } B \text{ distributivo}] \\
 &= ((x^c \vee x) \vee y) \vee (x \vee (y \vee y^c)) && [\text{conmutatividad, asociatividad de } \vee] \\
 &= (1 \vee y) \vee (x \vee 1) && [\text{definición de complemento}] \\
 &= 1 \vee 1 = 1
 \end{aligned}$$

La prueba de que $(x \vee y) \wedge (x^c \wedge y^c) = 0$ es análoga y se deja como ejercicio, así como la prueba de 3.19. \square

En un álgebra de Boole (B, \preceq) el orden \preceq queda completamente definido a través de las relaciones entre elementos y complementos. Más precisamente:

Lema 3.7.9. *Sea B un álgebra de Boole. Para $a, b \in B$ las siguientes afirmaciones son equivalentes:*

1. $a \preceq b$.
2. $a \wedge b^c = 0$.
3. $a^c \vee b = 1$.

Demostración. Veamos que el punto 1 implica el punto 2. Supongamos que $a \preceq b$. Entonces $a \vee b = b$. Luego, de las Leyes de De Morgan (Teorema 3.7.8) resulta

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

como queríamos ver. Aplicando las leyes de De Morgan a la igualdad en 2 obtenemos 3.

Veamos finalmente que el punto 3 implica el punto 1. Supongamos entonces que $a^c \vee b = 1$. Debemos probar que $a \wedge b = a$. Ahora, como B es distributivo, resulta:

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

como queríamos ver. \square

Como las álgebras de Boole tienen más estructura que un simple retículo, necesitamos dar una definición más adecuada tanto de subálgebra de Boole como de un morfismo de álgebras de Boole, es decir, no solo necesitamos que se preserve su estructura de retículo, sino que deben preservarse las otras propiedades que la definen.

Por ejemplo, un subretículo L' de un retículo acotado L no necesariamente es acotado. Y aunque lo fuera, y su máximo y mínimo coincidieran con el del retículo L que lo contiene, si L es complementado, L' no tiene por qué serlo (ver el Ejercicio 20). Por otra parte, como vimos en el Lema 3.6.9, si L es distributivo, entonces L' es distributivo. Definimos entonces:

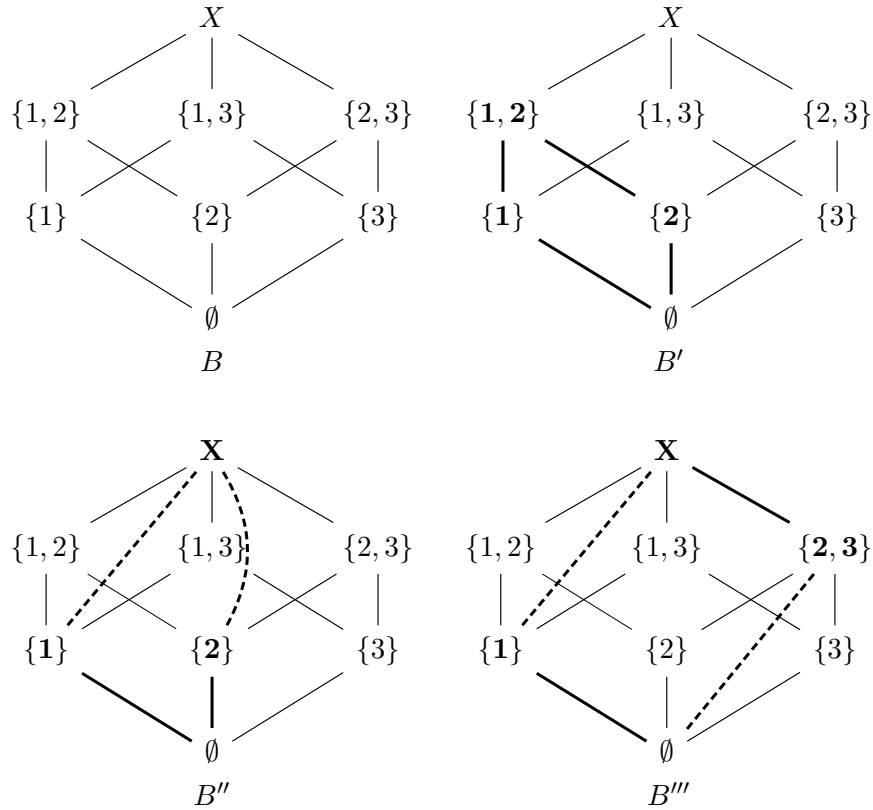
Definición 3.7.10. Sea B un álgebra de Boole y B' un subretículo de B . Decimos que B' es una subálgebra de Boole de B si:

1. $1_B \in B'$ y $0_B \in B'$ (entonces, necesariamente, 1_B y 0_B son máximo y mínimo de B');
2. Para cada $x \in B'$, $x^c \in B'$

La siguiente caracterización es inmediata. Dejamos la prueba como **ejercicio**.

Lema 3.7.11. Sea B un álgebra de Boole con máximo 1_B y mínimo 0_B y sea B' un subretículo de B . Entonces B' es una subálgebra de Boole de B si y sólo si B' es un álgebra de Boole con máximo 1_B y mínimo 0_B .

Ejemplo 3.7.12. Consideremos el álgebra de Boole $B = (\mathcal{P}(X), \subseteq)$ con $X = \{1, 2, 3\}$.



Entonces $B' = (\mathcal{P}(\{1, 2\}), \subseteq)$ es un álgebra de Boole que es un subretículo de B' pero no es subálgebra de Boole, pues $1_{B'} \neq 1_B$. Por otra parte, $B'' = (\{\emptyset, \{1\}, \{2\}, X\}, \subseteq)$ es un álgebra de Boole con $1_{B''} = 1_B$ y $0_{B''} = 0_B$, pero no es subálgebra de Boole, pues B'' no es un subretículo de B . Finalmente, $B''' = (\{\emptyset, \{1\}, \{2, 3\}, X\}, \subseteq)$ es una subálgebra de Boole de B . ■

Ejemplo 3.7.13. Consideremos los conjuntos

$$\mathcal{P}_f(\mathbb{N}) = \{A \subset \mathbb{N} : \#A < \infty\}, \quad \mathcal{P}_{cof}(\mathbb{N}) = \{A \subset \mathbb{N} : \#A^c < \infty\}.$$

$\mathcal{P}_f(\mathbb{N})$ es el conjunto de partes finitas de \mathbb{N} y $\mathcal{P}_{cof}(\mathbb{N})$ es el conjunto de partes *cofinitas* de \mathbb{N} , es decir, de aquellos subconjuntos tal que su complemento es finito.

Sea $B = \mathcal{P}_f(\mathbb{N}) \cup \mathcal{P}_{cof}(\mathbb{N})$. Entonces $B \subsetneq \mathcal{P}(\mathbb{N})$ (pues por ejemplo si A es el conjunto de números pares, $A \notin \mathcal{P}_f(\mathbb{N})$ y $A \notin \mathcal{P}_{cof}(\mathbb{N})$). Veamos que $(B, \cup, \cap, X, \emptyset)$ es un álgebra de Boole.

Comencemos probando que (B, \cup, \cap) es un subretículo de $(\mathcal{P}(\mathbb{N}), \cup, \cap)$. En efecto, si $C, D \in \mathcal{P}_f(\mathbb{N})$, entonces $C \cup D$ y $C \cap D$ son finitos y por lo tanto están en $\mathcal{P}_f(\mathbb{N}) \subset B$. Si $C, D \in \mathcal{P}_{cof}(\mathbb{N})$, entonces $C^c \cap D^c$ y $C^c \cup D^c$ son finitos, y entonces (por las Leyes de De Morgan) $C \cup D \in \mathcal{P}_{cof}(\mathbb{N})$, $C \cap D \in \mathcal{P}_{cof}(\mathbb{N})$. Finalmente, es fácil ver que si $C \in \mathcal{P}_f(\mathbb{N})$ y $D \in \mathcal{P}_{cof}(\mathbb{N})$, entonces

$$C \cup D = D \cup C \in \mathcal{P}_{cof}(\mathbb{N}), \quad C \cap D = D \cap C \in \mathcal{P}_f(\mathbb{N})$$

En cualquier caso, tenemos que si $C, D \in B$, entonces $C \cup D \in B$ y $C \cap D \in B$ como queríamos ver.

Recordemos que un subretículo de un retículo acotado no necesariamente es acotado, y lo mismo ocurre con un subretículo de un retículo complementado. En este caso, $\emptyset \in \mathcal{P}_f(\mathbb{N})$ y $X \in \mathcal{P}_{cof}(\mathbb{N})$, con lo cual B resulta acotado con el mismo máximo y mínimo que $\mathcal{P}(\mathbb{N})$. Además, es fácil ver tomando casos como antes, que si $D \in B$, entonces $D^c \in B$.

Concluimos que B es una subálgebra de Boole de $\mathcal{P}(\mathbb{N})$ ■

Algo similar al análisis que hemos hecho para definir las subálgebras de Boole ocurre cuando consideramos morfismos de retículos entre álgebras de Boole. En primer lugar, un morfismo de retículos acotados no tiene por qué ser un morfismo $\{0, 1\}$, y aunque lo fuera, a priori, no tendría por qué enviar el complemento de un elemento al complemento de su imagen. Esto motiva la siguiente:

Definición 3.7.14. Sean $(B, \vee, \wedge, 1_B, 0_B)$ y $(B', \vee', \wedge', 1_{B'}, 0_{B'})$ dos álgebras de Boole. Denotaremos por $(\cdot)^c$ la función complemento para ambas álgebras. Una función $f : B \rightarrow B'$ es un **morfismo de álgebras de Boole** si:

- f es un morfismo de retículos $\{0, 1\}$ (i.e., tal que $f(0_B) = 0_{B'}$, $f(1_B) = 1_{B'}$);
- para cada $x \in B$, $f(x^c) = f(x)^c$.

f es un **isomorfismo** de álgebras de Boole si tanto f como f^{-1} son morfismos de álgebras de Boole.

En realidad, la definición de morfismo de álgebras de Boole tiene algunas condiciones redundantes:

Teorema 3.7.15. Sean B y B' álgebras de Boole y $f : B \rightarrow B'$ un morfismo de retículos. Entonces las siguientes proposiciones son equivalentes:

1. f es un morfismo $\{0, 1\}$;
2. $f(x^c) = (f(x))^c$ para cada $x \in B$.

Por lo tanto, f es un morfismo de álgebras de Boole si y sólo si se verifica una de las condiciones 1 o 2.

Demostración. Supongamos primero que $f : B \rightarrow B'$ es un morfismo de retículos tal que $f(1_B) = 1_{B'}$ y $f(0_B) = 0_{B'}$. Sea $x \in B$ y pongamos $y = f(x)$, $y' = f(x^c)$. Entonces

$$y \vee' y' = f(x) \vee' f(x^c) = f(x \vee x^c) = f(1_B) = 1_{B'}$$

y de manera análoga $y \wedge' y' = 0_{B'}$. Luego y' es un complemento de y en B' , y como en un álgebra de Boole (al ser un retículo distributivo) el complemento es único, debe ser $y' = y^c$, esto es $f(x^c) = (f(x))^c$.

Supongamos ahora que $f(x^c) = (f(x))^c$ para cada $x \in B$. Entonces dado $x \in B$ cualquiera, tenemos

$$f(1_B) = f(x \vee x^c) = f(x) \vee' f(x^c) = 1_{B'}$$

y de manera análoga $f(0_B) = 0_{B'}$. □

Ejemplo 3.7.16. Sea B un álgebra de Boole y S una subálgebra de Boole de B . Entonces la inclusión $i : S \rightarrow B$, $i(x) = x$ es un morfismo de retículos tal que $i(1_S) = i(1_B) = 1_B$ y $i(0_S) = i(0_B) = 0_B$. Luego i es un morfismo de álgebras de Boole. ■

Teorema 3.7.17. Sean B y B' álgebras de Boole y $f : B \rightarrow B'$ una función. Si $f(x)^c = (f(x))^c$ para cada $x \in B$, entonces son equivalentes:

1. f es un morfismo de álgebras de Boole.
2. $f(x \vee y) = f(x) \vee' f(y)$ para cada $x, y \in B$.
3. $f(x \wedge y) = f(x) \wedge' f(y)$ para cada $x, y \in B$.

Demostración. Es claro que el punto 1 implica el punto 2, dado que un morfismo de álgebras de Boole es en particular un morfismo de retículos.

Veamos que el punto 2 implica el punto 3. Sean $x, y \in B$. Entonces del Teorema 3.7.8) tenemos:

$$f(x \wedge y) = f((x^c)^c \wedge (y^c)^c) = f((x^c \vee y^c)^c)$$

Recordemos que por hipótesis, para cada $z \in B$ vale que $f(z^c) = f(z)^c$. Luego, como estamos suponiendo que vale el punto 2 tenemos:

$$f((x^c \vee y^c)^c) = f(x^c \vee y^c)^c = (f(x^c) \vee' f(y^c))^c = (f(x)^c \vee' f(y)^c)^c.$$

Aplicando nuevamente el Teorema 3.7.8 resulta

$$f(x \wedge y) = (f(x)^c \vee' f(y)^c)^c = (f(x)^c)^c \wedge' (f(y)^c)^c = f(x) \wedge' f(y)$$

como queríamos ver.

Veamos finalmente que el punto 3 implica el punto 1. De manera completamente análoga a la anterior se prueba que bajo la hipótesis de que $f(z^c) = f(z)^c$ para cada $z \in B$, el punto 3 implica el punto 2. Por lo tanto f debe ser un morfismo de retículos. Luego como f verifica el punto 2 del Teorema 3.7.15, resulta que f es un morfismo de álgebras de Boole. □

Ejemplo 3.7.18. Sea $X \neq \emptyset$ un conjunto cualquiera y consideremos las álgebras de Boole $B = (\mathcal{P}(X), \subseteq)$ y $B' = \mathbf{2}$. Fijemos $x_0 \in X$ y definamos $f : B \rightarrow B'$ tal que

$$f(A) = \begin{cases} 1 & \text{si } x_0 \in A \\ 0 & \text{si } x_0 \notin A \end{cases}$$

Observemos que en $\mathbf{2}$, $0^c = 1$ y $1^c = 0$. Por otra parte si $A \in \mathcal{P}(X)$ es tal que $f(A) = 1$, es porque $x_0 \in A$, y por lo tanto $x_0 \notin CA = A^c$. Luego $f(A^c) = 0 = 1^c = f(A)^c$. Lo mismo ocurre si $f(A) = 0$.

Ahora bien, si $A, B \in \mathcal{C}$, tenemos que $x_0 \in A \cup B = A \vee B$ si y sólo si $x_0 \in A$ o $x_0 \in B$, o sea, si y sólo si $f(A) = 1$ o $f(B) = 1$. Luego

$$f(A \cup B) = 1 \iff f(A) = 1 \text{ o } f(B) = 1 \iff f(A) \vee' f(B) = 1$$

de donde $f(A \cup B) = f(A) \vee' f(B)$. Concluimos del Teorema 3.7.17 que f es un morfismo de álgebras de Boole. ■

Como consecuencia inmediata de los Teoremas 3.4.10, 3.5.13 y 3.6.11 tenemos el siguiente resultado. Dejamos los detalles de la prueba como **ejercicio**.

Teorema 3.7.19. Sean B un álgebra de Boole, B' un retículo y $f : B \rightarrow B'$ una función. Entonces:

1. Si f es un isomorfismo de retículos, entonces B' es un álgebra de Boole.
2. f es un isomorfismo de álgebras de Boole si y sólo si f es un isomorfismo de retículos.
3. f es un isomorfismo de álgebras de Boole si y sólo si f es un isomorfismo de posets.

Como los isomorfismos de álgebras de Boole son isomorfismos de retículos y viceversa, como consecuencia del Corolario 3.4.11 tenemos que:

Lema 3.7.20. Sea \mathcal{B} el conjunto de todas las álgebras de Boole y sea \sim la relación en \mathcal{B} dada por $B \sim B'$ si existe un isomorfismo de álgebras de Boole $f : B \rightarrow B'$. Entonces \sim es una relación de equivalencia.

Definición 3.7.21. Dos álgebras de Boole se dicen **isomorfas** si existe un isomorfismo de álgebras de Boole $f : B \rightarrow B'$ (y por lo tanto, existe un isomorfismo de álgebras de Boole $f^{-1} : B' \rightarrow B$).

Las propiedades de las álgebras de Boole del Teorema 3.7.8 son análogas a las propiedades de las operaciones unión, intersección y complemento de la teoría de conjuntos. Más aún, los ejemplos que vimos de álgebras de Boole finitas (Ejemplos 3.7.4 y 3.7.5) son isomorfas a algún álgebra de Boole $(\mathcal{P}(X), \subseteq)$ para un X adecuado. Cabe preguntarse si todas las álgebras de Boole son de este tipo.

Este resultado es en general falso como mostraremos en el siguiente ejemplo:

Ejemplo 3.7.22. Consideremos el álgebra de Boole $B = \mathcal{P}_f(\mathbb{N}) \cup \mathcal{P}_{cof}(\mathbb{N})$ del ejemplo 3.7.13.

Para ver que B no puede ser isomorfa a $(\mathcal{P}(X), \subseteq)$ para ningún conjunto X , basta analizar su cardinal. En efecto, es un hecho bien conocido (aunque difícil de probar) que $\mathcal{P}_f(\mathbb{N})$ y $\mathcal{P}_{cof}(\mathbb{N})$ son conjuntos infinitos numerables, es decir, su cardinal es \aleph_0 . Pero no existe ningún conjunto X tal que el cardinal de $\mathcal{P}(X)$ sea

\aleph_0 , pues si X es finito, entonces $\#\mathcal{P}(X) = 2^{\#X} \in \mathbb{N}$ y si X es infinito, debe ser al menos infinito numerable, es decir, su cardinal debe ser al menos \aleph_0 , y como es bien sabido, el cardinal de $\mathcal{P}(X)$ será al menos \aleph_1 . ■

En el caso finito sí es cierto que un álgebra de Boole B debe ser isomorfa a $(\mathcal{P}(X), \subseteq)$ para algún conjunto X (o equivalentemente, a 2^n para algún $n \in \mathbb{N}$). Antes de poder probar este resultado necesitamos introducir algunos conceptos.

Definición 3.7.23. Sea $(B, \preceq) = (B, \vee, \wedge, 1, 0)$ un álgebra de Boole. Un elemento $a \in B$ se denomina un **átomo** (o **elemento atómico**) si $a \neq 0$ y para cada $x \in B$ se verifica

$$x \preceq a \implies x = 0 \text{ o } x = a.$$

Observación 3.7.24. Observemos que un elemento a de un álgebra de Boole B es un átomo si a es un elemento minimal del poset $(B - \{0\}, \preceq_{|B-\{0\}})$.

Ejemplo 3.7.25. Las siguientes afirmaciones son inmediatas de verificar:

- En el álgebra de Boole $(\mathcal{P}(X), \subseteq)$, los átomos son los singuletes $\{x\}$ con $x \in X$.
- En $(D_n, |)$, con n un producto de primos distintos, los elementos atómicos son los divisores primos de n .
- En 2^n , $x = (\varepsilon_1, \dots, \varepsilon_n)$, con $\varepsilon_i \in \{0, 1\}$ es atómico si y sólo si $\varepsilon_j = 1$ exactamente para un índice $j \in \{1, \dots, n\}$. ■

Lema 3.7.26. Sea B un álgebra de Boole y sea $b \in B$. Entonces las siguientes afirmaciones son equivalentes:

1. a es un átomo de B .
2. Para cada $x \in B$, $a \preceq x$ o $a \wedge x = 0$, pero no ambas.
3. Para cada $x \in B$, $a \preceq x$ o $a \preceq x^c$, pero no ambas.

Demostración. Veamos que el punto 1 implica el punto 2. Supongamos que a es un átomo de B y sea $x \in B$. Si $a \preceq x$, entonces $a \wedge x = a \neq 0$. Supongamos que no ocurre que $a \preceq x$. Entonces $x \prec a$ o a y x no son comparables. En el primer caso, como a es un átomo, debe ser $x = 0$ y por lo tanto $a \wedge x = 0$. Si a y x no son comparables, entonces $b := a \wedge x \prec a$ y $b \prec x$. Nuevamente, como a es un átomo, debe ser $b = 0$.

Veamos ahora que el punto 2 implica el punto 3. Sean $a, x \in B$. Supongamos que $a \preceq x$. Entonces por hipótesis no puede ocurrir que $a \wedge x = 0$, y en particular $a \neq 0$. Como $a \preceq x$, por el Lema 3.7.9, $a \wedge x^c = 0 \neq a$, con lo cual no puede ocurrir que $a \preceq x^c$.

Supongamos ahora que no ocurre que $a \preceq x$. Entonces por hipótesis debe ser $a \wedge x = 0$, es decir, $a \wedge (x^c)^c = 0$, y por el Lema 3.7.9 resulta $a \preceq x^c$.

Veamos finalmente que el punto 3 implica el punto 1. Sea $a \in B$ un elemento que verifica el punto 3 y sea $x \in B$ tal que $x \preceq a$, es decir, $a \wedge x = x$. Si $a \neq x$, entonces no se verifica que $a \preceq x$ y por lo tanto vale

que $a \preceq x^c$. Por el Lema 3.7.9 resulta $0 = a \wedge (x^c)^c = a \wedge x = x$, es decir, $x = 0$. Concluimos que si $x \preceq a$, entonces $x = a$ o $x = 0$ y por lo tanto a es un átomo de B . \square

Lema 3.7.27. *Sea B un álgebra de Boole finita y sea $b \in B$, $b \neq 0$. Entonces existe un elemento atómico $a \in B$ tal que $a \preceq b$.*

Demostración. Si b es atómico, no hay nada que probar. Si b no es atómico, sea

$$B_b = \{x \in B - \{0\} : x \preceq b\}.$$

Por el Teorema 2.2.7 B_b tiene un elemento minimal a . Observemos que $a \in B_b$, y por lo tanto $a \preceq b$.

Veamos que a es un elemento minimal del poset $(B - \{0\}, \preceq)$. Sea $x \in B - \{0\}$ tal que $x \preceq a$. Como $a \preceq b$, resulta $x \preceq b$, o sea, $x \in B_b$, y como a es un elemento minimal de B_b , debe ser $x = a$, como queríamos probar. Sigue de la observación 3.7.24 que a es un átomo de B . \square

Lema 3.7.28. *Sea B un álgebra de Boole finita y sea $b \in B$, $b \neq 0$. Entonces b se descompone de manera única, salvo por el orden en que aparecen los elementos, en la forma*

$$(3.20) \quad b = a_1 \vee a_2 \vee \cdots \vee a_n.$$

donde $a_1, \dots, a_n \in B$ son átomos de B distintos dos a dos.

Más aún, los elementos a_i que intervienen en (3.20) son todos los elementos del conjunto

$$A_b = \{a \in B : a \text{ es un átomo de } B \text{ y } a \preceq b\}$$

y $b = \sup A_b$.

Demostración. Existencia: El conjunto A_b es finito dado que B es finito, y es no vacío por el Lema 3.7.27. Supongamos entonces que $A_b = \{a_1, \dots, a_n\}$ y pongamos

$$b' = a_1 \vee a_2 \vee \cdots \vee a_n$$

Por el Ejercicio 5 de este capítulo resulta $b' = \sup A_b$. Como b es claramente una cota superior de A_b , deberá ser $b' \preceq b$. Veamos que $b \preceq b'$. Por el Lema 3.7.9 debemos probar que

$$c := b \wedge (b')^c = 0.$$

Supongamos por el contrario que $c \neq 0$. Por el Lema 3.7.27 existirá un átomo a de B tal que $a \preceq c$. Como $c \preceq b$, en particular, $a \preceq b$ y por lo tanto $a \in A_b$. Luego existirá $j \in \{1, \dots, n\}$ tal que $a = a_j$.

Ahora bien, $a_j \preceq b' = \sup A_b$, y como $a_j \preceq c$ y $c \preceq (b')^c$, $a_j \preceq (b')^c$. Concluimos que a_j es un átomo de B tal que $a_j \preceq b'$ y $a_j \preceq (b')^c$, lo que no puede ocurrir por el Lema 3.7.26.

Unicidad: Supongamos que

$$(3.21) \quad b = a'_1 \vee \cdots \vee a'_k$$

donde a'_i son elementos atómicos distintos de B . Como $b = \sup\{a'_1, \dots, a'_k\}$, para cada $i = 1, \dots, k$ deberá ser $a'_i \preceq b$ y por lo tanto $a'_i \in A_b$. Luego para cada $i = 1, \dots, k$ existe $j(i) \in \{1, \dots, n\}$ tal que $a'_i = a_{j(i)}$.

Por lo tanto solo debemos probar que $k = n$, y entonces la descomposición (3.21) no es más que una permutación de la descomposición (3.20).

Supongamos entonces que existe $j_0 \in \{1, \dots, n\}$ que no interviene en la descomposición (3.21). Observemos que como a_{j_0} y $a_{j(i)}$ son átomos distintos de B , del Ejercicio 27 de este capítulo tenemos que $a_{j_0} \wedge a_{j(i)} = 0$ para cada $i = 1, \dots, k$. Luego del Lema 3.6.4 resulta

$$a_{j_0} \wedge b = (a_{j_0} \wedge a_{j(1)}) \vee (a_{j_0} \wedge a_{j(2)}) \vee \dots \vee (a_{j_0} \wedge a_{j(k)}) = 0$$

Pero entonces, por el Lema 3.7.26, no puede ocurrir que $a_{j_0} \preceq b$, lo cual es absurdo. \square

Siguiendo la demostración del Lema 3.7.28 tenemos:

Corolario 3.7.29. *Sea B un álgebra de Boole finita y sea $A \subseteq B$ un conjunto de átomos. Si $b = \sup A$, entonces $A = A_b = \{a \in B : a \text{ es un átomo de } B \text{ y } a \preceq b\}$.*

Teorema 3.7.30. *Si B es un álgebra de Boole finita, entonces B es isomorfa a $(\mathcal{P}(X), \subseteq)$ para algún conjunto X . Más precisamente, X es el conjunto de átomos de B .*

Demostración. Sea X el conjunto de átomos de B y, para cada $b \in B$, sea $A_b \subseteq X$ el conjunto definido en el Lema 3.7.28. Consideremos la función

$$f : B \rightarrow \mathcal{P}(X), \quad f(b) = A_b.$$

Veamos que f es un isomorfismo de álgebras de Boole. Por el Teorema 3.7.19 bastará probar que f es un isomorfismo de orden, y por el Teorema 2.5.6, basta probar que f es sobre y que para cada $b, c \in B$,

$$b \preceq c \iff A_b \subseteq A_c.$$

Para ver que f es sobre, sea $A \subseteq X$ un conjunto de átomos y sea $b = \sup A$. Entonces por el Corolario 3.7.29 resulta $A = A_b$ y por lo tanto $f(b) = A$.

Supongamos ahora que $b \preceq c$. Entonces si $a \in A_b$, resulta que a un átomo y $a \preceq b \preceq c$, con lo cual a es un átomo tal que $a \preceq c$, o sea, $a \in A_c$. Luego $A_b \subseteq A_c$.

Supongamos finalmente que $A_b \subseteq A_c$. Sea $A_b = \{a_1, \dots, a_k\}$ y $A_c = \{a_1, \dots, a_k, a_{k+1}, \dots, a_n\}$. Entonces por el Lema 3.7.28 resulta

$$b = a_1 \vee \dots \vee a_k \preceq (a_1 \vee \dots \vee a_k) \vee (a_{k+1} \vee \dots \vee a_n) = c$$

como queríamos probar. \square

Como consecuencia de este resultado tenemos:

Corolario 3.7.31. *Sea B un álgebra de Boole finita y sea X el conjunto de átomos de B . Si el cardinal de X es n , entonces B es isomorfa a 2^n y tiene cardinal 2^n .*

Corolario 3.7.32. *Dos álgebras de Boole finitas son isomorfas si y sólo si tienen el mismo cardinal.*

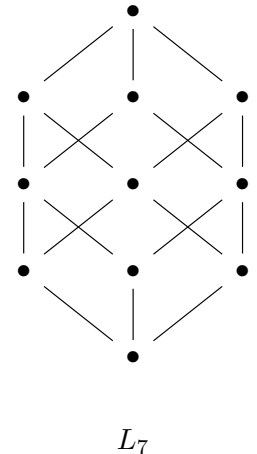
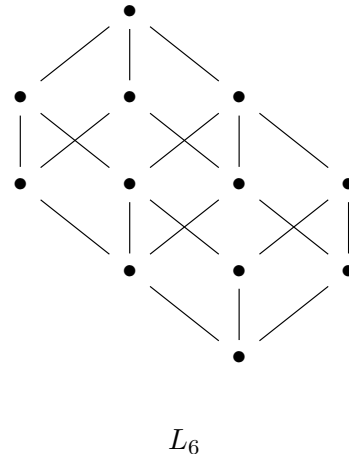
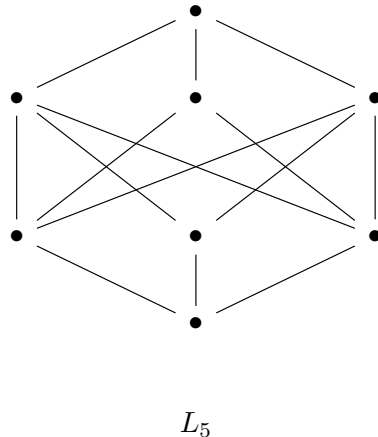
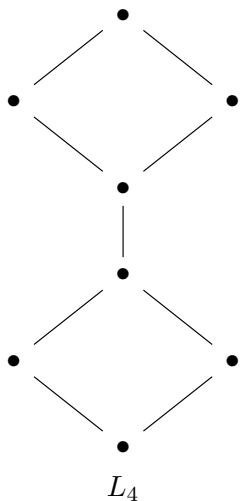
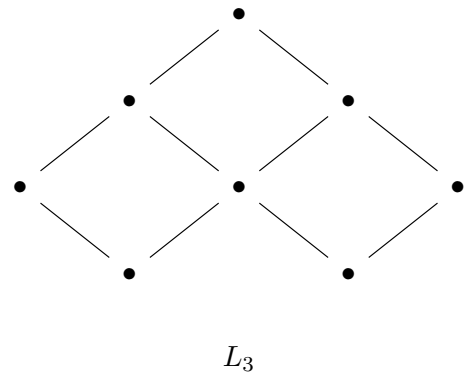
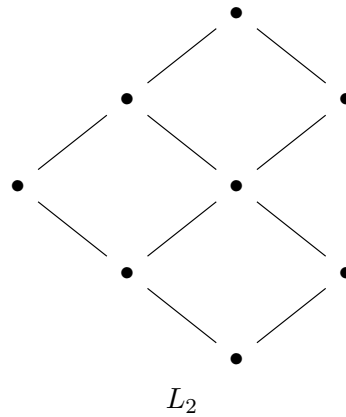
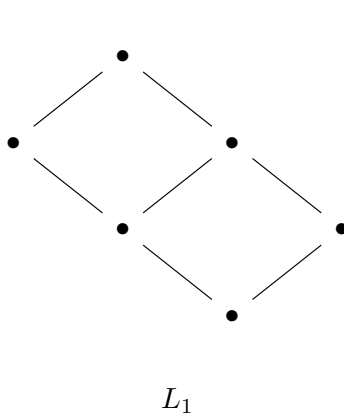
Demostración. Claramente si dos álgebras de Boole son isomorfas existe una biyección entre ellas y por lo tanto deben tener el mismo cardinal.

Supongamos entonces que B y B' son álgebras de Boole de cardinal 2^n . Sean X y X' los conjuntos de átomos de B y B' respectivamente.

Supongamos que B tiene cardinal k . Entonces por el Corolario 3.7.31 B es isomorfa a 2^k . Pero 2^k tiene cardinal 2^k y B tiene cardinal 2^n . Luego debe ser $k = n$ y B es isomorfa a 2^n . Con el mismo razonamiento B' es isomorfa a 2^n , y por lo tanto B y B' son isomorfas. \square

3.8. Ejercicios

1. ¿Cómo son los diagramas de Hasse de $(D_{p^2}, |)$, $(D_{p^3}, |)$, y más generalmente $(D_{p^k}, |)$, $k \in \mathbb{N}$, para un número primo $p \in \mathbb{N}$? Sea $n = p_1 p_2 \cdots p_l \in \mathbb{N}$ con p_j números primos distintos dos a dos tales que $p_i < p_j$ si $i < j$. Describir el diagrama de Hasse de $(D_n, |)$ para $l = 2, 3, 4$.
2. Determinar cuáles de los siguientes diagramas de Hasse admiten estructura reticular.



3. Mostrar que los siguientes posets son retículos. Determinar las operaciones \vee y \wedge en cada uno.
- a) $(\mathcal{S}(\mathbb{R}^2), \subseteq)$, donde $\mathcal{S}(\mathbb{R}^2)$ es el conjunto de subespacios vectoriales de \mathbb{R}^2 .
- b) (B^A, \leq) , donde: A es un conjunto cualquiera, (B, \preceq) es un retículo, $B^A = \{f : A \rightarrow B\}$ es el conjunto de funciones de A en B y \leq está dado por

$$f \leq g \Leftrightarrow f(a) \preceq g(a), \forall a \in A$$

c) Álgebra de Lindenbaum-Tarski.

4. Sean (L_1, \preceq_1) y (L_2, \preceq_2) retículos y consideremos el orden lexicográfico \preceq_{lex} en $L_1 \times L_2$. ¿En qué casos $(L_1 \times L_2, \preceq_{lex})$ es un retículo? En esos casos, ¿cuáles son las operaciones \vee y \wedge ?
5. Sea (L, \preceq) un retículo, $a_1, \dots, a_n \in L$ y sean

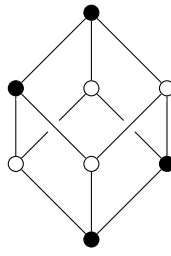
$$b = a_1 \vee a_2 \vee \dots \vee a_n, \quad c = a_1 \wedge a_2 \wedge \dots \wedge a_n.$$

Probar (por inducción sobre n) que $b = \sup\{a_1, \dots, a_n\}$ y $c = \inf\{a_1, \dots, a_n\}$. Concluir que si L es un retículo finito, todo subconjunto de L tiene ínfimo y supremo.

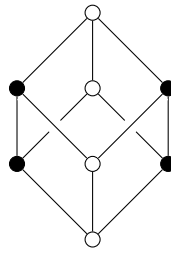
6. Sea L un retículo y sean $a, b, c \in L$. Probar que

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

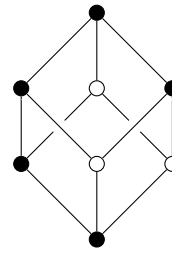
7. En los siguientes diagramas, los puntos negros determinan un subconjunto L_j ($j = 1, 2, 3$) de un retículo L . Determinar cuáles son subretículos de L



L_1



L_2



L_3

8. Sea (X, \preceq) un retículo y $a, b \in X$ con $a \preceq b$. Probar que los siguientes subconjuntos de X son subretículos.
- a) $I_a = \{x \in X : x \preceq a\}$
- b) $S_a = \{x \in X : b \preceq x\}$
- c) $[a, b] = \{x \in X : a \preceq x \preceq b\}$.
9. Probar que si L y S son retículos y L' y S' son subretículos de L y S respectivamente, entonces $L' \times S'$ es un subretículo de $(L \times S, \preceq_{prod})$.
10. Sea una función $f : X \rightarrow Y$. Considerar las funciones:

$$F : \mathcal{P}(Y) \rightarrow \mathcal{P}(X), \quad F(B) = f^{-1}(B) \text{ (imagen inversa)}$$

$$G : \mathcal{P}(X) \rightarrow \mathcal{P}(Y), \quad G(A) = f(A) \text{ (imagen directa)}$$

- a) Mostrar que F define un morfismo de retículo.

- b) Mostrar que G define un morfismo de retículo si y solo si f es inyectiva.
11. Sea (L, \preceq) un retículo. Un *polinomio* p en n -variables es una función $p : L^n \rightarrow L$ que pertenece al conjunto inductivo P_L :
- $i \in \{1, \dots, n\}$, $\pi_i \in P_L$, donde $\pi_i(x_1, \dots, x_n) = x_i$.
 - Si $f, g \in P_L$ entonces $f \vee g \in P_L$, donde $(f \vee g)(\bar{x}) = f(\bar{x}) \vee g(\bar{x})$.
 - Si $f, g \in P_L$ entonces $f \wedge g \in P_L$, donde $(f \wedge g)(\bar{x}) = f(\bar{x}) \wedge g(\bar{x})$.
- Probar que todo $p \in P_L$ es un morfismo de orden entre $(L^n, \preceq_{\text{prod}})$ y (L, \preceq) .
12. Sean (L, \preceq_L) y (S, \preceq_S) retículos tales que $S \subset L$ y consideremos la inclusión $i : S \rightarrow L$, $i(x) = x$ para cada $x \in S$. Probar que si i es un morfismo de retículos si y sólo si $\preceq_S = (\preceq_L)|_S$ y (S, \preceq_S) es un subretículo de L .
13. Probar los Corolarios 3.4.11 y 3.4.12
14. Sea $n = p_1 p_2 \cdots p_l \in \mathbb{N}$ tal que p_i son números primos distintos dos a dos. Probar que $(D_n, |)$ es isomorfo a $(P(I_l), \subseteq)$, con $I_l = \{1, 2, \dots, l\}$.
15. Sean L, L', S y S' retículos. Supongamos que $f : L \rightarrow L'$ y $g : S \rightarrow S'$ son morfismos de retículos. Definamos $f \times g : L \times S \rightarrow L' \times S'$ por $(f \times g)(x, y) = (f(x), g(y))$.
- a) Probar que $f \times g$ es un morfismo de retículos.
 - b) Probar que si L es isomorfo a L' y S es isomorfo a S' entonces $L \times S$ es isomorfo a $S \times S'$.
 - c) Probar que $(D_2, |) \times (D_4, |)$ es isomorfo a $(D_{12}, |)$.
16. Probar que si L y S son retículos isomorfos, entonces L^* es isomorfo a S^* .
17. Determinar si los retículos del Ejercicio 3 son acotados, y en ese caso, decidir si son complementados.
18. Probar que si L es un retículo acotado totalmente ordenado, los únicos elementos que admiten un complemento son 0 y 1.
19. Sea $f : L \rightarrow S$ un anti-isomorfismo de retículos. Probar que:
- a) L es acotado si y sólo si S es acotado.
 - b) L es complementado si y sólo si S es complementado.
 - c) Concluir que L es acotado (resp. complementado) si y sólo si L^* es acotado (resp. complementado).
20. Sea L un retículo y L' un subretículo de L .
- a) Probar que si L es acotado, L' no necesariamente es acotado.
 - b) Dar un ejemplo de un retículo acotado L y un subretículo acotado L' tal que $1_{L'} \neq 1_L$ y $0_{L'} \neq 0_L$. Es decir, aún cuando un subretículo sea acotado, su máximo y mínimo no tienen por qué coincidir con los respectivos elementos de L .
 - c) Dar un ejemplo de un retículo acotado L , un subretículo acotado L' con el mismo máximo y mínimo que L , pero tal que L sea complementado y L' no lo sea.
21. Determinar si los retículos del ejercicio 2 son no-modulares, modulares pero no-distributivos, o distributivos.

22. Sea (L, \preceq) un retículo. Probar que son equivalentes:
- a) (L, \preceq) es modular.
 - b) $a \succeq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c$ para todos $a, b, c \in X$.
 - c) $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$ para todos $a, b, c \in X$
 - d) $a \wedge (b \vee (a \wedge c)) = (a \wedge b) \vee (a \wedge c)$ para todos $a, b, c \in X$
23. Considerar el retículo $(\mathcal{S}(\mathbb{R}^2), \subseteq)$ de subespacios vectoriales de \mathbb{R}^2 .
- a) ¿Es $(\mathcal{S}(\mathbb{R}^2), \subseteq)$ un subretículo de $(\mathcal{P}(\mathbb{R}^2), \subseteq)$?
 - b) Mostrar que $(\mathcal{S}(\mathbb{R}^2), \subseteq)$ es un retículo modular no distributivo.
24. Probar el Teorema 3.6.23.
25. Sea B el álgebra de Boole del Ejemplo 3.7.13 y sea $f : B \rightarrow \mathbf{2}$ tal que $f(A) = 0$ si A es finito y $f(A) = 1$ si el complemento de A es finito. Probar que f es un morfismo de álgebras de Boole.
26. Sea $(B, \preceq) = (B, \vee, \wedge, 1, 0)$ un álgebra de Boole y sea $a \in B$. Probar que las siguientes afirmaciones son equivalentes:
- a) $a \in B$ es un átomo de B
 - b) Para cada $x, y \in B$, si $a \neq 0$ y $a \preceq x \vee y$, entonces $a \preceq x$ o $a \preceq y$.
 - c) Para cada $X \subseteq B$ tal que existe $M = \sup X$, si $a \neq 0$ y $a \preceq M$, entonces $a \preceq x$ para algún $x \in X$.
27. Probar que si $a \neq b$ son átomos en un álgebra de Boole B , entonces $a \wedge b = 0$.

Semigrupos, monoides y grupos

4.1. Operaciones binarias

Una *estructura algebraica* consiste de un conjunto X con una (o más) operaciones definidas en él. Ejemplos de operaciones son las habituales habituales (suma y producto) en los conjuntos numéricos \mathbb{N} , \mathbb{Z} , \mathbb{Q} o \mathbb{R} , pero también otras menos habituales como la composición de relaciones, el join y el meet en un retículo, etc.

A partir de este capítulo estudiaremos de forma abstracta un conjunto con una operación en él definida, y veremos que las distintas propiedades que tiene o no tiene dicha operación dan lugar a estructuras algebraicas diferentes. Comenzamos repasando algunos conceptos básicos:

Definición 4.1.1. Sea X un conjunto. Una **operación** (binaria y cerrada) en X es una función $*$: $X \times X \rightarrow X$. Denotamos $(X, *)$ para indicar que $*$ es una operación binaria en X . Normalmente denotamos $x * y := *(x, y)$. Decimos que:

- $*$ es **asociativa** si para cada $x, y, z \in X$, $*(x, *(y, z)) = (*(x, y), z)$, o sea

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

- $*$ es **conmutativa** si para cada $x, y, z \in X$, $*(x, y) = *(y, x)$, o sea

$$x * y = y * x.$$

Ejemplo 4.1.2. La suma y el producto en \mathbb{N} , \mathbb{Z} , \mathbb{Q} o \mathbb{R} son operaciones binarias asociativas y conmutativas definidas en estos conjuntos.

Lo mismo ocurre con el meet y el join en un retículo cualquiera L .

Si ahora consideramos el conjunto de todas las matrices a coeficientes reales, $\mathcal{M}_{n \times n}$, la suma de matrices es una operación asociativa y conmutativa, pero el producto es asociativo y no conmutativo. ■

La asociatividad y la conmutatividad son propiedades propias de una operación que involucran a todos los elementos del conjunto sobre el cual la operación está definida. Un conjunto puede tener además ciertos elementos *distinguidos* para una operación particular. Como veremos a continuación, la presencia o ausencia de alguno de ellos determinará estructuras diferentes en el conjunto.

Definición 4.1.3. Sea X un conjunto con una operación binaria $*$: $X \times X \rightarrow X$. Decimos que:

- $*$ admite un **elemento neutro a derecha** si existe $e_d \in X$ tal que para cada $x \in X$,

$$x * e_d = *(x, e_d) = x.$$

- $*$ admite un **elemento neutro a izquierda** si existe $e_i \in X$ tal que para cada $x \in X$,

$$e_i * x = *(e_i, x) = x.$$

Decimos que $*$ admite un **elemento neutro** (bilátero) o **elemento identidad** si existe $e \in X$ tal que e es un neutro a derecha y un neutro a izquierda, es decir, para cada $x \in X$,

$$e * x = x * e = x.$$

- Si $*$ admite un elemento neutro e , decimos que un elemento $x \in X$ admite un **inverso a derecha** para $*$ si existe un elemento $x_d^* \in X$ tal que

$$x * x_d^* = *(x, x_d^*) = e$$

$x \in X$ admite un **inverso a izquierda** si existe $x_i^* \in X$ tal que

$$x_i^* * x = *(x_i^*, x) = e.$$

$x \in X$ admite un **inverso** (bilátero) si existe $x^* \in X$ tal que x^* es inverso a izquierda y a derecha de x , es decir, si

$$x * x^* = x^* * x = e.$$

Si x admite un inverso se dice un elemento **invertible**.

Repasaremos en los siguientes ejemplos los elementos característicos de las operaciones que estudiamos hasta el momento, además de las operaciones conocidas en los conjuntos numéricos.

Ejemplo 4.1.4. Consideremos el conjunto $(\mathbb{N}, +)$ de los números naturales con la suma. $+$ es asociativa y conmutativa, pero no existe elemento neutro a derecha ni a izquierda. Por lo tanto tampoco tiene sentido hablar del inverso de ningún elemento.

Si ahora consideramos el producto (\cdot) en \mathbb{N} , \cdot es nuevamente una operación asociativa y conmutativa, con elemento neutro (el 1), y donde 1 es el único elemento que admite un inverso.

Pasemos a \mathbb{Z} . En este caso la suma, además de ser asociativa y conmutativa, admite un elemento neutro, el 0, y cada $k \in \mathbb{Z}$ admite un inverso, en este caso $-k$. El producto en \mathbb{Z} tiene las mismas propiedades que en \mathbb{N} , solo que aquí existen dos elementos invertibles: 1 y -1 .

En \mathbb{Q} y \mathbb{R} tanto la suma como el producto son operaciones asociativas, conmutativas, con elemento neutro (0 y 1 respectivamente). Todo elemento admite un inverso para la suma (su opuesto), y todo elemento, salvo el 0, admite un inverso para el producto (su recíproco). ■

Ejemplo 4.1.5. Consideremos el conjunto Rel_A de relaciones en un conjunto A . La unión, intersección y diferencia de relaciones definen operaciones en Rel_A . Veremos en los ejercicios qué propiedades tienen estas operaciones. Nos concentraremos aquí en la composición de relaciones. En este caso, \circ es una operación asociativa. En efecto, dadas \mathcal{R}, \mathcal{S} y \mathcal{T} en Rel_A , tenemos que para cada $x, y \in A$:

$$\begin{aligned} x(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} y &\iff \exists z \in A : x \mathcal{R} z \text{ y } z(\mathcal{T} \circ \mathcal{S}) y \\ &\iff \exists z, w \in A : x \mathcal{R} z, z \mathcal{S} w \text{ y } w \mathcal{T} y \\ &\iff \exists w \in A : x \mathcal{S} \circ \mathcal{R} w \text{ y } w \mathcal{T} y \\ &\iff x \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) y. \end{aligned}$$

Con lo cual $(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})$.

La relación diagonal, $\Delta = \{(a, a) : a \in A\}$ es un elemento neutro para la composición. En efecto, dada $\mathcal{R} \in \text{Rel}_A$ y $x, y \in A$ tenemos

$$\begin{aligned} x(\mathcal{R} \circ \Delta) y &\iff \exists z \in A : x \Delta z \text{ y } z \mathcal{R} y \\ &\iff x = z \text{ y } x \mathcal{R} y \\ &\iff x \mathcal{R} y. \end{aligned}$$

Por lo tanto $\mathcal{R} \circ \Delta = \mathcal{R}$, y de manera análoga se prueba que $\Delta \circ \mathcal{R} = \mathcal{R}$.

Observemos que dada una relación $\mathcal{R} \in \text{Rel}_A$, no tiene por qué ocurrir que \mathcal{R}^{-1} sea un inverso de \mathcal{R} para la operación de composición. Basta considerar por ejemplo la relación \mathcal{R} en $A = \{a, b, c\}$ dada por $\mathcal{R} = \{(a, c), (b, c)\}$. Entonces $\mathcal{R}^{-1} = \{(c, a), (c, b)\}$ y $\mathcal{R}^{-1} \circ \mathcal{R} = \{(a, a), (a, b), (b, a), (b, b)\} \neq \Delta$. Además $\mathcal{R} \circ \mathcal{R}^{-1} = \{(c, c)\} \neq \Delta$, con lo cual \mathcal{R}^{-1} no es un inverso a derecha ni a izquierda de \mathcal{R} (esto prueba además que, en general, \circ no es una operación conmutativa en Rel_A). Observemos que \mathcal{R} en realidad no puede admitir ningún inverso a derecha o izquierda. En efecto, tomemos una relación $\mathcal{S} \in \text{Rel}_A$ cualquiera. Entonces

$$x \in \text{Dom}(\mathcal{S} \circ \mathcal{R}) \implies \exists z \in A : x(\mathcal{S} \circ \mathcal{R}) z \implies \exists y \in A : x \mathcal{R} y \text{ y } y \mathcal{S} z \implies x \in \text{Dom}(\mathcal{R})$$

Es decir, $\text{Dom}(\mathcal{S} \circ \mathcal{R}) \subseteq \text{Dom}(\mathcal{R}) = \{a, b\} \neq \text{Dom}(\Delta)$, y por lo tanto para cualquier $\mathcal{S} \in \text{Rel}_A$ resulta $\mathcal{S} \circ \mathcal{R} \neq \Delta$. De manera similar se prueba que $\text{Im}(\mathcal{R} \circ \mathcal{S}) \subseteq \text{Im}(\mathcal{R}) = \{c\}$ y por lo tanto $\mathcal{R} \circ \mathcal{S} \neq \Delta$ cualquiera sea $\mathcal{S} \in \text{Rel}$. ■

Ejemplo 4.1.6. Sea $A \neq \emptyset$ y sea $\mathcal{F}(A) = \{f : A \rightarrow A\}$ el conjunto de las funciones de A en A . Entonces es posible componer dos elementos de $\mathcal{F}(A)$ y obtener otro elemento del mismo conjunto, con lo cual la composición de funciones es una operación bien definida en $\mathcal{F}(A)$.

Esta operación es asociativa, no conmutativa, y la función identidad $\text{Id} : A \rightarrow A$ tal que $\text{Id}(x) = x$ es el elemento neutro. Si una función es biyectiva, entonces admite un inverso. Sin embargo pueden existir funciones no biyectivas que admitan un inverso a derecha o izquierda.

Consideremos por ejemplo $A = \mathbb{N}$ y sea $f : \mathbb{N} \rightarrow \mathbb{N}$ tal que $f(n) = 2n$. Entonces si $g : \mathbb{N} \rightarrow \mathbb{N}$ es tal que

$$g(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ n & \text{si } n \text{ es impar} \end{cases}$$

resulta $g \circ f(n) = n$ para cada $n \in \mathbb{N}$, es decir, $g \circ f = \text{Id}$. Es claro que $f \circ g \neq \text{Id}$, y por lo tanto g es un inverso a izquierda de f pero no es un inverso a derecha. En realidad f admite infinitos inversos a izquierda, ya que podríamos haber definido g de cualquier manera sobre los impares y aún así seguiremos teniendo $g \circ f = \text{Id}$.

Observemos que f no admite ningún inverso a derecha. En efecto, si $h : \mathbb{N} \rightarrow \mathbb{N}$ fuese un inverso a derecha de f , tendríamos que para cada $n \in \mathbb{N}$,

$$n = \text{Id}(n) = f \circ h(n) = 2h(n)$$

pero esto implicaría que todo número natural es múltiplo de 2, lo cual es falso. ■

Además del neutro y los elementos invertibles, un conjunto con una operación binaria definida sobre él suele tener otros elementos distinguidos. Mencionamos a continuación los que tienen mayor relevancia:

Definición 4.1.7. Sea X un conjunto con una operación binaria $*$: $X \times X \rightarrow X$.

- Un elemento $a \in X$ se dice un **elemento absorbente a derecha** para $*$ si $x * a = a$ para cada $x \in X$, y se dice un **elemento absorbente a izquierda** para $*$ si $a * x = a$ para cada $x \in X$. a es un **elemento absorbente** si es absorbente a derecha e izquierda.
- Un elemento $a \in X$ se dice **idempotente** si $a * a = a$.
- Decimos que un elemento $a \in X$ es **cancelativo a derecha** si para cada $x, y \in X$ se verifica

$$x * a = y * a \implies x = y$$

$a \in X$ se dice **cancelativo a izquierda** si para cada $x, y \in X$ se verifica

$$a * x = a * y \implies x = y$$

$x \in X$ se dice **cancelativo** si es cancelativo a izquierda y a derecha.

Observación 4.1.8. Si una operación $*$ admite un elemento neutro (a derecha, izquierda o bilátero), éste es siempre un elemento idempotente. También será idempotente cualquier elemento absorbente. Dejamos como **ejercicio** probar que si $*$ admite un elemento absorbente (bilátero) este es único.

Ejemplo 4.1.9. En $(\mathbb{N}, +)$ no hay elementos absorbentes ni idempotentes, y cualquier elemento en $(\mathbb{N}, +)$ es cancelativo. Por otra parte, el producto en \mathbb{N} no admite elementos absorbentes, el único elemento idempotente es 1 y todo elemento es cancelativo.

Pasemos a \mathbb{Z} . En $(\mathbb{Z}, +)$ no hay elementos absorbentes ni idempotentes (salvo el 0) y todo elemento es cancelativo. El producto en \mathbb{Z} tiene las mismas propiedades que en \mathbb{N} , solo que aquí el 0 es además un elemento absorbente para el producto. 0 junto con la identidad 1 son los únicos elementos idempotentes. Todos los elementos distintos de 0 son cancelativos.

\mathbb{Q} y \mathbb{R} tienen las mismas propiedades que \mathbb{Z} para la suma. Respecto del producto, también aquí 0 es un elemento absorbente, con lo cual junto con 1 son elementos idempotentes, y son los únicos con esta propiedad. Todo elemento es cancelativo para la suma, y todo elemento distinto de 0 es cancelativo para el producto. ■

Ejemplo 4.1.10. Consideremos el conjunto $\mathcal{M}_{n \times n}$ de matrices $n \times n$ a coeficientes reales. La suma de matrices es asociativa, conmutativa, admite un elemento neutro (la matriz $0_{n \times n}$ cuyas entradas son todas 0), y todo elemento admite un inverso (si $M = (m_{ij}) \in \mathcal{M}_{n \times n}$, su inverso para la suma es la matriz $-M$ cuyas entradas son $(-M)_{ij} = -m_{ij}$). La matriz $0_{n \times n}$ es el único elemento idempotente y todos los elementos de $(\mathcal{M}_{n \times n}, +)$ son cancelativos. Todas las propiedades de la suma de matrices son consecuencia de las propiedades análogas de la suma de números reales.

Si consideremos en $\mathcal{M}_{n \times n}$ el producto usual de matrices (que es asociativo, pero no conmutativo), tenemos que $(\mathcal{M}_{n \times n}, \cdot)$ admite un elemento neutro, la matriz identidad Id , cuyas entradas son 1 en la diagonal y 0 en el resto. No todo elemento admite un inverso. De hecho, sabemos del álgebra lineal que $M \in \mathcal{M}_{n \times n}$ admite inverso si y sólo si $\det(M) \neq 0$.

La matriz $0_{n \times n}$ es un elemento absorbente para el producto. Si denotamos E_i la matriz cuya entrada ii es 1 y el resto de las entradas son todas 0, tenemos que E_i es un elemento idempotente de $\mathcal{M}_{n \times n}$. Tenemos aquí un ejemplo de elemento idempotente que no es la identidad ni un elemento absorbente. En $(\mathcal{M}_{n \times n}, \cdot)$ los elementos invertibles son cancelativos. Existen además elementos no invertibles que admiten inversos a derecha o izquierda. En ese caso, tendremos elementos cancelativos a derecha o izquierda respectivamente. Dejamos como **ejercicio** dar ejemplos de estas situaciones. ■

Ejemplo 4.1.11. Consideremos el conjunto $(\mathcal{F}(A), \circ)$ de funciones $f : A \rightarrow A$ con la composición de funciones (ver Ejemplo 4.1.6). Aquí también existen elementos idempotentes distintos del neutro. Por ejemplo, si f es una función constante, resulta claro que $f \circ f = f$. Existen además elementos cancelativos a derecha o izquierda que no son cancelativos. Por ejemplo, en $\mathcal{F}(\mathbb{N})$, la función $f : \mathbb{N} \rightarrow \mathbb{N}$ dada por $f(n) = 2n$ es cancelativa a izquierda, pero no a derecha. En efecto, si $g : \mathbb{N} \rightarrow \mathbb{N}$ es la función que vale $n/2$ sobre los pares y n sobre los impares, vimos en el Ejemplo 4.1.6 que $g \circ f = \text{Id}$. Luego tendremos

$$f \circ a = f \circ b \implies g \circ (f \circ a) = g \circ (f \circ b) \implies a = b.$$

Pero si ahora tomamos

$$h(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ 3n & \text{si } n \text{ es impar} \end{cases}$$

tendremos

$$g \circ f(n) = n = h \circ f(n)$$

con lo cual $g \circ f = h \circ f$ pero $g \neq h$. ■

Ejemplo 4.1.12. Consideremos un retículo (L, \preceq) . Las operaciones \vee y \wedge son asociativas y conmutativas y todo elemento es idempotente, ya que $x \vee x = x \wedge x = x$ para cada $x \in L$.

Analicemos la existencia de un elemento neutro para \wedge (que al ser \wedge conmutativa bastará ver si es neutro a derecha o izquierda). Observemos que $e \in L$ será un neutro si $e \wedge x = x$ para cada $x \in L$, esto es, $x = \inf\{x, e\}$, y por lo tanto $x \preceq e$ para cada $x \in L$. Luego L tendrá un elemento neutro si y sólo si L tiene un máximo. En ese caso, es fácil ver que ningún elemento distinto del máximo es invertible. En efecto, dado $x \in L$, $x \neq e$, para cualquier otro $x^* \in L$ se verifica que $x \wedge x^* \preceq x \neq e$.

Si además L tiene un mínimo m , entonces $m \wedge x = m$ para cualquier $x \in L$, por lo tanto un mínimo de L es un elemento absorbente de \wedge .

De manera análoga, obtenemos que \vee tiene un elemento neutro si y sólo si L tiene un mínimo. Y si además L tiene un máximo, entonces éste es un elemento absorbente para \vee . ■

Ejemplo 4.1.13. Muchas veces para construir ejemplos o contraejemplos de conjuntos con alguna operación, que pretendemos que satisfaga o no una cierta propiedad es útil considerar conjuntos finitos y una operación que esté dada por una tabla. Dicha tabla se denomina **tabla de Cayley** de la operación. Consideremos un conjunto de tres elementos $X = \{a, b, c\}$ con una operación $*$ definida por:

$*$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

Es inmediato de la tabla que a es el elemento neutro de $*$. Sin embargo, tenemos que

$$b * b = a, \quad b * c = c * b = a$$

con lo cual b admite dos inversos distintos para $*$. Lo mismo ocurre con c . Como la tabla es simétrica respecto de la diagonal, la operación $*$ es conmutativa. Sin embargo no es asociativa, como se observa haciendo

$$b * (b * c) = b * a = b, \quad (b * b) * c = a * c = c.$$

Podemos de la misma manera construir operaciones con más de un elemento neutro a derecha o izquierda:

\odot	a	b	c
a	a	a	c
b	b	b	a
c	c	c	a

\diamond	a	b	c
a	a	b	c
b	a	b	c
c	c	a	a

De las tablas resulta evidente que a y b son neutros a derecha para \odot y son neutros a izquierda para \diamond . ■

En el ejemplo 4.1.13 vimos que una operación puede tener más de un neutro a izquierda o derecha, pero no consideramos ningún ejemplo de una operación con más de un neutro (bilátero). Como veremos, esto no es posible:

Lema 4.1.14. *Sea $*$ una operación en un conjunto X . Si $*$ admite un elemento neutro, éste es único.*

Demostración. Supongamos que e y e' son elementos neutros para una operación $*$. Entonces tendremos por un lado que $*(e, e') = e'$, pues e es elemento neutro, pero al mismo tiempo $*(e, e') = e$, pues también e' es neutro. Como $*$ es una función, y por ende cada elemento puede tener una única imagen, concluimos que $e = e'$. \square

También observamos en el Ejemplo 4.1.13 que incluso si una operación admite un neutro (único) un elemento puede admitir más de un elemento inverso. Esto sin embargo no puede ocurrir si la operación es asociativa:

Lema 4.1.15. *Sea $*$ una operación en un conjunto X que es asociativa y admite un elemento neutro. Si un elemento admite un inverso, entonces el inverso es único.*

Demostración. Sea $*$ una operación asociativa en X que admite un neutro $e \in X$. Supongamos que existe $x \in X$ que admite dos inversos. Es decir, existen x^* , $x^{**} \in X$ tales que

$$x * x^* = x^* * x = e, \quad x * x^{**} = x^{**} * x = e.$$

Tendremos entonces

$$x^{**} = x^{**} * e = x^{**} * (x * x^*) = (x^{**} * x) * x^* = e * x^* = x^*$$

como queríamos probar. \square

Notación 4.1.16. *Si $*$ es una operación en X con elemento neutro y un elemento $x \in X$ admite un único elemento inverso (por ejemplo si $*$ es asociativa), éste se denota por x^{-1} .*

Observación 4.1.17. *Es importante notar que la asociatividad de la operación no garantiza, aún existiendo elemento neutro, que cada elemento tenga un inverso (aunque sabemos que en caso de existir, éste será único). Si consideramos el producto en \mathbb{Z} , por ejemplo, existe un elemento neutro (1) y aún así ningún elemento distinto de ± 1 admite un inverso.*

Por otra parte, incluso si la operación es asociativa y admite un elemento neutro, un elemento puede tener más de un inverso a derecha o izquierda (ver el Ejemplo 4.1.6). En este caso, estos inversos laterales no podrán ser inversos (biláteros).

Observación 4.1.18. *Si una operación admite un neutro e , éste es siempre un elemento invertible, dado que $e * e = e$.*

Lema 4.1.19. *Sea X un conjunto con una operación binaria $*$ que admite un elemento neutro. Entonces:*

1. *Si x^* es un inverso a derecha (resp. a izquierda) de $x \in X$, entonces x es un inverso a izquierda (resp. a derecha) de x^* .*
2. *Si x admite un inverso x^{-1} , entonces x es también el inverso de x^{-1} , esto es, $(x^{-1})^{-1} = x$.*
3. *Si $*$ es asociativa y x e y admiten inversos, entonces $x * y$ admite un inverso y $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Demostración. Las dos primeras propiedades son inmediatas de la definición de inverso. Probemos la última. Supongámslo que $*$ es asociativa y x e y admiten inversos. Entonces

$$(x * y) * (y^{-1} * x^{-1}) = ((x * y) * y^{-1}) * x^{-1} = (x * (y * y^{-1})) * x^{-1} = (x * e) * x^{-1} = x * x^{-1} = e.$$

La prueba de que $(y^{-1} * x^{-1}) * (x * y) = e$ es análoga. \square

4.2. Subconjuntos cerrados, productos y cocientes

Veremos en lo que sigue una serie de operaciones que se obtienen a partir de otras. El caso más sencillo de este fenómeno ocurre cuando podemos considerar una operación $*$ en un conjunto X , pero definida sobre un subconjunto de X :

Definición 4.2.1. Sea X un conjunto con una operación $*$ y sea $Y \subset X$. Decimos que $*$ es **cerrada** en Y (o que Y es un **subconjunto cerrado** para $*$) si para cada $x, y \in Y$, $x * y \in Y$.

En este caso, $*$: $Y \times Y \rightarrow Y$ define una operación en Y , que se denomina la **operación restringida** o **inducida** desde X , o **heredada** de X .

Ejemplo 4.2.2. Consideremos el subconjunto $\mathcal{B}(A)$ de $\mathcal{F}(A)$ formado por las funciones biyectivas de A en A . Como la composición de funciones biyectivas es una función biyectiva, concluimos que la composición de funciones en $\mathcal{F}(A)$ es una operación cerrada en $\mathcal{B}(A)$. \blacksquare

Ejemplo 4.2.3. Consideremos el subconjunto $GL(n, \mathbb{R})$ de matrices no singulares $n \times n$. Como el producto de matrices no singulares es una matriz no singular (pues $\det(AB) = \det(A)\det(B)$), $GL(n, \mathbb{R})$ es un subconjunto cerrado de $\mathcal{M}_{n \times n}$ para el producto de matrices.

Observemos que a diferencia del producto, la suma de matrices no se induce a $GL(n, \mathbb{R})$. Por ejemplo, la matriz identidad Id y su opuesta $-\text{Id}$ son matrices en $GL(n, \mathbb{R})$ y sin embargo su suma es la matriz nula que es una matriz singular. Luego $GL(n, \mathbb{R})$ no es un subconjunto cerrado para la suma de matrices. \blacksquare

Analizaremos a continuación que propiedades de la operación original se preservan cuando la operación se induce a un subconjunto.

Definición 4.2.4. Sea $*$ una operación en un conjunto X . Decimos que una propiedad de $*$ es **hereditaria** si esta propiedad se verifica en cualquier subconjunto cerrado Y de X con la operación inducida desde X .

Lema 4.2.5. Sea $*$ una operación en un conjunto X y sea $Y \subset X$ un subconjunto cerrado para $*$. Entonces:

1. La asociatividad es una propiedad hereditaria. Es decir, si $*$ es asociativa en X , entonces $*$ es asociativa en Y .
2. La conmutatividad es una propiedad hereditaria. Es decir, si $*$ es conmutativa en X , entonces $*$ es conmutativa en Y .

3. Si e es un neutro en X y $e \in Y$, entonces e es un neutro en Y .
4. Si Y hereda el neutro de X y $x \in Y$ admite un inverso x^* (a derecha, izquierda o bilátero) en X tal que $x^* \in Y$, entonces x^* es un inverso (a derecha, izquierda o bilátero) de x para la operación restringida a Y .

Demostración. Las asociatividad y la conmutatividad de la operación inducida a un subconjunto cerrado de X son inmediatas. Dejamos los detalles como **ejercicio**. Probemos los puntos 3 y 4. Supongamos que e es el elemento neutro de X para $*$. Entonces, si $e \in Y$, para cada $y \in Y$ se verifica $e * y = y * e = y$ en X . Pero como la operación en Y es la misma que en X , concluimos que e también es un neutro en Y .

Si ahora $x \in Y$ admite un inverso x^* en X (supondremos que bilátero, las pruebas de los otros casos son análogas), como $e \in Y$ resulta $x * x^* = x^* * x = e$ tanto en X como en Y . Luego x^* es un inverso de x en Y para la operación inducida. \square

Analizaremos a continuación algunos ejemplos. Veremos que en algunos casos un subconjunto cerrado Y de un conjunto X con una operación $*$ puede no heredar algunos elementos característicos de X , pero a su vez la operación inducida en Y puede en otros casos tener más propiedades que la operación en X .

Ejemplo 4.2.6. Retomemos el Ejemplo 4.2.2. Vimos que la composición de funciones se induce desde $\mathcal{F}(A)$ (el conjunto de funciones con dominio y codominio un conjunto A) al conjunto de biyecciones $\mathcal{B}(A)$. Por lo tanto la composición es asociativa en $\mathcal{B}(A)$. Al igual que ocurre en $\mathcal{F}(A)$, la composición no es conmutativa en $\mathcal{B}(A)$ (aunque esto no puede deducirse del Lema 4.2.5 como veremos a continuación). La función identidad es un elemento neutro en $\mathcal{F}(A)$ que se hereda a $\mathcal{B}(A)$. Además, como una función es biyectiva si y sólo si es invertible, cada elemento de $\mathcal{B}(A)$ hereda su inverso de $\mathcal{F}(A)$. En particular, todo elemento de $\mathcal{B}(A)$ es invertible.

Lo mismo ocurre cuando inducimos el producto de matrices al subconjunto cerrado $GL(n, \mathbb{R})$ (ver Ejemplo 4.2.3). El producto en $GL(n, \mathbb{R})$ es asociativo, no conmutativo, hereda el neutro de $\mathcal{M}_{n \times n}$ (la matriz identidad) y además todo elemento de $GL(n, \mathbb{R})$ es invertible.

Si ahora consideramos el subconjunto $Y = \{\lambda \text{Id} : \lambda \in \mathbb{R}\}$ de $\mathcal{M}_{n \times n}$, vemos fácilmente que Y es un subconjunto cerrado de $\mathcal{M}_{n \times n}$ para el producto de matrices, y el producto en Y es además conmutativo, aunque no lo sea en todo $\mathcal{M}_{n \times n}$. \blacksquare

Ejemplo 4.2.7. A esta altura es importante notar que el elemento neutro no tiene por qué heredarse cuando inducimos una operación a un subconjunto cerrado. Por ejemplo, \mathbb{N} es un subconjunto de \mathbb{Z} cerrado para la suma. La operación inducida sigue siendo asociativa y conmutativa pero no admite neutro (pues $0 \notin \mathbb{N}$). Lo mismo ocurre con los inversos, incluso cuando el neutro se hereda. Por ejemplo \mathbb{N}_0 hereda el neutro de \mathbb{Z} pero no hereda el inverso de ningún elemento. \blacksquare

Ejemplo 4.2.8. Vimos en el Lema 4.2.5 que si un subconjunto cerrado Y de X hereda el neutro, entonces éste es un elemento neutro en Y (y por lo tanto único, si es un neutro bilátero). Puede ocurrir sin embargo que Y no herede el neutro de X y aún así tenga un nuevo elemento neutro. Más aún, elementos no invertibles

en X pueden serlo en Y . Consideremos por ejemplo el subconjunto $Y = \left\{ A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ de $\mathcal{M}_{2 \times 2}$. Como $A \cdot A = A$, el producto de matrices se induce a Y . Además, como Y tiene a A como único elemento, es claro que A es neutro en Y , y por lo tanto un elemento invertible de Y . Observemos sin embargo que A no es invertible en $\mathcal{M}_{2 \times 2}$. ■

Además de considerar subconjuntos cerrados de un conjunto con una operación, podemos construir nuevos conjuntos con operaciones a partir de dos o más conjuntos dados, definiendo una operación en el producto cartesiano de estos conjuntos:

Definición 4.2.9. Sean $*_X$ una operación en un conjunto X y $*_Y$ una operación en un conjunto Y . Se denomina **operación producto** de $*_X$ y $*_Y$ a la operación $*$ en $X \times Y$ dada por

$$(x, y) * (x', y') = (x *_X x', y *_Y y').$$

Teorema 4.2.10. Sean $*_X$ una operación en un conjunto X , $*_Y$ una operación en un conjunto Y y $*$ la operación producto en $X \times Y$. Entonces:

1. Si $*_X$ y $*_Y$ son asociativas, entonces $*$ es asociativa.
2. Si $*_X$ y $*_Y$ son conmutativas, entonces $*$ es conmutativa.
3. Si e_X es un elemento neutro (a derecha, izquierda o bilátero) en X y e_Y es un elemento neutro del mismo tipo en Y , entonces (e_X, e_Y) es un neutro en $X \times Y$ (a derecha, izquierda o bilátero resp.).
4. Si X e Y tienen ambos un elemento neutro y $x \in X$ e $y \in Y$ admiten un elemento inverso x^* , y^* respectivamente (a derecha, izquierda o bilátero), entonces (x^*, y^*) es un inverso (a derecha, izquierda o bilátero resp.) de (x, y) en $X \times Y$.

Demostración. Comencemos probando la asociatividad de $*$. Tenemos:

$$\begin{aligned} ((x, y) * (x', y')) * (x'', y'') &= (x *_X x', y *_Y y') * (x'', y'') = ((x *_X x') *_X x'', (y *_Y y') *_Y y'') \\ &= (x *_X (x' *_X x''), y *_Y (y' *_Y y'')) = (x, y) * (x' *_X x'', y' *_Y y'') \\ &= (x, y) * ((x', y') * (x'', y'')). \end{aligned}$$

Si $*_X$ y $*_Y$ son conmutativas, entonces para cada $(x, y), (x', y') \in X \times Y$, se tiene

$$(x, y) * (x', y') = (x *_X x', y *_Y y') = (x' *_X x, y' *_Y y) = (x', y') * (x, y)$$

con lo cual $*$ es conmutativa.

Supongamos ahora que $*_X$ admite un neutro a derecha e_X y $*_Y$ admite un neutro a derecha e_Y . Entonces para cada $(x, y) \in X \times Y$, resulta:

$$(x, y) * (e_X, e_Y) = (x *_X e_X, y *_Y e_Y) = (x, y)$$

con lo cual (e_X, e_Y) es un neutro a derecha de $*$. La prueba para el neutro a izquierda o bilátero es análoga y se deja como **ejercicio**.

Supongamos finalmente que X e Y tienen ambos un elemento neutro e_X y e_Y respectivamente. Entonces $e = (e_X, e_Y)$ será el neutro (bilátero) de $X \times Y$. Sen $x \in X$ e $y \in Y$ elementos que admiten inversos a derecha x^* e y^* en X e Y respectivamente. Entonces

$$(x, y) * (x^*, y^*) = (x *_X x^*, y *_Y y^*) = (e_X, e_Y) = e$$

con lo cual (x^*, y^*) es un inverso a derecha de (x, y) (la prueba para el inverso a izquierda y bilátero es análoga). \square

Ejemplo 4.2.11. Consideremos \mathbb{R}^2 con la suma usual, es decir, tal que

$$(x, y) + (x', y') = (x + x', y + y')$$

Entonces esta suma no es más que la operación producto de la suma en \mathbb{R} con sí mismo. Luego la suma en \mathbb{R}^2 será asociativa, conmutativa, con elemento neutro $(0, 0)$ y cada elemento (x, y) admite un inverso $(-x, -y)$. \square

Observación 4.2.12. Tanto la definición de la operación producto como sus propiedades pueden generalizarse al producto cartesiano de cualquier colección finita de conjuntos con sus respectivas operaciones.

Finalizamos esta sección definiendo la operación inducida a un conjunto cociente. Supongamos que X es un conjunto con una operación $*$ y consideramos una relación de equivalencia \sim en X . Podemos construir el conjunto cociente X/\sim . Nos interesa determinar cuándo es posible inducir la operación de X a X/\sim :

Definición 4.2.13. Sea X es un conjunto con una operación $*$ y \sim una relación de equivalencia en X . Decimos que $*$ **se induce al cociente** X/\sim si se verifica que:

$$\left. \begin{array}{l} x \sim x' \\ y \sim y' \end{array} \right\} \implies x * y \sim x' * y'.$$

Si $*$ se induce al cociente X/\sim queda bien definida una operación en X/\sim , que seguiremos denotando por $*$, definida por $*$: $(X/\sim) \times (X/\sim) \rightarrow X/\sim$,

$$[x] * [y] := [x * y].$$

donde $[x]$ denota la clase de equivalencia de x para la relación \sim .

Ejemplo 4.2.14. Los enteros módulo m . Sea $m \in \mathbb{N}$ y consideremos la relación de congruencia módulo m en \mathbb{Z} (ver Ejemplo 1.6.10), es decir, dados $x, y \in \mathbb{Z}$,

$$x \equiv y (m) \iff x - y \text{ es múltiplo de } m.$$

Recordemos que denotamos por \mathbb{Z}_m al conjunto cociente de \mathbb{Z} por esta relación. Veamos que la suma y el producto en \mathbb{Z} se inducen al cociente \mathbb{Z}_m . Sean entonces $x, y, x', y' \in \mathbb{Z}$ tales que $x \equiv x' (m)$ e $y \equiv y' (m)$. Existirán $k, k' \in \mathbb{Z}$ tales que

$$x - x' = km, \quad y - y' = km.$$

Sumando miembro a miembro ambas igualdades tenemos que

$$(x + y) - (x' + y') = (x - x') + (y - y') = km + k'm = (k + k')m$$

Luego $x + y \equiv x' + y' (m)$ como queríamos ver.

Pasando al producto, tenemos que

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') = ykm + x'k'm = (yk + x'k)m$$

de donde $xy \equiv x'y' (m)$.

Podemos ilustrar con algunos ejemplos en \mathbb{Z}_m qué significa que las operaciones estén bien definidas en el cociente.

Tomemos por ejemplo en \mathbb{Z}_5 los elementos $\bar{1}$ y $\bar{3}$. Entonces por definición $\bar{1} + \bar{3} = \overline{1+3} = \bar{4}$. Pero $\bar{1} = \bar{6}$ y $\bar{3} = \bar{18}$. Luego que $+$ esté bien definida en el cociente significa que con la definición que dimos debería ser $\bar{6} + \bar{18} = \bar{1} + \bar{3}$. Y en efecto, $\bar{6} + \bar{18} = \overline{6+18} = \bar{24} = \bar{4}$.

También tenemos que $\bar{1} \cdot \bar{3} = \overline{1 \cdot 3} = \bar{3}$ y $\bar{6} \cdot \bar{18} = \overline{6 \cdot 18} = \bar{108} = \bar{3}$. ■

Ejemplo 4.2.15. Sea $A \neq \emptyset$ y consideremos el conjunto $(\mathcal{F}(A), \circ)$ de funciones $f : A \rightarrow A$ con la composición de funciones (ver Ejemplo 4.2.2). Fijemos $a \in A$ y definamos la relación \sim en A por

$$f \sim g \iff f(a) = g(a).$$

Es fácil verificar que \sim es una relación de equivalencia en $\mathcal{F}(A)$.

Tomemos por ejemplo $A = \{a, b, c\}$ y las funciones constantes $f : A \rightarrow A$, $f(x) = c$, $g : A \rightarrow A$, $g(x) = b$, y sean

$$f' : A \rightarrow A, f'(a) = c, f'(b) = a, f'(c) = b$$

$$g' : A \rightarrow A, g'(a) = b, g'(b) = b, g'(c) = c.$$

Entonces $f \sim f'$ pues $f(a) = f'(a) = c$, y $g \sim g'$ pues $g(a) = g'(a) = b$. Sin embargo,

$$f \circ g(a) = c, \quad f' \circ g'(a) = a$$

con lo cual $f \circ g \not\sim f' \circ g'$ (también puede verse que $g \circ f \not\sim g' \circ f'$). Por lo tanto la composición de funciones no se induce al cociente $\mathcal{F}(A)/\sim$, es decir, no puede definirse $[f] \circ [g]$ por $[f \circ g]$ dado que el resultado de la composición $f \circ g$ depende de los representantes elegidos de $[f]$ y $[g]$. ■

Teorema 4.2.16. Sea $*$ una operación en un conjunto X y sea \sim una relación de equivalencia en X tal que $*$ se induce al cociente X/\sim . Entonces:

1. Si $*$ es asociativa en X , la operación inducida a X/\sim es asociativa.
2. Si $*$ es conmutativa en X , la operación inducida a X/\sim es conmutativa.
3. Si e es un elemento neutro (a derecha, izquierda o bilátero) para $*$ en X , entonces $[e]$ es un neutro con las mismas características para la operación inducida en X/\sim .
4. Si $x \in X$ posee un inverso (a derecha, izquierda o bilátero) x^* , entonces $[x^*]$ es un inverso (con las mismas características de x^*) para la operación inducida en X/\sim .

Demostración. Comencemos probando la asociatividad. Sean $[x], [y], [z] \in Z/\sim$. Entonces

$$([x] * [y]) * [z] = [x * y] * [z] = [(x * y) * z] = [x * (y * z)] = [x] * [y * z] = [x] * ([y] * [z]).$$

La prueba de la conmutatividad es análoga y la dejamos como **ejercicio**

Supongamos ahora que e es un neutro a derecha de $*$ (los otros casos son análogos). Entonces para cada $x \in X$, $x * e = x$. Sea $[x] \in X/\sim$ cualquiera. Entonces

$$[x] * [e] = [x * e] = [x]$$

con lo cual $[e]$ es un neutro a derecha en X/\sim .

Finalmente, si x admite un inverso a derecha x^* en X , entonces $x * x^* = e$ y por lo tanto

$$[x] * [x^*] = [x * x^*] = [e]$$

de donde deducimos que $[x^*]$ es un inverso a derecha de $[x]$ en X/\sim . Los otros casos son análogos. \square

Ejemplo 4.2.17. Sea $m \in \mathbb{N}$ y consideremos el cociente $(\mathbb{Z}_m, +)$ (ver Ejemplo 4.2.14). Como 0 es el neutro de $(\mathbb{Z}, +)$, $\bar{0}$ es el elemento neutro de $(\mathbb{Z}_m, +)$. Además, en \mathbb{Z} , todo elemento x tiene un inverso, su opuesto $-x$. Por lo tanto $\overline{-x}$ es el inverso de \bar{x} en \mathbb{Z}_m . Observe que si $0 \leq x \leq m-1$, $\overline{-x} = \overline{m-x}$, dado que

$$(-x) - (m-x) = -x - m + x = -m$$

y entonces $-x \equiv m-x \pmod{m}$.

Consideremos ahora el producto en \mathbb{Z}_m . En este caso, $\bar{1}$ es el elemento neutro de (\mathbb{Z}_m, \cdot) , pues 1 es el neutro de (\mathbb{Z}, \cdot) . En (\mathbb{Z}, \cdot) los únicos elementos invertibles son 1 y -1 . Por lo tanto $\bar{1}$ y $\overline{-1} = \overline{m-1}$ son elementos invertibles de (\mathbb{Z}_m, \cdot) . Sin embargo, el Teorema 4.2.16 garantiza que las clases de elementos invertibles de un conjunto X son elementos invertibles del cociente, pero no necesariamente son las únicas.

Analicemos para qué elementos $k \in \mathbb{Z}$ resulta \bar{k} invertible en (\mathbb{Z}_m, \cdot) . Por definición, \bar{k} será un elemento invertible si existe \bar{k}^* tal que $\bar{k} \cdot \bar{k}^* = \bar{1}$, o equivalentemente, si

$$k \cdot k^* \equiv 1 \pmod{m} \iff \exists \lambda \in \mathbb{Z} : k \cdot k^* - 1 = \lambda \cdot m.$$

Es decir, \bar{k} es invertible en (\mathbb{Z}_m, \cdot) si y sólo si existen $k^* \in \mathbb{Z}$ y $t = -\lambda \in \mathbb{Z}$ tales que

$$k^* \cdot k + t \cdot m = 1.$$

Concluimos del Lema 2.3.11 que \bar{k} es un elemento invertible de (\mathbb{Z}_m, \cdot) si y sólo si $\text{m.c.d.}(k, m) = 1$, es decir, k y m son coprimos. En ese caso, el inverso de \bar{k} es el factor que acompaña a k en la combinación lineal entera de k y m que da como resultado 1.

Por ejemplo en \mathbb{Z}_{10} los elementos invertibles son $\bar{1}, \bar{3}, \bar{7}$ y $\bar{9}$. Como el inverso de un elemento invertible es también un elemento invertible, los inversos de elementos invertibles deben buscarse en la lista de elementos invertibles. Por lo tanto, en un caso sencillo como este, pueden encontrarse por inspección directa. Así, $\bar{1}^{-1} = \bar{1}$. Por otra parte,

$$\bar{3} \cdot \bar{7} = \overline{21} = \bar{1}$$

y por lo tanto $\bar{3}^{-1} = \bar{7}$ y $\bar{7}^{-1} = \bar{3}$. Finalmente, no queda otra opción que $\bar{9}^{-1} = \bar{9}$, lo que se comprueba fácilmente dado que $\bar{9} \cdot \bar{9} = \bar{81} = \bar{1}$.

Supongamos ahora que estamos trabajando en \mathbb{Z}_{3663} y consideremos $\overline{104}$. Determinar si 104 y 3663 son coprimos puede resultar relativamente sencillo descomponiendo ambos números en factores primos. Pero ¿cómo encontramos el inverso de 104, en caso de que fuera coprimo con 3663? Podemos responder ambas preguntas simultáneamente aplicando el Algoritmo de Euclides (ver Teorema 2.3.8). Para ello hacemos:

$$3663 = 35 \cdot 104 + 23$$

$$104 = 4 \cdot 23 + 12$$

$$23 = 1 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

Concluimos que $\text{m.c.d.}(104, 3663) = 1$ y por lo tanto $\overline{104}$ es invertible. Desandamos el Algoritmo de Euclides para obtener:

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 = 12 - 1 \cdot (23 - 1 \cdot 12) = -23 + 2 \cdot 12 \\ &= -23 + 2 \cdot (104 - 4 \cdot 23) = 2 \cdot 104 - 9 \cdot 23 \\ &= 2 \cdot 104 - 9 \cdot (3663 - 35 \cdot 104) \\ &= 317 \cdot 104 - 9 \cdot 3663. \end{aligned}$$

Luego $\overline{104}^{-1} = \overline{317}$ (y en efecto, $104 \cdot 317 = 32968 = 9 \cdot 3663 + 1$) ■

4.3. Semigrupos, monoides y grupos

Como es evidente la existencia y unicidad de elemento neutro y elementos inversos son propiedades fundamentales de una operación. La propiedad asociativa es aquella que asegura que el inverso, en caso de existir sea único, además de tener consecuencias importantes en la aritmética de la operación. Por lo tanto es interesante en sí mismo estudiar de manera abstracta un conjunto con una operación que reúna alguna de estas propiedades, comenzando por la asociatividad.

Definición 4.3.1. Sea X un conjunto con una operación $*$: $X \times X \rightarrow X$.

- Si $*$ es asociativa, $(X, *)$ se denomina un **semigrupo**.
- Si $(X, *)$ es un semigrupo que admite un elemento neutro, $(X, *)$ se denomina un **monoide**.
- Si $(x, *)$ es un monoide donde todo elemento tiene un elemento inverso, $(X, *)$ se denomina un **grupo**.
- Si $*$ es conmutativa, cualquiera de las estructuras anteriores se dice **conmutativa**. Si $(X, *)$ es un grupo conmutativo, se denomina un **grupo abeliano**.

Notación 4.3.2. Normalmente denotamos por (G, \cdot) a un grupo con su operación. Cuando la operación es clara por el contexto generalmente se omite. Más aún, es usual denotar $g_1 \cdot g_2$ como $g_1 g_2$ (es decir,

yuxtaponiendo los elementos). Es importante observar a esta altura que si bien la operación de manera abstracta se denota por \cdot , esta no necesariamente representa lo que comúnmente entendemos por un producto y es posible (y frecuente) utilizar notaciones distintas, como por ejemplo $+$, en los distintos ejemplos particulares.

Notación 4.3.3. Si X es un conjunto numérico (por ejemplo \mathbb{N} , \mathbb{Z} , \mathbb{R} , etc.) o un cociente de estos conjuntos tal que $0 \in X$, en lo que sigue denotaremos por X^* a $X - \{0\}$.

Ejemplo 4.3.4. Analicemos la estructura de los conjuntos numéricos y de matrices con las operaciones más comunes:

1. $(\mathbb{N}, +)$ es un semigrupo conmutativo y (\mathbb{N}, \cdot) es un monoide conmutativo. $(\mathbb{N}_0, +)$ es un monoide conmutativo.
2. (\mathbb{Z}, \cdot) es un monoide conmutativo, pero no es un grupo. $(\mathbb{Z}, +)$ es un grupo abeliano, cuyo elemento neutro es el 0 y el inverso de un elemento $k \in \mathbb{Z}$ es su opuesto $-k$.
3. $(\mathbb{Q}, +)$, (\mathbb{Q}^*, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}^*, \cdot) , $(\mathbb{C}, +)$ y (\mathbb{C}^*, \cdot) son grupos abelianos.
4. (\mathcal{M}_n, \cdot) , donde \cdot es el producto usual de matrices es un monoide no conmutativo, pero no es un grupo. Como hemos visto, el producto de matrices se induce a $GL(n, \mathbb{R})$, el conjunto de matrices inversibles, y $(GL(n, \mathbb{R}), \cdot)$ es un grupo no abeliano. ■

Ejemplo 4.3.5. Sea (L, \preceq) un retículo y consideremos las operaciones meet \wedge y join \vee definidas en L . Entonces (L, \wedge) y (L, \vee) son semigrupos conmutativos. Si además L es acotado, entonces (L, \wedge) y (L, \vee) son monoides conmutativos con neutros 0 y 1 respectivamente. ■

Ejemplo 4.3.6. Funciones, biyecciones y el grupo simétrico. $\mathcal{F}(X)$ (el conjunto de funciones de X en X) con la composición de funciones \circ es un monoide no conmutativo. Si nos restringimos a $\mathcal{B}(X)$, el conjunto de funciones biyectivas, entonces $(\mathcal{B}(X), \circ)$ es un grupo no abeliano. Un caso de particular interés se tiene cuando X es un conjunto finito. Supongamos que $X = \{x_1, \dots, x_n\}$, entonces es fácil ver que $\mathcal{B}(X)$ tiene $n!$ elementos. En efecto, cualquier biyección de X en sí mismo se identifica con una permutación de los elementos de X . Comúnmente se denota por S_n al grupo $\mathcal{B}(\{1, \dots, n\})$ y se llama **grupo simétrico de orden n** .

Si tomáramos por ejemplo $X = \{1, 2, 3, 4\}$ podremos representar cada función biyectiva $f : X \rightarrow X$ a través de dos filas: en la superior listamos todos los elementos de X , y en la inferior colocamos la imagen de cada uno de ellos por f . Así, si escribimos

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

tendremos que $f(1) = 1$, $f(2) = 3$, $f(3) = 2$ y $f(4) = 4$. O sea, f es la permutación que intercambia 2 y 3 y deja 1 y 4 fijos. Esta forma de representar las funciones biyectivas en un conjunto finito permite describir fácilmente la composición de dos funciones. Consideremos ahora

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Entonces:

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Este ejemplo sencillo muestra que S_n es no abeliano. ■

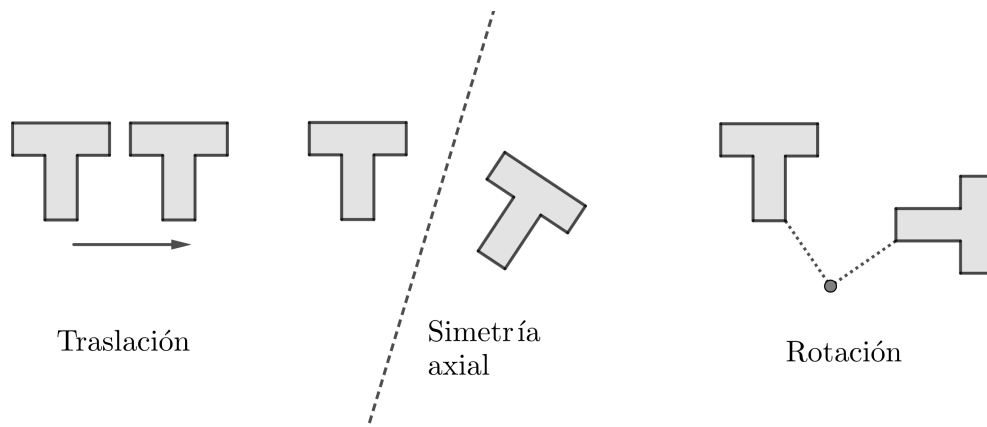
Ejemplo 4.3.7. Rotaciones del plano. Para cada $\theta \in \mathbb{R}$, sea $R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ una rotación en ángulo θ alrededor del origen de coordenadas. Denotemos por $\mathcal{R} = \{R_\theta : \theta \in \mathbb{R}\}$. Como $R_\theta \circ R_\rho = R_{\theta+\rho}$, la composición de funciones es cerrada en \mathcal{R} . Más aún, $R_0 = \text{Id}$ y $R_\theta \circ R_{-\theta} = R_{-\theta} \circ R_\theta = \text{Id}$. Por lo tanto (\mathcal{R}, \circ) es un grupo. A diferencia de lo que ocurre con $(\mathcal{B}(\mathbb{R}^2), \circ)$, es fácil ver que (\mathcal{R}, \circ) es un grupo abeliano.

Observemos que la descripción $\theta \leftrightarrow R_\theta$ no es biunívoca: para cada θ y cada $k \in \mathbb{Z}$, $R_\theta = R_{\theta+2k\pi}$. ■

Ejemplo 4.3.8. Isometrías del plano. Sea $\text{Iso}(\mathbb{R}^2)$ al conjunto de isometrías del plano euclídeo. Esto es, $\text{Iso}(\mathbb{R}^2)$ son las funciones biyectivas $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ tales que $d(f(x), f(y)) = d(x, y)$, siendo d la distancia usual en \mathbb{R}^2 . Claramente $\text{Id} \in \text{Iso}(\mathbb{R}^2)$. Si $g, h \in \text{Iso}(\mathbb{R}^2)$ entonces para cada $x, y \in \mathbb{R}^2$, resulta

$$d(g \circ f(x), g \circ f(y)) = d(g(f(x)), g(f(y))) = d(f(x), f(y)) = d(x, y)$$

con lo cual $g \circ f \in \text{Iso}(\mathbb{R}^2)$. Luego la composición de funciones se induce a $\text{Iso}(\mathbb{R}^2)$ y $(\text{Iso}(\mathbb{R}^2), \circ)$ es un monoide. No es difícil ver que si f es una isometría de \mathbb{R}^2 entonces f^{-1} también lo es. Concluimos que $(\text{Iso}(\mathbb{R}^2), \circ)$ es un grupo. Como es bien conocido, las isometrías del plano son rotaciones (alrededor de un centro arbitrario), traslaciones, simetrías axiales respecto de rectas y simetrías en deslizamiento, que surgen de la composición de una simetría axial y una traslación según un vector paralelo a la recta de reflexión.



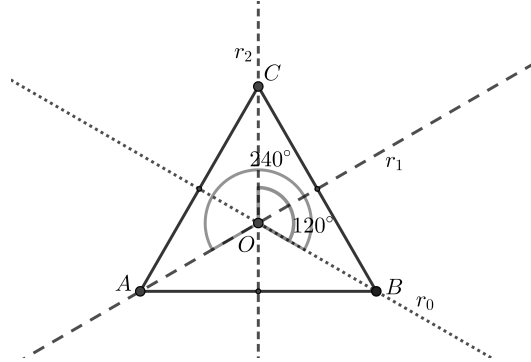
Ejemplo 4.3.9. Grupos diedrales. Sea P_n un polígono regular de n lados en el plano \mathbb{R}^2 . Sea

$$D_n = \{f \in \text{Iso}(\mathbb{R}^2) : f(P_n) = P_n\}.$$

Si $f, g \in D_n$, entonces $g \circ f(P_n) = g(f(P_n)) = g(P_n) = P_n$, con lo cual D_n es un subconjunto cerrado de $\text{Iso}(\mathbb{R}^2)$ para la composición de funciones. Más aún, es inmediato que $\text{Id} \in D_n$ y no es difícil ver que si $f \in D_n$, entonces $f^{-1} \in D_n$. Con lo cual (D_n, \circ) es un grupo, denominado **grupo diedral** del polígono P_n . A priori la notación D_n puede parecernos inadecuada, dado que este grupo no depende únicamente de la

cantidad de lados (o vértices) del polígono P_n sino que depende de P_n en su totalidad. Es decir, si P_n y P'_n son polígonos regulares distintos de n lados, sus grupos diedrales asociados serán distintos. Sin embargo, como veremos más adelante, las propiedades de estos grupos son independientes del polígono que hayamos elegido y sólo dependen de n (ver Ejemplo 4.7.23).

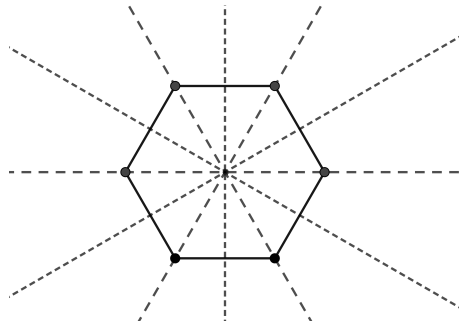
Consideremos por ejemplo un triángulo equilátero T . Entonces las isometrías del plano que mandan T en sí mismo (o sea, dejan T invariante) son la identidad Id , las rotaciones R_1 y R_2 alrededor del circuncentro O en 120° y 240° y las simetrías axiales S_0, S_1 y S_2 respecto de las tres alturas r_0, r_1 y r_2 del triángulo:



A continuación presentamos la tabla de Cayley de D_3 . Dejamos como **ejercicio** verificar el resultado de cada operación:

\circ	Id	R_1	R_2	S_0	S_1	S_2
Id	Id	R_1	R_2	S_0	S_1	S_2
R_1	R_1	R_2	Id	S_1	S_2	S_0
R_2	R_2	Id	R_1	S_2	S_0	S_1
S_0	S_0	S_2	S_1	Id	R_2	R_1
S_1	S_1	S_0	S_2	R_1	Id	R_2
S_2	S_2	S_1	S_0	R_2	R_1	Id

El grupo D_6 , asociado a un hexágono consta de Id , de las rotaciones alrededor del circuncentro en los ángulos $60^\circ, 120^\circ, 180^\circ, 240^\circ$ y 300° , de tres las simetrías axiales respecto de las rectas que unen vértices opuestos y tres simetrías axiales respecto de las rectas que unen los puntos medios de lados opuestos:



En términos generales, si denotamos por D_n al grupo diedral asociado a un polígono regular de n lados, centrado en el origen y de lado 1, D_n es un grupo de orden $2n$. Contiene \ln rotaciones $R_k = R_{\frac{2k\pi}{n}}$,

$k = 0, \dots, n-1$ (observar que $R_0 = \text{Id}$) y, si n es impar, las n simetrías respecto de las rectas que unen cada vértice con el punto medio de su lado opuesto, y si n es par, $n/2$ simetrías respecto de las rectas que unen vértices opuestos y $n/2$ simetrías respecto de las rectas que unen los puntos medios de lados opuestos.

En la siguiente figura se muestran los efectos del grupo diedral D_8 , dejamos como ejercicio identificar qué transformación se ha aplicado al octógono original para obtener cada una de las distintas configuraciones:



Si fijamos una recta de reflexión r_0 en el polígono P_n y nombramos las otras rectas de reflexión r_1, r_2, \dots, r_{n-1} en el orden en el que aparecen en sentido antihorario, tendremos que la composición en D_n está dada por las siguientes reglas:

$$R_i \circ R_j = R_j \circ R_i = R_{i+j}, \quad S_i \circ R_j = S_{i-j}, \quad R_i \circ S_j = S_{i+j}, \quad S_i \circ S_j = R_{i-j}$$

donde en las operaciones $i+j$ e $i-j$ debe tomarse el respectivo representante de $\overline{i+j}$ o $\overline{i-j}$ en \mathbb{Z}_n entre 0 y $n-1$ (por ejemplo, en D_3 , $R_1 \circ R_2 = R_{1+2} = R_0$, dado que $1+2 \equiv 0(3)$). ■

A partir de los Teoremas 4.2.10 y 4.2.16 podemos demostrar fácilmente que el producto y el cociente de cualquiera de las estructuras que hemos presentado es una estructura del mismo tipo. Dejamos los detalles de la prueba como **ejercicio**:

Teorema 4.3.10 (Estructuras producto). *Sean $(X, *_X)$ e $(Y, *_Y)$ dos conjuntos con operaciones binarias y consideremos el conjunto $(X \times Y, *)$ con la operación producto. Entoces*

1. *si X e Y son semigrupos, entonces $X \times Y$ es un semigrupo.*
2. *si X e Y son monoides, entonces $X \times Y$ es un monoide. Más aún, si e_X y e_Y son las identidades en X e Y respectivamente, entonces (e_X, e_Y) es la identidad en $X \times Y$.*
3. *si X e Y son grupos, entonces $X \times Y$ es un grupo. Más aún, si e_X y e_Y son las identidades en X e Y respectivamente, entonces (e_X, e_Y) es la identidad en $X \times Y$; y si x^{-1} e y^{-1} son los inversos de x e y respectivamente, entonces (x^{-1}, y^{-1}) es el inverso de (x, y) en $X \times Y$.*

Ejemplo 4.3.11. Como $(\mathbb{R}, +)$ es un grupo abeliano, entonces $(\mathbb{R}^2, +)$ con la suma usual es un grupo abeliano. Más generalmente, $(\mathbb{R}^n, +)$ con la operación suma componente a componente es un grupo abeliano, para cualquier $n \in \mathbb{N}$. ■

Teorema 4.3.12 (Estructuras cociente). *Si $(X, *)$ es un conjunto con una operación binaria y \sim es una relación de equivalencia en X tal que $*$ se induce al cociente X/\sim , entonces*

1. *si X es un semigrupo, X/\sim es un semigrupo.*
2. *si X es un monoide, X/\sim es un monoide. Más aún, si e es la identidad en X , entonces $[e]$ es la identidad en X/\sim .*
3. *si X es un grupo, entonces X/\sim es un grupo. Más aún, si e es la identidad en X , entonces $[e]$ es la identidad en X/\sim y para cada $x \in X$, $[x]^{-1} = [x^{-1}]$.*

Ejemplo 4.3.13. A partir de este resultado podemos deducir que $(\mathbb{Z}_m, +)$ es un grupo abeliano y que (\mathbb{Z}_m, \cdot) es un monoide conmutativo. Como ya hemos observado en el Ejemplo 4.2.17, el cociente X/\sim puede tener más propiedades que $(X, *)$. Por ejemplo, en (\mathbb{Z}, \cdot) los únicos elementos invertibles son ± 1 , por lo tanto en (\mathbb{Z}_m, \cdot) , $\bar{1}$ y $\overline{-1} = \overline{m-1}$ son elementos invertibles. Sin embargo, son también invertibles los elementos \bar{k} tales que m. c. d. $(k, m) = 1$. En particular, si p es primo, todo elemento en (\mathbb{Z}_p, \cdot) distinto de $\bar{0}$ es invertible, y por lo tanto (\mathbb{Z}_p^*, \cdot) (donde $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$) es un grupo abeliano. ■

4.4. Potencias

La asociatividad de una operación permite definir la *potencia* de un elemento elevado a un exponente natural de modo tal que la potenciación tenga las propiedades habituales. Más precisamente:

Definición 4.4.1. *Sea $(X, *)$ un semigrupo. Dado $x \in X$ y $n \in \mathbb{N}$, el elemento $x^n \in X$ se define recursivamente como:*

- $x^1 = x$.
- $x^{n+1} = x^n * x$, para todo $n \in \mathbb{N}$.

Cabe observar que esta definición puede hacerse para cualquier operación, siempre que se respete el orden en que se operan los elementos. Sin embargo, si la operación $*$ no es asociativa, tendremos por ejemplo que $x^3 = x^2 * x$ (por definición), en general no coincide con $x * x^2$, dado que no tiene por qué ocurrir que $(x * x) * x = x * (x * x)$. Consideremos por ejemplo el conjunto $X = \{a, b, c\}$ con la operación $*$ dada por la siguiente tabla:

$*$	a	b	c
a	b	b	c
b	c	a	b
c	a	c	b

Entonces $(a * a) * a = b * a = c$ y $a * (a * a) = a * b = b$.

Veremos a continuación que en un semigrupo la potenciación verifica las propiedades conocidas:

Teorema 4.4.2. *Sea $(X, *)$ un semigrupo. Entonces para cada $m, n \in \mathbb{N}$ y cada $a \in X$ se verifican*

1. $a^m * a^n = a^n * a^m = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

Demostración. Probemos la primera propiedad. Sea $a \in X$ y fijemos $m \in \mathbb{N}$ cualquiera. Consideremos la proposición

$$p(n) : a^m * a^n = a^{m+n}.$$

Probaremos por inducción que $p(n)$ es verdadera para cada $n \in \mathbb{N}$.

Observemos que $p(1)$ es verdadera trivialmente, dado que por definición $a^m * a^1 = a^m * a = a^{m+1}$.

Supongamos entonces que $p(n)$ es verdadera y veamos que $p(n+1)$ es verdadera. Observemos que

$$a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} * a.$$

Por hipótesis inductiva $a^{m+n} = a^m * a^n$, y además por definición $a^n * a = a^{n+1}$. Luego tendremos

$$a^{m+(n+1)} = a^{m+n} * a = (a^m * a^n) * a = a^m * (a^n * a) = a^m * a^{n+1}$$

como queríamos ver.

Concluimos que $a^{m+n} = a^m * a^n$ para cada $n \in \mathbb{N}$. Como $m \in \mathbb{N}$ es arbitrario, concluimos que la propiedad es válida para cualquier $m, n \in \mathbb{N}$. Finalmente, resulta

$$a^n * a^m = a^{n+m} = a^{m+n} = a^m * a^n.$$

Para probar la segunda propiedad procedemos de manera similar. Fijemos $m \in \mathbb{N}$ y sea

$$q(n) : (a^m)^n = a^{mn}.$$

Por definición, $(a^m)^1 = a^m = a^{m \cdot 1}$ con lo cual $q(1)$ es verdadera. Supongamos que $q(n)$ es verdadera, entonces:

$$(a^m)^{n+1} \stackrel{(\dagger)}{=} (a^m)^n * a^m \stackrel{(\dagger\dagger)}{=} a^{mn} * a^m$$

donde en (\dagger) aplicamos la definición y en $(\dagger\dagger)$ la hipótesis inductiva. Pero por la primera propiedad que probamos en el punto 1, $a^{mn} * a^m = a^{mn+m} = a^{m(n+1)}$. Luego $(a^m)^{n+1} = a^{m(n+1)}$ y $q(n+1)$ es verdadera. Concluimos que $q(n)$ es verdadera para todo $n \in \mathbb{N}$, y como $m \in \mathbb{N}$ es arbitrario resulta el punto 2. \square

Observación 4.4.3. *Es importante observar que, en general, no vale la propiedad distributiva de la potencia respecto de la operación dada en un semigrupo arbitrario. Esto es, en general, si $a \neq b$,*

$$(a * b)^n \neq a^n * b^n.$$

Consideremos por ejemplo el grupo simétrico (S_3, \circ) (ver Ejemplo 4.3.6) y sean $f, g \in S_3$ dadas por

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Entonces

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \implies (g \circ f)^2 = (g \circ f) \circ (g \circ f) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{Id}.$$

Por otro lado,

$$f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{Id} \implies g^2 \circ f^2 = \text{Id} \circ f^2 = f^2 \neq (g \circ f)^2.$$

Puede demostrarse por inducción (dejamos la prueba como **ejercicio**) que:

Lema 4.4.4. Sea $(X, *)$ un semigrupo conmutativo. Entonces para cada $a, b \in X$ y cada $n \in \mathbb{N}$ se verifica $(a * b)^n = a^n * b^n$.

Definición 4.4.5. Sea $(X, *)$ un monoide con identidad e y sea $n \in \mathbb{N}$. Tenemos definido a^n para cada $n \in \mathbb{N}$ de acuerdo a la Definición 4.4.1. Definimos además

$$a^0 = e$$

con lo cual queda definido a^n para cada $n \in \mathbb{N}_0$.

Teorema 4.4.6. Sea $(X, *)$ un monoide. Entonces para cada $m, n \in \mathbb{N}_0$ y cada $a \in X$ se verifican

1. $a^m * a^n = a^n * a^m = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.
3. Si $(X, *)$ es conmutativo, entonces $(a * b)^n = a^n * b^n$ para cada $a, b \in X$ y cada $n \in \mathbb{N}_0$.

Demostración. Por el Teorema 4.4.2 las propiedades 1 y 2 valen para $n, m \in \mathbb{N}$.

Observemos además que por definición, $a^0 * a^0 = e * e = e = a^0 = a^{0+0}$ y $(a^0)^0 = e^0 = e = a^{0 \cdot 0}$ con lo cual las propiedades 1 y 2 valen cuando $n = m = 0$.

Fijemos entonces $m \in \mathbb{N}$ cualquiera y tomemos $n = 0$. Resulta:

$$a^m * a^0 = a^m * e = a^m = a^{m+0} \quad \text{y} \quad (a^m)^0 = e = a^0 = a^{m \cdot 0}.$$

De manera análoga se prueba que si $n \in \mathbb{N}$ y $m = 0$, $a^0 * a^n = a^{0+n}$. Para probar el punto 2 cuando $m = 0$ y $n \in \mathbb{N}$, observemos que $(a^0)^m = e^m$, con lo cual debemos probar que $e^m = e = a^{0 \cdot m}$ para cada $m \in \mathbb{N}$. La prueba es inmediata procediendo por inducción: en efecto, $e^1 = e$, y si suponemos que $e^m = e$, entonces $e^{m+1} = e^m * e = e * e = e$.

Observemos finalmente que el punto 3 vale para cada $n \in \mathbb{N}$ por el Lema 4.4.4. Para $n = 0$ tenemos $(a * b)^0 = e = e * e = a^0 * b^0$. □

Definición 4.4.7. Sea (G, \cdot) un grupo. Tenemos definido a^n para $n \in \mathbb{N}_0$. Si $k \in \mathbb{Z}$ con $k < 0$, se define $a^k := (a^{-1})^{-k}$.

Observación 4.4.8. Obsevemos que la notación a^{-1} adquiere aquí un doble significado: por un lado, representa el inverso de $a \in G$, y por otro, es a “elevado a la potencia -1 ”. Estas dos definiciones claramente coinciden. En efecto, denotemos por a^* el inverso de a y por a^{-1} a a elevado a la -1 . Entonces $a^{-1} = (a^*)^{(-(-1))} = (a^*)^1 = a^*$.

Teorema 4.4.9. Sea (G, \cdot) un grupo. Entonces para cada $m, n \in \mathbb{Z}$ y cada $a \in G$ se verifican

1. $a^m \cdot a^n = a^n \cdot a^m = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.
3. Si G es un grupo abeliano, entonces $(a \cdot b)^n = a^n \cdot b^n$ para cada $n \in \mathbb{Z}$ y cada $a, b \in G$.

Demostración. Ya hemos probado en el Teorema 4.4.6 que las propiedades son válidas cuando $m, n \in \mathbb{N}_0$.

Fijemos $m \in \mathbb{Z}$, $m < 0$ y tomemos $n = 0$. Entonces $a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$.

Fijemos ahora $m \in \mathbb{Z}$, $m < 0$ y consideremos la proposición

$$p(n) : a^m \cdot a^n = a^{m+n}.$$

Probaremos por inducción que $p(n)$ es válida para cada $n \in \mathbb{N}$.

Comencemos por el caso base $n = 1$. Como $m < 0$, $m = -1$ o $m < -1$. Si $m = -1$, $m + 1 = 0$ y en ese caso $a^{m+1} = e = a^{-1} \cdot a = a^m \cdot a^1$. Si $m < -1$, entonces $m + 1 < 0$. Luego por definición,

$$a^{m+1} = (a^{-1})^{-(m+1)} = (a^{-1})^{-(m+1)} \cdot (a^{-1} \cdot a) = ((a^{-1})^{-(m+1)} \cdot a^{-1}) \cdot a$$

Ahora bien, como $-(m+1) \in \mathbb{N}$, por el Teorema 4.4.6 (aplicado a las potencias de $a^{-1} \in G$) resulta

$$(a^{-1})^{-(m+1)} \cdot a^{-1} = (a^{-1})^{-(m+1)+1} = (a^{-1})^{-m} = a^m$$

Luego $a^{m+1} = a^m \cdot a$ como queríamos probar.

Supongamos que $p(n)$ es verdadera. Entonces

$$a^m \cdot a^{n+1} = a^m \cdot (a^n \cdot a) = (a^m \cdot a^n) \cdot a \stackrel{(\dagger)}{=} a^{m+n} \cdot a \stackrel{(\dagger\dagger)}{=} a^{m+n+1}$$

donde (\dagger) vale por la hipótesis inductiva y $(\dagger\dagger)$ es el caso base. Luego $p(n+1)$ es verdadera.

Concluimos que $a^m \cdot a^n = a^{m+n}$ para cada $m \in \mathbb{Z}$ y cada $n \in \mathbb{N}_0$.

Finalmente, si $n < 0$, entonces $-n > 0$ y aplicando la propiedad que hemos probado a $a^{-1} \in G$ resulta

$$a^m \cdot a^n = (a^{-1})^{-m} \cdot (a^{-1})^{-n} = (a^{-1})^{-m-n} = a^{m+n}$$

lo que concluye la prueba del punto 1.

La propiedad 2 también es consecuencia del Teorema 4.4.6 si $m, n \geq 0$. Supongamos entonces que $m < 0$, $n \geq 0$. Entonces $-m > 0$ y por el Teorema 4.4.6 aplicado a $a^{-1} \in G$ resulta

$$(a^m)^n = ((a^{-1})^{-m})^n = (a^{-1})^{-mn} = a^{mn}$$

Concluimos que el punto 2 vale para cualquier $m \in \mathbb{Z}$, $n \in \mathbb{N}_0$.

Veamos ahora que para cada $m \in \mathbb{N}_0$ vale

$$(4.1) \quad (a^m)^{-1} = a^{-m}.$$

Para $m = 0$ y $m = 1$ es trivial. Supongamos entonces que esta propiedad vale para $m \in \mathbb{N}$ y veamos que vale para $m + 1$. En efecto,

$$(a^{m+1})^{-1} = (a^m \cdot a)^{-1} = a^{-1} \cdot (a^m)^{-1} = a^{-1} \cdot a^{-m} \stackrel{\text{punto 1}}{=} a^{-1-m} = a^{-(m+1)}$$

Finalmente, si $m \in \mathbb{Z}$ y $n < 0$, entonces $-n > 0$ y por lo que acabamos de probar:

$$(a^m)^n = ((a^m)^{-1})^{-n} \stackrel{(4.1)}{=} (a^{-m})^{-n} \stackrel{(\dagger)}{=} a^{(-m)(-n)} = a^{mn}$$

donde (\dagger) vale dado que $-m \in \mathbb{Z}$ y $-n \in \mathbb{N}$. □

Observación 4.4.10. *Hasta ahora hemos utilizado la notación $*$ o \cdot para indicar una operación genérica en un conjunto X . Esta notación puede hacernos pensar erróneamente que la operación en el conjunto es un producto, y no resulta tan intuitiva para describir las propiedades que tienen otras operaciones como la suma. Por ejemplo, si X es un semigrupo y $x \in X$, la potencia x^n (para $n > 0$) representa el elemento que se obtiene de operar iteradamente x con sí mismo n -veces. Si consideramos el semigrupo $(\mathbb{N}, +)$ y tomamos $m \in \mathbb{N}$, por la definición de potencia tendremos $m^2 = m + m$, $m^3 = m^2 + m$, y más generalmente, $m^{k+1} = m^k + m$ para cada $k \in \mathbb{N}$. Esto es claramente contradictorio con la definición de potencia que tenemos en los conjuntos numéricos, donde este concepto está efectivamente asociado a un producto. Es por ello que para describir mejor las propiedades de los conjuntos donde está definida una suma, utilizaremos lo que se denomina como **notación aditiva**.*

Notación 4.4.11. *Sea X un semigrupo conmutativo donde está definida una operación suma $(+)$. Si $(X, +)$ es un semigrupo, para cada $n \in \mathbb{N}$ y cada $x \in X$ denotamos por nx al elemento de X definido recursivamente como*

$$1x = x, \quad (n+1)x = nx + x.$$

Si $(X, +)$ es un monoide conmutativo, se define además $0x = e$.

Si $(X, +)$ es un grupo abeliano, el inverso de x se denota $-x$ y para $k \in \mathbb{Z}$, $k < 0$ se define

$$kx = (-k)(-x).$$

Notación 4.4.12. Suma directa. *Si $(X, +)$, $(Y, +)$ son semigrupos, monoides o grupos conmutativos cuya operación es una suma, el producto $X \times Y$ se denomina **suma directa** de $(X, +)$ e $(Y, +)$ y se denota $X \oplus Y$. La operación producto sigue denotándose por $+$.*

Reformulamos a continuación las propiedades de los Teoremas 4.4.2 y 4.4.9 en notación aditiva:

Teorema 4.4.13. *Sea $(X, +)$ un semigrupo conmutativo. Entonces para cada $a \in X$ y cada $n, m \in \mathbb{N}$,*

1. $na + ma = (n + m)a$.
2. $m(na) = (mn)a$.

Si $(X, +)$ es un monoide conmutativo, las propiedades anteriores valen para $n, m \in \mathbb{N}_0$, y si $(X, +)$ es un grupo abeliano, valen para $n, m \in \mathbb{Z}$.

4.5. Subestructuras

Nos proponemos ahora definir las **subestructuras** correspondientes a las estructuras algebraicas que hemos definido en la sección 4.3. Una subestructura de $(X, *)$ no es más que un subconjunto cerrado $Y \subseteq X$ que tal que $(Y, *)$ es una estructura algebraica del mismo tipo que $(X, *)$ e Y heredada todos los elementos característicos de X (en las estructuras que estamos considerando, se trata eventualmente del neutro o los inversos de cada elemento).

Observemos que:

- Si $(X, *)$ es un semigrupo, y $Y \subseteq X$ es un subconjunto cerrado, entonces por el Lema 4.2.5, $(Y, *)$ es un semigrupo.
- Si $(X, *)$ es un monoide y $Y \subseteq X$ es un subconjunto cerrado, el neutro e de X no necesariamente se hereda a Y . En el caso de que $e \in Y$, por el Lema 4.2.5 $(Y, *)$ es un monoide.
- Lo mismo ocurre si (G, \cdot) es un grupo y (H, \cdot) es un subconjunto cerrado: la identidad de G y los inversos de los elementos de H no necesariamente se heredan a H , pero en caso de que esto ocurra, por el Lema 4.2.5 (H, \cdot) es un grupo.

Por lo tanto definimos:

Definición 4.5.1. *Sea $(X, *)$ un semigrupo. Un **subsemigrupo** de X es un subconjunto $Y \subseteq X$ tal que Y es un subconjunto cerrado para $*$.*

Observación 4.5.2. *Como ya hemos observado, la asociatividad de una operación es una propiedad que hereda cualquier subconjunto cerrado. Por lo tanto si $Y \subseteq (X, *)$ es un subsemigrupo de un semigrupo $(X, *)$, entonces $(Y, *)$ (con la operación restringida) es en sí mismo un semigrupo. Recíprocamente, es trivial que si $(Y, *)$ (con la misma operación $*$ de X) es un semigrupo, entonces es un subsemigrupo de X (pues estamos asumiendo implícitamente que $*$ es una operación definida en Y , y por lo tanto Y es un subconjunto cerrado para $*$).*

*En conclusión $(Y, *)$ es un subsemigrupo de $(X, *)$ si y sólo si $Y \subseteq X$ y $(Y, *)$ es un semigrupo.*

Ejemplo 4.5.3. Sea $n \in \mathbb{N}$ y sea Y el subconjunto de múltiplos positivos de n . Si $x, y \in Y$, existen $k, k' \in \mathbb{N}$ tales que $x = kn$, $y = k'n$. Luego $x + y = (k + k')n$, con lo cual Y es un subconjunto cerrado para la suma. Concluimos que $(Y, +)$ es un subsemigrupo de $(\mathbb{N}, +)$. ■

Definición 4.5.4. Sea $(X, *)$ un monoide. Un **submonoide** de $(X, *)$ es un subconjunto $Y \subseteq X$ cerrado para $*$ tal que si e_X es la identidad de X , entonces $e_X \in Y$.

Observación 4.5.5. Un submonoide Y de un monoide $(X, *)$ es en sí mismo un monoide, con la misma identidad que X . A diferencia de lo que ocurre con los semigrupos (y de la misma manera que ocurre con los retículos, ver la sección 3.3) un subconjunto de un monoide puede ser un monoide, pero no necesariamente ser un submonoide (es decir, puede tener otra identidad).

Ejemplo 4.5.6. Consideremos un monoide cualquiera $(X, *)$ con identidad e . Sea $x \in X$ un elemento idempotente distinto de e (por ejemplo, podemos considerar un retículo L con la operación \wedge o \vee , y $x \in L$ cualquiera). Entonces $Y = \{x\}$ es un monoide, dado que $x * x = x$, y por lo tanto x es la identidad en Y . Sin embargo, como $x \neq e$, Y no es un submonoide de X . ■

Ejemplo 4.5.7. Consideremos el monoide (\mathbb{N}, \cdot) , cuya identidad es 1. Si consideramos el subconjunto Y de múltiplos de $n \in \mathbb{N}$ (ver Ejemplo 4.5.3), tenemos que si $x, y \in Y$, existen $k, k' \in \mathbb{N}$ tales que $x = kn$, $y = k'n$ y por lo tanto

$$x \cdot y = (kn) \cdot (k'n) = (kkn) \cdot n.$$

Luego Y es un subconjunto cerrado para \cdot y por lo tanto es un subsemigrupo de (\mathbb{N}, \cdot) . Sin embargo si $n \neq 1$ entonces $1 \notin Y$, con lo cual Y no es un submonoide de (\mathbb{N}, \cdot) . ■

Ejemplo 4.5.8. (\mathbb{Z}_m, \cdot) es un monoide. Consideremos $m = 10$ y tomemos $Y = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$. Entonces los resultados de multiplicar entre sí elementos de Y están dados en la siguiente tabla:

\cdot	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{7}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{1}$	$\bar{9}$	$\bar{3}$
$\bar{9}$	$\bar{9}$	$\bar{7}$	$\bar{3}$	$\bar{1}$

Luego Y es un subconjunto cerrado de (\mathbb{Z}_{10}, \cdot) tal que $\bar{1} \in Y$, con lo cual (Y, \cdot) es un submonoide. Observamos además que (Y, \cdot) es un grupo. ■

Ejemplo 4.5.9. Sea $(\mathcal{B}(X), \circ)$ el grupo de biyecciones de un conjunto X con la composición de funciones. Entonces $\mathcal{B}(X)$ es un subconjunto cerrado del monoide $(\mathcal{F}(X), \circ)$. Como la función identidad Id es biyectiva, $\text{Id} \in \mathcal{B}(X)$. Pero Id es el neutro de $(\mathcal{F}(X), \circ)$, con lo cual $(\mathcal{B}(X), \circ)$ es un submonoide de $(\mathcal{F}(X), \circ)$. En realidad, se trata de un submonoide que a su vez es un grupo (observemos que no afirmamos que es un subgrupo, puesto que $(\mathcal{F}(X), \circ)$ no tiene estructura de grupo). ■

Definición 4.5.10. Sea (G, \cdot) un grupo con identidad e . Un **subgrupo** de G es un subconjunto H de G cerrado para \cdot tal que $e \in H$ y $x^{-1} \in H$ para cada $x \in H$. Si H es un subgrupo de G , lo denotamos $H < G$.

Nuevamente, un subgrupo de un grupo G es un grupo, con la misma identidad de G . En este caso, la recíproca también vale. En los siguientes resultados caracterizaremos los subgrupos de un grupo G .

Teorema 4.5.11. *Sea (G, \cdot) un grupo y sea $H \subset G$ un subconjunto cerrado. H es un subgrupo de G si y sólo si (H, \cdot) es un grupo.*

Demostración. Si (H, \cdot) es un subgrupo de G , ya hemos visto que (H, \cdot) es un grupo.

Supongamos entonces que (H, \cdot) es un grupo. Sea e la identidad del grupo (G, \cdot) y e' es la identidad de (H, \cdot) . Veamos que $e = e'$.

Sea $h \in H$ cualquiera. Como e' es la identidad de H , resulta $h \cdot e' = h$. Ahora bien, como G es un grupo, h tiene un inverso $h^{-1} \in G$. Luego podemos premultiplicar por h^{-1} en G en la igualdad anterior y obtenemos

$$e = h^{-1} \cdot h = h^{-1} \cdot (h \cdot e') = (h^{-1} \cdot h) \cdot e' = e'.$$

Sea ahora h^* el inverso de h en H (y sigamos denotando por h^{-1} el inverso de h en G). Entonces

$$h^* = h^* \cdot e = h^* \cdot (h \cdot h^{-1}) = (h^* \cdot h) \cdot h^{-1} = e \cdot h^{-1} = h^{-1}.$$

Concluimos que H es un subconjunto cerrado de G tal que $e \in H$ y $h^{-1} \in H$ para cada $h \in H$. Luego H es un subgrupo de G . \square

Teorema 4.5.12. *Sea G un grupo y H un subconjunto de G . Entonces H es un subgrupo de G si y sólo si para todo $a, b \in H$ se verifica $ab^{-1} \in H$ (donde b^{-1} es el inverso de b en G).*

Demostración. Si H es un subgrupo de (G, \cdot) es inmediato que $ab^{-1} \in H$ para cada $a, b \in H$.

Supongamos entonces que H es un subconjunto de G que verifica que $ab^{-1} \in H$ cada vez que $a, b \in H$. Pongamos $f(a, b) = ab^{-1}$. Entonces por hipótesis, $f(a, b) \in H$ para cada $a, b \in H$.

Tomemos $a \in H$. Entonces $f(a, a) \in H$. Pero $f(a, a) = a \cdot a^{-1} = e$ (donde e es la identidad en G). Concluimos que $e \in H$.

Como $e \in H$, resulta que para cada $a \in H$, $f(e, a) \in H$, es decir, $f(e, a) = e \cdot a^{-1} = a^{-1} \in H$.

Finalmente, si $a, b \in H$, entonces $a, b^{-1} \in H$ y por lo tanto $f(a, b^{-1}) \in H$. Pero

$$f(a, b^{-1}) = a \cdot (b^{-1})^{-1} = ab$$

con lo cual H es un subconjunto cerrado para la operación de G que contiene a la identidad de G y al inverso de cada uno de sus elementos. Luego (H, \cdot) es un subgrupo de (G, \cdot) . \square

Ejemplo 4.5.13. Si $(X, *)$ es una de las tres estructuras que estamos estudiando, claramente $Y = X$ es una subestructura de X . Si X es un monoide o un grupo, también $Y = \{e\}$ es un submonoide o un subgrupo de X respectivamente. Estas subestructuras se denominan **triviales**. \blacksquare

Definición 4.5.14. Sea $(X, *)$ un semigrupo. Si $(Y, *)$ es un subsemigrupo y $Y \neq X$, $(Y, *)$ se denomina un **subsemigrupo propio** de X . Si $(X, *)$ es un monoide o un grupo y $(Y, *)$ es un submonoide o un subgrupo tal que $Y \neq X$ y $Y \neq \{e\}$, $(Y, *)$ se denomina un **submonoide o un subgrupo propio** de X .

Ejemplo 4.5.15. Consideremos el subconjunto $H = \{\bar{0}, \bar{2}, \bar{4}\}$ del grupo $(\mathbb{Z}_6, +)$. Tenemos que el inverso de $\bar{2}$ es $\bar{4}$ y por lo tanto el inverso de $\bar{4}$ es $\bar{2}$. Además

$$\bar{0} + \bar{2} = \bar{2}, \bar{0} + \bar{4} = \bar{4}, \bar{2} + \bar{2} = \bar{4}, \bar{2} + \bar{4} = \bar{0}, \bar{4} + \bar{4} = \bar{2}$$

es decir, $\bar{a} + \bar{b} \in H$ para cualquier $\bar{a}, \bar{b} \in H$, y por lo tanto H es un subgrupo propio de \mathbb{Z}_6 . Si ahora tomamos $K = \{\bar{0}, \bar{1}, \bar{3}, \bar{5}\}$, vemos que $\bar{1} + \bar{3} = \bar{4} \notin K$, con lo cual K no es un subgrupo de \mathbb{Z}_6 , puesto que la operación ni siquiera es cerrada en K . ■

Ejemplo 4.5.16. Fijemos $m \in \mathbb{Z}$ y sea $H = \text{Mul}(m)$ el conjunto de múltiplos de m . Sean $z, w \in H$. Entonces existen $k_1, k_2 \in \mathbb{Z}$ tales que $z = k_1m$, $w = k_2m$. Luego

$$z + (-w) = k_1m - k_2m = (k_1 - k_2)m \in H.$$

Concluimos del Teorema 4.5.12 que H es un subgrupo de $(\mathbb{Z}, +)$. Veremos en el Teorema 4.6.10 que todos los subgrupos de $(\mathbb{Z}, +)$ son de esta forma. ■

Dado un subconjunto Y de un semigrupo, un monoide o un grupo $(X, *)$, en muchos problemas interesa determinar cuál es la menor subestructura de $(X, *)$ que contiene a Y . Dedicaremos el resto de esta sección a abordar este problema.

Lema 4.5.17. Sea $(X, *)$ un semigrupo (monoide o grupo) y sea $\{Y_j\}_{j \in J}$ una familia de subsemigrupos (submonoides o subgrupos resp.). Entonces $\bigcap_{j \in J} Y_j$ es un subsemigrupo (submonoide, subgrupo resp.) de $(X, *)$.

Demostración. Pongamos $Y = \bigcap_{j \in J} Y_j$. Sean $x, y \in Y$. Entonces $x, y \in Y_j$ para cada $j \in J$. Como cada Y_j es un subsemigrupo, $x * y \in Y_j$ para cada $j \in J$. Luego $x * y \in \bigcap_{j \in J} Y_j$ con lo cual $(Y, *)$ es un subsemigrupo de $(X, *)$.

Si X es un monoide y cada Y_j es un submonoide, entonces $e \in Y_j$ para cada $j \in J$, con lo cual $e \in Y$ y $(Y, *)$ es un submonoide de $(X, *)$.

Finalmente, si $(X, *)$ es un grupo y $x \in Y$, entonces como cada Y_j es un subgrupo, $x^{-1} \in Y_j$ para cada $j \in J$. Luego $x^{-1} \in Y$. Por lo tanto $(Y, *)$ es un monoide tal que $x^{-1} \in Y$ para cada $x \in Y$, es decir, $(Y, *)$ es un subgrupo de $(X, *)$. □

Teorema 4.5.18. Sea $(X, *)$ un semigrupo (un monoide o un grupo) y sea $Y \subseteq X$ un subconjunto no vacío. Sea \mathcal{F}_Y la familia de subestructuras de $(X, *)$ que contienen a Y . Entonces $\langle Y \rangle = \bigcap_{Z \in \mathcal{F}_Y} Z$ es el menor subsemigrupo (submonoide, subgrupo resp.) de $(X, *)$ que contiene a Y .

Demostración. Por el Lema 4.5.17, $\langle Y \rangle$ es una subestructura de $(X, *)$ que contiene a Y . Si ahora W es una subestructura de $(X, *)$ que contiene a Y , entonces $W \in \mathcal{F}_Y$ y por lo tanto $\langle Y \rangle \subseteq W$. Luego $\langle Y \rangle$ es la menor subestructura de $(X, *)$ que contiene a Y . \square

Definición 4.5.19. Sea $(X, *)$ un semigrupo, monoide o grupo y sea $Y \subset X$. Sea \mathcal{F}_Y la familia de subsemigrupos, submonoides o subgrupos de X respectivamente que contienen a Y . Entonces

$$\langle Y \rangle = \bigcap_{Z \in \mathcal{F}_Y} Z$$

se denomina **subsemigrupo, submonoide o subgrupo generado por Y** .

Teorema 4.5.20. Sea X un semigrupo, monoide o grupo y sea $Y \subset X$. Entonces:

1. Si $(X, *)$ es un semigrupo, entonces

$$\begin{aligned} \langle Y \rangle &= \{a_1^{n_1} * a_2^{n_2} * \cdots * a_k^{n_k} : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{N}\} \\ &= \{n_1 a_1 + n_2 a_2 + \cdots + n_k a_k : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{N}\} \end{aligned}$$

2. Si $(X, *)$ es un monoide, entonces

$$\begin{aligned} \langle Y \rangle &= \{a_1^{n_1} * a_2^{n_2} * \cdots * a_k^{n_k} : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{N}_0\} \\ &= \{n_1 a_1 + n_2 a_2 + \cdots + n_k a_k : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{N}_0\} \end{aligned}$$

3. Si (X, \cdot) es un grupo, entonces

$$\begin{aligned} \langle Y \rangle &= \{a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{Z}\} \\ &= \{n_1 a_1 + n_2 a_2 + \cdots + n_k a_k : k \in \mathbb{N}, a_j \in Y \text{ para cada } j = 1, \dots, k, n_1, \dots, n_k \in \mathbb{Z}\} \end{aligned}$$

donde la expresión entre paréntesis corresponde, en cada caso, a la notación aditiva.

Demostración. Haremos la prueba para el caso en que X sea un grupo. Dejamos los detalles de las demás pruebas como **ejercicio**. Sea $K = \{a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} : k \in \mathbb{N}, n_j \in \mathbb{Z}, a_j \in Y \forall j = 1, \dots, k\}$. Observemos primero que K es un subgrupo de X . Sean $x = a_1^{n_1} \cdots a_k^{n_k}$ e $y = b_1^{m_1} \cdots b_r^{m_r}$ dos elementos arbitrarios de K . Observemos que $y^{-1} = b_r^{-m_r} \cdots b_2^{-m_2} b_1^{-m_1}$ y por lo tanto

$$xy^{-1} = a_1^{n_1} \cdots a_k^{n_k} b_r^{-m_r} \cdots b_2^{-m_2} b_1^{-m_1} \in K$$

dado que $a_i, b_j \in Y$ y $n_1, \dots, n_k, -m_r, \dots, -m_1 \in \mathbb{Z}$. Luego $K < X$ y $Y \subset K$, de donde $\langle Y \rangle \subset K$. Por otro lado, como $\langle Y \rangle$ contiene a todos los elementos de Y y la operación del grupo es cerrada en Y , si $k \in \mathbb{N}$ y $a_j \in Y$ para cada $j = 1, \dots, k$, entonces para cualesquiera $n_1, \dots, n_k \in \mathbb{Z}$, $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ es un elemento de $\langle Y \rangle$. Luego $K \subset \langle Y \rangle$. Concluimos que $K = \langle Y \rangle$ como queríamos probar. \square

Ejemplo 4.5.21. Consideremos el semigrupo $(\mathbb{N}, +)$. Si $k \in \mathbb{N}$, entonces $\langle \{k\} \rangle$ es el semigrupo de los múltiplos positivos de k . En particular, $\langle \{1\} \rangle = \mathbb{N}$. Sea ahora $X = \{2, 3\}$. Entonces por el Teorema 4.5.20

$$\langle \{2, 3\} \rangle = \{2x : x \in \mathbb{N}\} \cup \{3y : y \in \mathbb{N}\} \cup \{2x + 3y : x, y \in \mathbb{N}\}.$$

Observemos que $\langle \{2, 3\} \rangle$ contiene a 2 y a todos sus múltiplos, a 3 y a todos sus múltiplos, pero $\langle \{2, 3\} \rangle \neq \mathbb{N}$. En efecto, para cada $x, y \in \mathbb{N}$, $2x \geq 2$, $3x \geq 3$ y $2x + 3y \geq 5$. Luego, por ejemplo, $1 \notin \langle \{2, 3\} \rangle$.

Veamos que efectivamente

$$\langle \{2, 3\} \rangle = \mathbb{N} - \{1\}.$$

Ya vimos que $\langle \{2, 3\} \rangle \subseteq \mathbb{N} - \{1\}$. Sea entonces $n \in \mathbb{N} - \{1\}$. Si n es par, entonces n es múltiplo de 2 y por lo tanto $n \in \langle \{2, 3\} \rangle$. Si n es impar, como $n \neq 1$, $n = 2k + 1$ para algún $k \in \mathbb{N}$. Si $k = 1$, $n = 3 \in \langle \{2, 3\} \rangle$. Si $k > 1$, entonces $n = 2(k - 1) + 2 + 1 = 2(k - 1) + 3 \in \langle \{2, 3\} \rangle$. ■

Ejemplo 4.5.22. En el grupo \mathbb{Z} , tenemos también que $\langle \{1\} \rangle = \mathbb{Z}$. Consideremos ahora $X = \{2, 3\}$. Nuevamente, por el Teorema 4.5.20,

$$\langle \{2, 3\} \rangle = \{2x : x \in \mathbb{Z}\} \cup \{3y : y \in \mathbb{Z}\} \cup \{2x + 3y : x, y \in \mathbb{Z}\} = \{2x + 3y : x, y \in \mathbb{Z}\}$$

donde en este caso la última igualdad vale pues podemos tomar $x = 0$ o $y = 0$.

Ahora bien, $1 = 3 - 2 \in \langle \{2, 3\} \rangle$. Como $\langle \{2, 3\} \rangle$ es un grupo, tendremos que $k \cdot 1 \in \langle \{2, 3\} \rangle$ para todo $k \in \mathbb{Z}$. Esto es, $\langle \{1\} \rangle \subseteq \langle \{2, 3\} \rangle$, y por lo tanto $\mathbb{Z} \subseteq \langle \{2, 3\} \rangle$. Concluimos que $\langle \{2, 3\} \rangle = \mathbb{Z}$. Dejamos como **ejercicio** probar que si $m, n \in \mathbb{Z}$ son coprimos, es decir $\text{m. c. d.}(m, n) = 1$, entonces $\langle \{m, n\} \rangle = \mathbb{Z}$.

Tomemos ahora $X = \{12, 15\}$. Entonces

$$\langle \{12, 15\} \rangle = \{12x + 15y : x, y \in \mathbb{Z}\}.$$

Observemos que $1 \notin \langle \{12, 15\} \rangle$, pues en ese caso deberían existir $x, y \in \mathbb{Z}$ tales que $1 = 12x + 15y$, y por lo tanto tendríamos $\text{m. c. d.}(12, 15) = 1$, lo que no ocurre. Por lo tanto $\langle \{12, 15\} \rangle \neq \mathbb{Z}$. Sin embargo, $12 = 3 \cdot 4$ y $15 = 3 \cdot 5$. Luego, cada elemento $k \in \langle \{12, 15\} \rangle$ puede escribirse como

$$k = 3(4x + 5y), \quad \text{con } x, y \in \mathbb{Z}.$$

Ahora bien, $\text{m. c. d.}(4, 5) = 1$, y por lo tanto existirán $x_0, x_1 \in \mathbb{Z}$ tales que $4x_0 + 5x_1 = 1$. Concluimos que $3 = 3(4x_0 + 5x_1) \in \langle \{12, 15\} \rangle$ y con el mismo argumento que antes tendremos que $\langle \{12, 15\} \rangle$ contiene a todos los múltiplos de 3, esto es,

$$\text{Mul}(3) \subseteq \langle \{12, 15\} \rangle.$$

Si ahora $k = 12x + 15y$, entonces trivialmente $3 \mid k$ dado que $3 \mid 12$ y $3 \mid 15$. Luego $k \in \text{Mul}(3)$. Concluimos que $\langle \{12, 15\} \rangle = \text{Mul}(3)$. Dejamos como **ejercicio** probar que si $n, m \in \mathbb{Z}$, entonces $\langle \{m, n\} \rangle = \text{Mul}(\text{m. c. d.}(m, n))$. ■

4.6. Grupos cíclicos

Definición 4.6.1. Sea (G, \cdot) un grupo. El grupo generado por un conjunto de la forma $\{a\}$ se denomina **subgrupo cíclico** de G generado por a y se denota $\langle a \rangle$.

Si existe $a \in G$ tal que $G = \langle a \rangle$, G se dice un **grupo cíclico** y a un **generador** de G .

Recordemos que por definición, el grupo cíclico generado por a es el menor subgrupo de G que contiene a a por lo tanto:

Lema 4.6.2. Sea (G, \cdot) un grupo y sea H un subgrupo de G . Si $a \in H$, entonces $\langle a \rangle < H$.

Como consecuencia inmediata del Teorema 4.5.20 tenemos además:

Corolario 4.6.3. Sea (G, \cdot) un grupo y sea $a \in G$. Entonces $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ (en notación aditiva, $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$).

Definición 4.6.4. Sea G un grupo y $a \in G$. Se denomina **orden de G** al cardinal de G de lo denota $o(G)$. Se denomina **orden de a** al orden del grupo cíclico $\langle a \rangle$ generado por a . Se lo denota $o(a)$.

Observación 4.6.5. En cualquier grupo (G, \cdot) con identidad e , $\langle e \rangle = \{e\}$ y por lo tanto $o(e) = 1$. Si $a \neq e$, entonces al menos $e, a \in \langle a \rangle$, con lo cual $o(a) \geq 2$. Luego e es el único elemento de orden 1 de G .

Ejemplo 4.6.6. Generadores de $(\mathbb{Z}, +)$. Hemos visto que $\mathbb{Z} = \langle 1 \rangle$, con lo cual \mathbb{Z} es un grupo cíclico de orden infinito generado por 1. También $\mathbb{Z} = \langle -1 \rangle$, con lo cual -1 también es un generador de \mathbb{Z} .

Para cualquier $m \in \mathbb{Z}$ distinto de ± 1 , $\langle m \rangle = \text{Mul}(m)$, el subgrupo de los múltiplos de m . Si $m = 0$, $\langle m \rangle = \{0\}$ y si $m \neq 0$, $m \neq \pm 1$, $\langle m \rangle$ es un subgrupo propio de \mathbb{Z} .

Concluimos que ± 1 son los únicos generadores de \mathbb{Z} . ■

Ejemplo 4.6.7. Generadores de $(\mathbb{Z}_m, +)$. El grupo $(\mathbb{Z}_m, +)$ también es un grupo cíclico, dado que para cada $\bar{x} \in \mathbb{Z}_m$, $\bar{x} = \overline{x \cdot 1}$ y por el Ejercicio 15 de este capítulo, $\overline{x \cdot 1} = x \cdot \bar{1}$. Luego $\langle \bar{1} \rangle = \mathbb{Z}_m$.

¿Existen otros generadores de \mathbb{Z}_m ? Supongamos que \bar{a} es un generador. Entonces para cada $\bar{x} \in \mathbb{Z}_m$, deberá existir $k \in \mathbb{Z}$ tal que $\bar{x} = k\bar{a} = \overline{ka}$. En particular, debe existir $k \in \mathbb{Z}$ tal que $\bar{1} = \overline{ka}$, o sea $1 - ka$ es un múltiplo de m . Luego existirá además $k' \in \mathbb{Z}$ tal que $1 - ka = k'm$, o lo que es lo mismo, $ka + k'm = 1$. Concluimos que si a es un generador de \mathbb{Z}_m , entonces $\text{m. c. d.}(a, m) = 1$.

Recíprocamente, supongamos que $\text{m. c. d.}(a, m) = 1$. Entonces existen $k, k' \in \mathbb{Z}$ tales que $ka + k'm = 1$, y por lo tanto

$$\bar{1} = \overline{ka + k'm} = \overline{ka} + \overline{k'm} = \overline{ka} + \bar{0} = k\bar{a}$$

Luego, dado $\bar{x} \in \mathbb{Z}_m$, $\bar{x} = x\bar{1} = (kx)\bar{a}$ y por lo tanto \bar{a} es un generador de $(\mathbb{Z}_m, +)$.

Concluimos entonces que \bar{a} es un generador de $(\mathbb{Z}_m, +)$ si y sólo si $\text{m. c. d.}(a, m) = 1$. En particular, si m es primo, todos los elementos son generadores. ■

Ejemplo 4.6.8. Consideremos el grupo diedral $D_3 = \{\text{Id}, R_1, R_2, S_0, S_1, S_2\}$ (ver Ejemplo 4.3.9). Entonces observando la tabla de Cayley de D_3 tenemos que:

$$\langle \text{Id} \rangle = \{\text{Id}\}, \quad \langle R_1 \rangle = \{\text{Id}, R_1, R_2\} = \langle R_2 \rangle, \quad \langle S_0 \rangle = \{\text{Id}, S_0\}, \quad \langle S_1 \rangle = \{\text{Id}, S_1\}, \quad \langle S_2 \rangle = \{\text{Id}, S_2\}.$$

Tenemos entonces que $o(\text{Id}) = 1$, $o(R_1) = o(R_2) = 3$, $o(S_0) = o(S_1) = o(S_2) = 2$. Concluimos que D_3 no es cíclico, pero $D_3 = \langle \{S_0, S_1, S_2\} \rangle$.

Si ahora tomamos el grupo diedral $D_n = \{R_i, S_i\}_{i=0, \dots, n}$ tenemos que $S_i^2 = S_i \circ S_i = R_{i-i} = R_0 = \text{Id}$, y por lo tanto

$$S_i^k = \begin{cases} \text{Id} & \text{si } k \text{ es par} \\ S_i & \text{si } k \text{ es impar} \end{cases}$$

con lo cual $\langle S_i \rangle = \{\text{Id}, S_i\}$ y $o(S_i) = 2$ para cada $i = 1, \dots, n$.

Por otra parte, $R_1^k = R_k$, con lo cual $\langle R_1 \rangle = \{R_i\}_{i=0, \dots, n-1}$.

Consideremos el subgrupo $H = \{R_i\}_{i=0, \dots, n}$ de D_3 . Entonces H es cíclico y R_1 es un generador. Para un índice i genérico, tenemos que

$$R_i^k = R_{k_0}, \quad \text{donde } k_0 \equiv ki \pmod{n}$$

Por lo tanto tendremos que R_i es un generador de H si y sólo si i es un generador de \mathbb{Z}_n , es decir, si $\text{m.c.d.}(i, n) = 1$. ■

Enunciamos en el siguiente resultado las conclusiones de los ejemplos anteriores:

Lema 4.6.9. $(\mathbb{Z}, +)$ y $(\mathbb{Z}_m, +)$ son grupos cíclicos para cada $m \in \mathbb{N}$. Los únicos generadores de $(\mathbb{Z}, +)$ son ± 1 , y \bar{a} es un generador de $(\mathbb{Z}_m, +)$ si y sólo si $\text{m.c.d.}(a, m) = 1$.

Teorema 4.6.10 (Subgrupos de \mathbb{Z}). Sea H un subgrupo de $(\mathbb{Z}, +)$. Entonces $H = \langle m \rangle$ para algún $m \in \mathbb{Z}$.

Demostración. Ya vimos en el Ejemplo 4.5.16 que $H = \text{Mul}(m) = \langle m \rangle$ es un subgrupo de \mathbb{Z} cualquiera sea $m \in \mathbb{Z}$. Observemos que $\mathbb{Z} = \langle 1 \rangle$ y $\{0\} = \langle 0 \rangle$, es decir, los subgrupos triviales de $(\mathbb{Z}, +)$ son de subgrupos cíclicos de $(\mathbb{Z}, +)$.

Sea ahora H un subgrupo propio cualquiera de $(\mathbb{Z}, +)$. En particular $H \neq \{0\}$. Luego $S = H \cap \mathbb{N}$ es no vacío (pues al ser subgrupo, debe contener cada elemento y su opuesto, y uno de ellos es positivo). Por el principio del buen orden (Teorema 2.3.1) S tiene un elemento mínimo, digamos $m \in H$. Probaremos que $\langle m \rangle = H$.

Como $m \in H$, del Lema 4.6.2 resulta $\langle m \rangle \subset H$.

Si ahora $h \in H$ podemos aplicar el algoritmo de la división para dividir h por m y obtener $h = qm + r$, con $0 \leq r < m$. Como h y qm son elementos de H , resulta $r = h - qm \in H$. Si $r > 0$, entonces $r \in S$. Pero $r < m$ lo que lleva a una contradicción. Luego debe ser $r = 0$ y por lo tanto $h \in \langle m \rangle$. Concluimos que $H \subset \langle m \rangle$ y por lo tanto $H = \langle m \rangle$. □

4.7. Morfismos

Al estudiar conjuntos con operaciones binarias nos interesa estudiar las funciones entre ellos que preserven estas operaciones. Estas funciones reciben el nombre genérico de *morfismos*. Más específicamente, si $(X, *)$ y (Y, \odot) son conjuntos con operaciones binarias, un **morfismo** de $(X, *)$ en (Y, \odot) es una función $f : X \rightarrow Y$ tal que

$$(4.2) \quad f(x * y) = f(x) \odot f(y).$$

Como es esperable, no siempre un morfismo entre dos conjuntos con operaciones binarias preserva las demás características que puede tener ese conjunto (como por ejemplo mapear neutro en neutro o inversos en inversos, si los hubiese). Es por eso que para definir un morfismo entre las distintas estructuras algebraicas debemos pensar en qué propiedades extra tendremos que pedirle a la función f .

Como los semigrupos no tienen elementos característicos, definimos:

Definición 4.7.1. Sean $(X, *)$ e (Y, \odot) semigrupos. Una función $f : X \rightarrow Y$ que verifique (4.2) se denomina un **morfismo** u **homomorfismo de semigrupos**.

Ejemplo 4.7.2. Consideremos la función $f : \mathbb{N} \rightarrow \mathbb{N}$, $f(n) = 2n$. Si $m, n \in \mathbb{N}$ tenemos

$$f(n + m) = 2(n + m) = 2n + 2m = f(n) + f(m).$$

Concluimos que f es un homomorfismo de semigrupos de $(\mathbb{N}, +)$ en $(\mathbb{N}, +)$.

Pero f no es un homomorfismo de semigrupos de (\mathbb{N}, \cdot) en (\mathbb{N}, \cdot) , pues por ejemplo $f(2 \cdot 3) = f(6) = 12$, pero $f(2) \cdot f(3) = 4 \cdot 6 = 24$.

Por lo tanto para establecer si una función entre dos conjuntos es o no un homomorfismo es indispensable conocer las operaciones de las cuales están dotados esos conjuntos. ■

Ejemplo 4.7.3. Sea $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_{2 \times 2}$. Sea $(X, *)$ un semigrupo cualquiera y definamos $f : X \rightarrow Y$, $f(x) = a$ para cada $x \in X$. Como $a^2 = a$, tendremos que $f(x * y) = a = a \cdot a = f(x) \cdot f(y)$ con lo cual f es un homomorfismo de semigrupos de $(X, *)$ en $(M_{2 \times 2}, \cdot)$.

Observemos que $(M_{2 \times 2}, \cdot)$ es un monoide. Luego si $(X, *)$ es un monoide, f será un morfismo para el cual $f(e_X) = a \neq \text{Id}$. Es decir, un morfismo que sólo verifique (4.2) no necesariamente mapea la identidad del dominio en la identidad del codominio. ■

El Ejemplo 4.7.3 muestra que para definir un homomorfismo de monoides, y que se preserven los elementos característicos, debemos imponer una condición más a la dada por (4.2):

Definición 4.7.4. Sean $(X, *)$ e (Y, \odot) monoides con identidades e_X y e_Y respectivamente. Una función $f : X \rightarrow Y$ se denomina un **morfismo** u **homomorfismo de monoides** si f verifica (4.2) y $f(e_X) = e_Y$.

Ejemplo 4.7.5. Sean (L, \vee, \wedge) y (L', \vee', \wedge') dos retículos acotados, con máximos 1 y $1'$ y mínimos 0 y $0'$ respectivamente. Entonces (L, \vee) es un monoide con neutro 0 y (L, \wedge) es un monoide con neutro 1, y lo mismo ocurre con L' . En particular, (L, \vee) , (L, \wedge) , (L', \vee') , (L', \wedge') son semigrupos.

Un morfismo de retículos $f : L \rightarrow L'$ es un homomorfismo de semigrupos de (L, \vee) en (L', \vee') y de (L, \wedge) en (L', \wedge') . Para que f sea un morfismo de monoides debe ocurrir que $f(0) = 0'$ y $f(1) = 1'$, esto es, f es un morfismo de retículos $\{0, 1\}$. ■

Siguiendo con la línea de razonamiento con la que definimos los morfismos de semigrupos y monoides daremos a continuación la definición de morfismo de grupos. Advertimos desde ya que esta definición no es estándar, dado que impone una serie de condiciones a un morfismo de grupos que, como veremos inmediatamente, son innecesarias. Sin embargo, elegimos seguir el criterio que adoptamos hasta ahora: un morfismo entre dos estructuras cualesquiera debe ser una función que preserve la operación que define la estructura y todos sus elementos característicos:

Definición 4.7.6. Sean (G, \cdot) y $(H, *)$ dos grupos. Una función $f : G \rightarrow H$ se denomina un **homomorfismo de grupos** si verifica las siguientes condiciones:

1. vale (4.2), esto es, $f(x \cdot y) = f(x) * f(y)$ para cada $x, y \in G$.
2. $f(e_G) = e_H$
3. $f(x^{-1}) = (f(x))^{-1}$ para cada $x \in G$.

Teorema 4.7.7. Sean (G, \cdot) y $(H, *)$ grupos. Entonces $f : G \rightarrow H$ es un homomorfismo de grupos si y sólo si f es un homomorfismo de semigrupos, es decir, verifica (4.2).

Demostración. Claramente, si f es un homomorfismo de grupos, entonces f verifica (4.2).

Supongamos entonces que $f : G \rightarrow H$ es un homomorfismo de semigrupos. Para ver que f envía el neutro de G en el neutro de H observemos que

$$e_H * f(e_G) = f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$$

Multiplicando a derecha ambos lados de la igualdad por $f(e_G)^{-1}$, obtenemos que $e_H = f(e_G)$ como queríamos probar.

Por otra parte, si $x \in G$, entonces $f(x \cdot x^{-1}) = f(e_G) = e_H$. Luego

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = e_H$$

de donde $f(x^{-1}) = f(x)^{-1}$. □

Observación 4.7.8. Como ya hemos advertido, en casi toda la bibliografía se define un morfismo de grupos como una función que verifica (4.2) y se obtienen las otras condiciones directamente como propiedades.

Teorema 4.7.9. Sean X, Y, Z semigrupos (resp. monoides o grupos) y $f : X \rightarrow Y$, $g : Y \rightarrow Z$ homomorfismos de semigrupos (resp. monoides o grupos). Entonces, para las estructuras correspondientes,

1. $g \circ f$ es un homomorfismo.
2. Si f es biyectivo, entonces f^{-1} es un homomorfismo.

Demostración. Sean $(X, *)$, (Y, \odot) y (Z, \cdot) semigrupos. Entonces:

$$g \circ f(x * y) = g(f(x * y)) = g(f(x) \odot f(y)) = g(f(x)) \cdot g(f(y)) = (g \circ f(x)) \cdot (g \circ f(y)).$$

Luego $g \circ f$ es un homomorfismo de semigrupos. Automáticamente, resulta del Teorema 4.7.7 que si X, Y, Z son grupos, $g \circ f$ es un homomorfismo de grupos.

Si X, Y, Z son monoides, como f y g son homomorfismos de monoides entonces $f(e_X) = e_Y$ y $g(e_Y) = e_Z$. Luego

$$g \circ f(e_X) = g(f(e_X)) = g(e_Y) = e_Z,$$

con lo cual $g \circ f$ es un homomorfismo de monoides.

Sea $f : (X, *) \rightarrow (Y, \odot)$ es un homomorfismo biyectivo. Sean $u, v \in Y$ y $x, y \in X$ tales que $f(x) = u$, $f(y) = v$. Entonces

$$f^{-1}(u \odot v) = f^{-1}(f(x) \odot f(y)) = f^{-1}(f(x * y)) = x * y = f^{-1}(u) * f^{-1}(v).$$

Luego si X e Y son semigrupos, f^{-1} es un homomorfismo de semigrupos y lo mismo ocurre si X e Y son grupos. Finalmente, si X e Y son monoides, como $f(e_X) = e_Y$, entonces $f^{-1}(e_Y) = e_X$ con lo cual f^{-1} también es un homomorfismo de monoides. \square

Definición 4.7.10. Sea f un homomorfismo de semigrupos, monoides o grupos. Decimos que

- f es un **monomorfismo** si f es inyectivo.
- f es un **epimorfismo** si f es sobreyectivo.
- f es un **isomorfismo** si f es biyectivo y f^{-1} es un morfismo.

Como consecuencia del Teorema 4.7.9 resulta inmediato que:

Corolario 4.7.11. Sean $f : X \rightarrow Y$, $g : Y \rightarrow Z$ homomorfismos de semigrupos, monoides o grupos. Entonces:

1. f es un isomorfismo si y sólo si f es biyectivo.
2. Si f y g son monomorfismos, epimorfismos o isomorfismos, entonces $g \circ f$ también es un monomorfismo, epimorfismo, isomorfismo resp.

Ejemplo 4.7.12. Sea $(X, *)$ un semigrupo, monoide o grupo. Es evidente que $\text{Id} : (X, *) \rightarrow (X, *)$ es un isomorfismo. Más aún, si $(Y, *)$ es un subsemigrupo, submonoide o subgrupo respectivamente, la inclusión $i : (Y, *) \rightarrow (X, *)$ (que no es más que Id_Y) es un monomorfismo. \blacksquare

Definición 4.7.13. Dos semigrupos, monoides o grupos X e Y se dicen **isomorfos** si existe un isomorfismo $f : X \rightarrow Y$.

Como la identidad es un isomorfismo, el inverso de un isomorfismo es un isomorfismo y la composición de isomorfismos es un isomorfismo, tenemos:

Corolario 4.7.14. La relación $X \sim Y$ si y sólo si X e Y son isomorfos es una relación de equivalencia en el conjunto de todos los semigrupos, monoides o grupos respectivamente.

Ejemplo 4.7.15. Consideremos la proyección al cociente $f : \mathbb{Z} \rightarrow \mathbb{Z}_m$, para un $m \in \mathbb{Z}$ cualquiera. Esto es, $f(x) = \bar{x}$. Hemos visto que $\bar{x} + \bar{y} = \overline{x+y}$, que expresado en términos de f significa que

$$f(x+y) = f(x) + f(y)$$

y por lo tanto f es un homomorfismo de grupos. f es claramente un epimorfismo, pero no es un monomorfismo pues $f(x+km) = f(x)$ para cualquier $k \in \mathbb{Z}$. ■

Ejemplo 4.7.16. Sea $\mathcal{R} = \{R_\theta : \theta \in \mathbb{R}\}$ el grupo de rotaciones del plano alrededor del origen, con la composición de funciones (ver el Ejemplo 4.3.7). Consideremos $f : (\mathbb{R}, +) \rightarrow (\mathcal{R}, \circ)$ dada por $f(\theta) = R_\theta$. Tenemos entonces

$$f(\theta + \rho) = R_{\theta+\rho} = R_\theta \circ R_\rho = f(\theta) \circ f(\rho)$$

con lo cual f es un homomorfismo de grupos.

Claramente f es un epimorfismo (pues cada rotación está definida por un ángulo), pero no es un monomorfismo pues $f(\theta + 2k\pi) = f(\theta)$ para cualquier $\theta \in \mathbb{R}$ y cualquier $k \in \mathbb{Z}$. ■

Definición 4.7.17. Sea X un semigrupo, monoide o grupo. Un homomorfismo $f : X \rightarrow X$ se denomina un **endomorfismo** y un isomorfismo $f : X \rightarrow X$ se denomina un **automorfismo**.

Teorema 4.7.18. Sea X un semigrupo, monoide o grupo. Entonces el conjunto

$$\text{Aut}(X) = \{f : X \rightarrow X : f \text{ es un automorfismo de } X\}$$

es un grupo con la composición de funciones.

Demostración. Observemos que $\text{Aut}(X) \subset \mathcal{B}(X)$, el conjunto de biyecciones de X , que es un grupo con la composición de funciones. Luego, en vistas del Teorema 4.5.11 bastará probar que $\text{Aut}(X)$ es un subgrupo de $(\mathcal{B}(X), \circ)$.

Ahora bien, si $f, g \in \text{Aut}(X)$, entonces por el Corolario 4.7.11 resulta que $g^{-1} \in \text{Aut}(X)$ y $f \circ g^{-1} \in \text{Aut}(X)$. Luego del Teorema 4.5.12 concluimos que $(\text{Aut}(X), \circ)$ es un subgrupo de $(\mathcal{B}(X), \circ)$. □

Definición 4.7.19. Sea $(X, *)$ un semigrupo, monoide o grupo. El grupo $(\text{Aut}(X), \circ)$ se denomina **grupo de automorfismos de X** .

Ejemplo 4.7.20. Sea G un grupo y $a \in G$. Consideremos la aplicación $I_a : G \rightarrow G$ dada por $I_a(g) = aga^{-1}$. Veamos que I_a es un automorfismo de G . Observemos primero que

$$I_a(g_1g_2) = ag_1g_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = I_a(g_1)I_a(g_2).$$

Por lo tanto I_a es un endomorfismo de G . Además, si $I_a(g) = I_a(g')$, entonces $aga^{-1} = ag'a^{-1}$, y multiplicando a derecha por a e izquierda por a^{-1} ambos miembros de la igualdad resulta $g = g'$. Luego I_a es un monomorfismo.

Finalmente, dado $g' \in G$, pongamos $g = a^{-1}g'a \in G$. Entonces $I_a(g) = a(a^{-1}g'a)a^{-1} = g'$, con lo cual I_a es sobre y por lo tanto un automorfismo. ■

Definición 4.7.21. Sea G un grupo y $a \in G$. El automorfismo $I_a : G \rightarrow G$ se denomina **conjugación por a** . Si un automorfismo $f \in \text{Aut}(G)$ es la conjugación por un elemento de G , entonces f se denomina un **automorfismo interior** de G .

Veremos a continuación como se comportan las subestructuras de una estructura dada (semigrupo, monoide o grupo) via un homomorfismo.

Teorema 4.7.22. Sea $f : X \rightarrow Y$ un homomorfismo de semigrupos, monoides o grupos. Entonces

1. Si Z es una subestructura de X (subsemigrupo, submonoide o subgrupo según corresponda) entonces $f(Z)$ es una subestructura de Y . Si f es un monomorfismo, Z y $f(Z)$ son estructuras isomorfas.
2. Si W es una subestructura de Y , entonces $f^{-1}(W)$ es una subestructura de X .

Demostración. Sea Z una subestructura de (X, \cdot) y veamos que $f(Z)$ es una subestructura de $(Y, *)$. Para ello sean $b_1, b_2 \in f(Z)$ y sean $a_1, a_2 \in Z$ tales que $f(a_1) = b_1$ y $f(a_2) = b_2$. Como Z es una subestructura de X , $a_1 \cdot a_2 \in Z$.

Supongamos primero que X y Y son semigrupos y Z es un subsemigrupo de X . Entonces

$$b_1 * b_2 = f(a_1) * f(a_2) = f(a_1 \cdot a_2) \in f(Z)$$

Luego $f(Z)$ es un subsemigrupo de Y .

Si X y Y son monoides con identidad e_X y e_Y respectivamente y Z es un submonoide de X , entonces $e_X \in Z$. Además $f(Z)$ es un subsemigrupo de Y y, al ser f un homomorfismo de monoides, $e_Y = f(e_X) \in f(Z)$. Luego $f(Z)$ es un submonoide de Y .

Finalmente si X y Y son grupos, y Z es un subgrupo de X , entonces $a_1a_2^{-1} \in Z$. Luego

$$b_1 * b_2^{-1} = f(a_1) * f(a_2)^{-1} = f(a_1) * f(a_2^{-1}) = f(a_1 \cdot a_2^{-1}) \in f(Z).$$

Concluimos por el Teorema 4.5.12 que $f(Z)$ es un subgrupo de Y .

Supongamos ahora que f es un monomorfismo. Entonces es inmediato que $f|_Z : Z \rightarrow f(Z)$ es un isomorfismo, y por lo tanto Z y $f(Z)$ son isomorfas.

Probaremos el punto 2 solo para el caso en que X e Y son grupos y f es un homomorfismo de grupos. Los demás casos son similares y los dejamos como **ejercicio**.

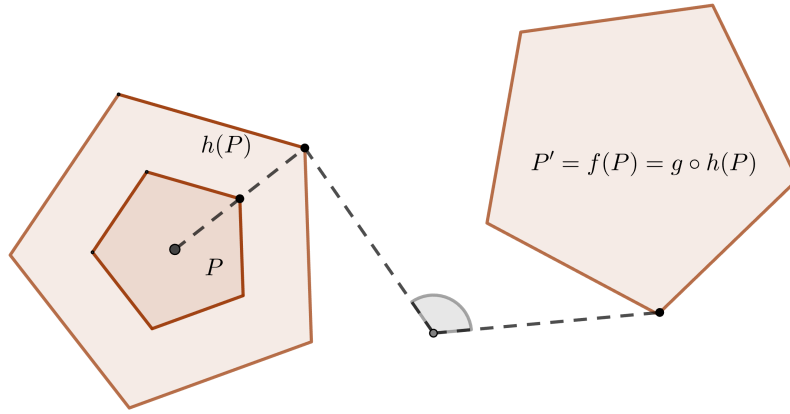
Supongamos entonces que W es un subgrupo de Y y sean $a_1, a_2 \in f^{-1}(W)$. Entonces $f(a_1), f(a_2) \in W$, y por lo tanto

$$f(a_1) * f(a_2)^{-1} \in W \implies f(a_1 \cdot a_2^{-1}) \in W$$

con lo cual $a_1 \cdot a_2^{-1} \in f^{-1}(W)$ y por el Teorema 4.5.12 resulta que $f^{-1}(W)$ es un subgrupo de X . \square

Ejemplo 4.7.23. Probaremos en este ejemplo que los grupos diedrales asociados a polígonos regulares con la misma cantidad de lados son isomorfos (ver Ejemplo 4.3.9)

Sean P y P' dos polígonos regulares de n lados. P y P' son polígonos *semejantes* y por lo tanto existe una homotecia $h : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ (es decir, una transforación de la forma $h(v) = \lambda v$ para algún $\lambda > 0$) y una isometría $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ tal que $f = g \circ h : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ mapea P en P' , es decir, $f(P) = P'$. Observemos que h es biyectiva con $h^{-1}(v) = \frac{1}{\lambda}v$. Pongamos $\tilde{P} = f(P)$. Entonces \tilde{P} es un polígono regular de n lados y $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ es una isometría tal que $g(\tilde{P}) = P'$ (y por lo tanto $g^{-1}(P') = \tilde{P}$).



Denotemos por D_n , \tilde{D}_n y D'_n los grupos diedrales asociados a P , \tilde{P} y P' respectivamente. Esto es, D_n , \tilde{D}_n y D'_n son las isometrías del plano que dejan P , \tilde{P} y P' invariantes respectivamente. En particular $D_n < \text{Iso}(\mathbb{R}^2) < \mathcal{B}(\mathbb{R}^2)$ y lo mismo ocurre con \tilde{D}_n y con D'_n .

Como $g \in \text{Iso}(\mathbb{R}^2)$, la conjugación $I_g : \text{Iso}(\mathbb{R}^2) \rightarrow \text{Iso}(\mathbb{R}^2)$ es un automorfismo de grupos. Supongamos que $a \in \tilde{D}_n$, es decir, $a(\tilde{P}) = \tilde{P}$. Entonces si $b = I_g(a)$, resulta

$$b(P') = g(a(\underbrace{g^{-1}(P')}_{\tilde{P}})) = g(\underbrace{a(\tilde{P})}_{\tilde{P}}) = g(\tilde{P}) = P'.$$

Concluimos que $I_g(\tilde{D}_n) \subseteq D'_n$. Si ahora $b \in D'_n$, de manera análoga se prueba que $a = I_g^{-1}(b) \in \tilde{D}_n$ y $f(a) = b$. Luego $I_g(\tilde{D}_n) = D'_n$ y por el Teorema 4.7.22 resulta $\tilde{D}_n \simeq D'_n$.

Consideremos la conjugación por h en $\mathcal{B}(\mathbb{R}^2)$. Sea $a \in \text{Iso}(\mathbb{R}^2)$, es decir, para cada $v, w \in \mathbb{R}^2$,

$$d(a(v), a(w)) = d(v, w).$$

Veamos que $I_h(a) \in \text{Iso}(\mathbb{R}^2)$. Pongamos $b = I_h(a) = h \circ a \circ h^{-1}$, es decir, si $v \in \mathbb{R}^2$,

$$b(v) = \lambda a(\lambda^{-1}v).$$

Entonces si $v, w \in \mathbb{R}^2$,

$$\begin{aligned} d(b(v), b(w)) &= d(\lambda a(\lambda^{-1}v), \lambda a(\lambda^{-1}w)) = \lambda d(a(\lambda^{-1}v), a(\lambda^{-1}w)) = \lambda^{-1}d(\lambda v, \lambda w) \\ &= \lambda^{-1}\lambda d(v, w) = d(v, w). \end{aligned}$$

Concluimos que $I_h(\text{Iso}(\mathbb{R}^2)) \subseteq \text{Iso}(\mathbb{R}^2)$. La otra contención es análoga al caso anterior, y por lo tanto $I_h(\text{Iso}(\mathbb{R}^2)) = \text{Iso}(\mathbb{R}^2)$. Tenemos entonces que $I_h|_{\text{Iso}(\mathbb{R}^2)} : \text{Iso}(\mathbb{R}^2) \rightarrow \text{Iso}(\mathbb{R}^2)$ es un automorfismo de grupos. Ahora, de la misma manera que probamos que $I_g(\tilde{D}_n) = D'_n$ podemos probar que $I_h(D_n) = \tilde{D}_n$. Por lo tanto concluimos que $D_n \simeq \tilde{D}_n \simeq D'_n$. ■

Ejemplo 4.7.24. Consideremos la función determinante, $\det : (GL(n, \mathbb{R}), \cdot) \rightarrow (\mathbb{R}^*, \cdot)$. Recordemos que $\det(A \cdot B) = \det(A) \cdot \det(B)$, y por lo tanto \det es un homomorfismo de grupos.

El conjunto $\{1\}$ es un subgrupo de \mathbb{R}^* , dado que 1 es la identidad. Por lo tanto $\det^{-1}(1)$ es un subgrupo de $GL(n, \mathbb{R})$, denominado *grupo lineal especial* y denotado por $SL(n, \mathbb{R})$. Más precisamente,

$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det A = 1\}$$

es un subgrupo de $GL(n, \mathbb{R})$. ■

Ejemplo 4.7.25. El ejemplo anterior puede generalizarse a cualquier homomorfismo de grupos. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Entonces $K = f^{-1}(e_H)$ es un subgrupo de G , pues es la preimagen del subgrupo trivial $\{e_H\}$ de H . ■

Definición 4.7.26. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Se denomina **núcleo** o **kernel** de f al subgrupo de G dado por

$$\ker(f) = \{x \in G : f(x) = e_H\} = f^{-1}(e_H)$$

Teorema 4.7.27. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Entonces: f es un monomorfismo si y sólo si $\ker(f) = \{e_G\}$.

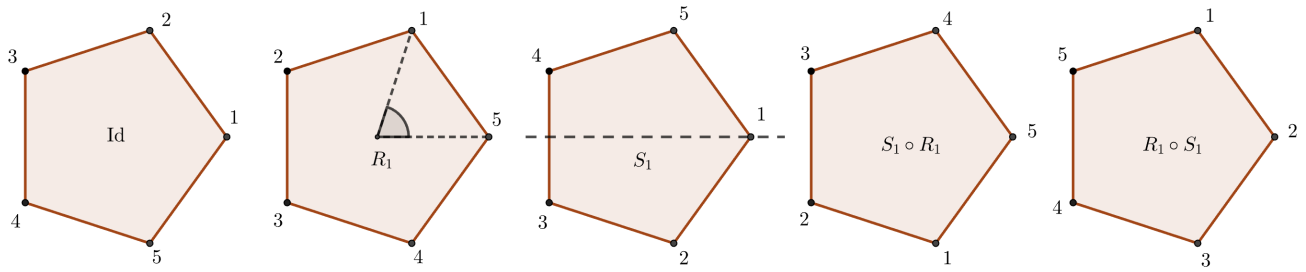
Demostración. Supongamos que f es un monomorfismo y sea $a \in G$ tal que $a \in \ker(f)$, o sea, $f(a) = e_H$. Como $f(e_G) = e_H$, resulta $f(a) = f(e_G)$, y como f es inyectiva, $a = e_G$. Luego $\ker(f) = \{e_G\}$.

Supongamos ahora que $\ker(f) = \{e_G\}$ y sean $a_1, a_2 \in G$ tales que $f(a_1) = f(a_2)$. Entonces

$$f(a_1)f(a_2)^{-1} = e_H \implies f(a_1a_2^{-1}) = e_H$$

Luego $a_1a_2^{-1} \in \ker(f) = \{e_G\}$, y por lo tanto $a_1a_2^{-1} = e_G$, de donde $a_1 = a_2$ y f es inyectiva. □

Ejemplo 4.7.28. Consideremos el grupo diedral D_n asociado a un polígono regular P_n . Como cada elemento $f \in D_n$ deja el polígono P_n invariante (es decir, $f(P_n) = P_n$), f debe mapear cada vértice de P_n a un vértice de P_n . Luego, si $X = \{x_1, \dots, x_n\}$ son los vértices de P_n , podemos pensar a f como una biyección $f|_X : X \rightarrow X$, restringiendo tanto el dominio como el codominio. La función $\varphi : (D_n, \circ) \rightarrow (\mathcal{B}(X), \circ)$ es claramente un homomorfismo (pues las operaciones en el dominio y el codominio son las mismas, y φ es esencialmente una inclusión). Además si $f : P_n \rightarrow P_n$ deja fijos todos los vértices de P_n (es decir, $\varphi(f) = \text{Id}$), entonces f debe ser la identidad (dejamos los detalles como **ejercicio**). De esta manera, $\ker \varphi = \{\text{Id}\}$ y por lo tanto $\varphi : D_n \rightarrow \mathcal{B}(X)$ es un monomorfismo. Por otra parte $\mathcal{B}(X) \simeq S_n$, con lo cual D_n es isomorfo a $\varphi(D_n)$ que es un subgrupo de S_n . En la siguiente figura mostramos cómo actúan sobre los vértices del pentágono regular la rotación R_1 , la simetría S_1 y sus composiciones:



En este caso, por ejemplo,

$$\varphi(R_1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad \varphi(S_1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Observemos que $o(D_n) = 2n$ y $o(S_n) = n!$ por lo tanto $\varphi(D_n) \neq S_n$ a menos que $n = 3$. En ese caso tendremos que $D_3 \simeq S_3$. ■

4.8. Ejercicios

1. En las tablas siguientes se muestra una operación $*$ en el conjunto $X = \{a, b, c\}$ e $Y = \{a, b, c, d, e\}$ respectivamente. Analizar las propiedades de $*$.

a)

$*$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

b)

$*$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	a	e	d
c	c	d	e	a	b
d	d	e	b	c	a
e	e	a	d	b	c

2. Considerar en \mathbb{R} la operación $x * y = \sqrt[3]{x^3 + y^3}$ y analizar sus propiedades.
3. Analizar que propiedades tienen la unión y la intersección de relaciones en Rel_A , siendo $A \neq \emptyset$.

4. Probar que una operación admite a lo sumo un elemento absorbente. Dar un ejemplo de un conjunto con una operación que admita más de un elemento absorbente a derecha o izquierda.
5. Sea $n \in \mathbb{N}$ fijo y consideremos $Y_n = \{z \in \mathbb{C} : z^n = 1\}$ el conjunto de las raíces n -ésimas de 1. Probar que Y_n es cerrado bajo el producto usual en \mathbb{C} y analizar qué propiedades tiene el producto en Y_n .
6. Consideremos la relación \sim en \mathbb{R} dada por $x \sim y$ si $x - y \in \mathbb{Z}$.
 - a) Probar que \sim es una relación de equivalencia en \mathbb{R} y que la suma se induce al cociente \mathbb{R}/\sim .
 - b) ¿Se induce al cociente el producto en \mathbb{R} ?
 - c) ¿Se induce al cociente la operación del Ejercicio 2?
7. Sea $(X, *)$ un conjunto con una operación binaria y \sim una relación de equivalencia en X que se induce al cociente X/\sim . Una función $f : X \rightarrow Y$ se dice *equivariante* si para cada $x, y \in X$,

$$x \sim y \implies f(x) = f(y).$$

Probar que una función equivariante induce una función bien definida $\bar{f} : X/\sim \rightarrow Y$, dada por $\bar{f}([x]) = [f(x)]$.

8. Analizar en cada caso si el conjunto con la operación dada es un grupo, un monoide o un semigrupo.

a) $(\mathbb{Z}, -)$.

b) $(\mathbb{R}^*, /)$

c) (\mathbb{R}^+, \cdot) .

d) (\mathbb{C}, \cdot)

e) $(\mathbb{R}[x], +)$ y $(\mathbb{R}[x], \cdot)$, el conjunto de polinomios a coeficientes reales con la suma y el producto usuales de polinomios.

f) $(M(n, \mathbb{Z}), +)$, $(M(n, \mathbb{Z}), \cdot)$ y $(GL(n, \mathbb{Z}), \cdot)$ donde $M(n, \mathbb{Z})$ es el conjunto de matrices $n \times n$ con coeficientes en \mathbb{Z} y $GL(n, \mathbb{Z})$ es el subconjunto de matrices de determinante distinto de 0 en $M(n, \mathbb{Z})$, con la suma y el producto de matrices.

9. Sea $(X, *)$ un semigrupo y sea e un elemento cualquiera tal que $e \notin X$. Definimos $e * x = x * e = x$ para cada $x \in X$. Probar que si $X' = X \cup \{e\}$, entonces $(X', *)$ es un monoide.
10. Sea G un monoide en el cual todo elemento admite un inverso a derecha. Probar que G es un grupo. Llegar a la misma conclusión si todo elemento de G admite un inverso a izquierda.
11. Sea $(M, *)$ un monoide y sea G el subconjunto de M formado por los elementos invertibles de M . Probar que $(G, *)$ es un grupo.
12. Sea $(M, *)$ un monoide conmutativo y sean $x_1, x_2, \dots, x_n \in M$. Probar que $x_1 * x_2 * \dots * x_n$ es invertible si y sólo si cada x_i , $i = 1, \dots, n$ es invertible.
13. Un semigrupo se dice *cancelativo* si todo elemento es cancelativo (a derecha e izquierda). Probar que todo semigrupo cancelativo finito G es un grupo. Mostrar que esta conclusión puede ser falsa si G es infinito.

14. Sea G un grupo. Probar que las siguientes afirmaciones son equivalentes (entre paréntesis se enuncian las propiedades en notación aditiva):
- G es abeliano.
 - $(ab)^2 = a^2b^2$ para cada $a, b \in G$ ($2(a+b) = 2a+2b$).
 - $(ab)^{-1} = a^{-1}b^{-1}$ para cada $a, b \in G$ ($-(a+b) = -a+(-b)$).
 - $(ab)^n = a^n b^n$ para cada $a, b \in G$ y cada $n \in \mathbb{Z}$ ($n(a+b) = na+nb$).
15. Probar que para cada $k \in \mathbb{Z}$ y cada $\bar{a} \in \mathbb{Z}_m$, $k\bar{a} = \overline{ka}$.
16. Sean $(X, *_X)$ e $(X', *_X')$ semigrupos y sean Y, Y' subsemigrupos de X y X' respectivamente. Probar que $X \times X'$ es un subsemigrupo del semigrupo $(X \times X', *)$, donde $*$ es la operación producto.
- Resolver el mismo ejercicio cambiando semigrupo por monoide o grupo y subsemigrupo por submonoide o subgrupo respectivamente.
17. Probar que los siguiente son subgrupos del grupo $(GL(n, \mathbb{R}), \cdot)$ de matrices invertibles $n \times n$ con el producto de matrices:
- $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det A = 1\}$.
 - $Diag(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : a_{ij} = 0 \text{ si } i \neq j\}$.
 - $O(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : A^t A = Id\}$.
 - $SO(n, \mathbb{R}) = \{A \in O(n) : \det(A) = 1\}$.
18. Sea S un subconjunto finito de un grupo G . Probar que S es un subgrupo de G si y sólo si la operación de G es cerrada en S .
19. Sea G un grupo y sea
- $$Z(G) = \{a \in G : ab = ba \forall b \in G\}.$$
- Probar que $Z(G)$ es un subgrupo abeliano de G , denominado **centro** de G . Concluir que G es abeliano si y sólo si $G = Z(G)$.
 - Probar que $Z(GL(n, \mathbb{R}))$ es el subgrupo de matrices diagonales no nulas.
20. Sea $(X, *)$ un semigrupo (monoide o grupo) y sea \mathcal{S} el conjunto de subsemigrupos (submonoides o subgrupos respectivamente). Probar que (\mathcal{S}, \subseteq) es un retículo y describir las operaciones join y meet. Concluir que, en general, (\mathcal{S}, \subseteq) no es un subretículo de $(\mathcal{P}(X), \subseteq)$.
21. Sea G un grupo finito de orden par. Probar que existe un elemento $a \neq e$ de G tal que $a^2 = e$.
22. Sea G un grupo y $a, b \in G$. Probar que $o(a) = o(a^{-1})$, $o(ab) = o(ba)$ y $o(b^{-1}ab) = o(a)$.
23. Sea G el grupo multiplicativo de matrices no singulares 2×2 a coeficientes racionales. Sean $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Probar que $o(A) = 4$, $o(B) = 3$ pero AB tiene orden infinito.
24. Sean $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Probar que el subgrupo $\langle A, B \rangle$ de $GL(2, \mathbb{R})$ generado por A y B es un subgrupo no abeliano de orden 8.
25. Sean $a, b \in (\mathbb{Z}, +)$. Probar que $\langle \{a, b\} \rangle = \langle d \rangle$ donde $d = \text{m. c. d.}(a, b)$.

26. Sea $(X, *)$ un semigrupo (monoide o grupo) generado por un conjunto Y , es decir, $\langle Y \rangle = X$. Sean $f : X \rightarrow X'$ y $g : X \rightarrow X'$ homomorfismos de X en un semigrupo (resp. monoide, grupo) X' . Probar que si $f(y) = g(y)$ para cada $y \in Y$, entonces $f = g$.
27. Sea $f : X \rightarrow Y$ un homomorfismo y sea $a \in X$.
- Probar que $f(a^n) = f(a)^n$ para cada $n \in \mathbb{N}$ si X e Y son semigrupos; para cada $n \in \mathbb{N}_0$ si X e Y son monoides y para cada $n \in \mathbb{Z}$ si X e Y son grupos. Concluir que $f(\langle \{a\} \rangle) = \langle \{f(a)\} \rangle$.
 - Probar que si X es un grupo cíclico generado por a e Y es un grupo cualquiera, f está unívocamente determinado por $f(a)$, es decir, basta conocer $f(a)$ para conocer $f(x)$ para cualquier $x \in X$.
28. Sean G y H grupos isomorfos. Probar que:
- $o(G) = o(H)$.
 - $Z(H) = f(Z(G))$.
 - G es abeliano si y sólo si H es abeliano.
 - G es cíclico si y sólo si H es cíclico. En ese caso, a es un generador de G si y sólo si $f(a)$ es un generador de H .
 - Si $f : G \rightarrow H$ es el isomorfismo, $o(a) = o(f(a))$ para cada $a \in G$.
29. Sean X, X', Y, Y' semigrupos (resp. monoides o grupos) y sean $f : X \rightarrow X'$, $g : Y \rightarrow Y'$ homomorfismos.
- Probar que $f \times g : X \times Y \rightarrow X' \times Y'$ dado por $(f \times g)(x, y) = (f(x), g(y))$ es un homomorfismo.
 - Probar que si f y g son monomorfismos (resp. epimorfismos, isomorfismos), entonces $f \times g$ es un monomorfismo (resp. epimorfismo, isomorfismo).
 - Probar que $X \times Y \simeq Y \times X$.
 - Sean G y H grupos. Probar que $G \times \{e_H\}$ es un subgrupo de $G \times H$ isomorfo a G y $\{e_G\} \times H$ es un subgrupo de $G \times H$ isomorfo a H .
 - Dar un ejemplo de grupos H_1, H_2, K_1, K_2 tales que $H_1 \times H_2 \cong K_1 \times K_2$, pero H_i no es isomorfo a K_j para ningún $i, j = 1, 2$.
30. En cada uno de los siguientes casos, probar que G y H son grupos isomorfos.
- $G = (\{-1, 1\}, \cdot)$, $H = (\mathbb{Z}_2, +)$.
 - G es el grupo de elementos invertibles del monoide (\mathbb{Z}_8, \cdot) y $H = (\mathbb{Z}_2, +) \oplus (\mathbb{Z}_2, +)$.
 - $G = (\mathbb{Z}_4, +)$ y $H = \langle i \rangle$ el subgrupo cíclico de (\mathbb{C}^*, \cdot) generado por la unidad imaginaria i .
 - G es cualquier subgrupo de $(\mathbb{Z}, +)$ y $H = (\mathbb{Z}, +)$.
31. Probar que un grupo G es abeliano si y sólo si la aplicación $f : G \rightarrow G$ dada por $f(a) = a^{-1}$ es un automorfismo de G .

Grupos

5.1. Coclasas a derecha e izquierda

A partir de este capítulo indicaremos una operación genérica en un grupo G como un producto \cdot , o eventualmente como una suma $+$. En el segundo caso, 0 representará siempre el elemento neutro de G . En el caso que la operación sea un producto, indicaremos indistintamente el producto de dos elementos x e y , indistintamente por $x \cdot y$ o xy .

El objetivo de estas primeras secciones es estudiar los posibles *grupos cociente* que pueden obtenerse a partir de un grupo dado. Es decir, nos interesa determinar qué relaciones de equivalencia \sim , definidas en un grupo G , hacen que la operación de G se induzca al cociente G/\sim . Veremos que estas relaciones están unívocamente definidas por un tipo particular de subgrupos, denominados *subgrupos normales*. Para ello, comenzaremos estudiando en esta sección las denominadas *congruencia a derecha* y *congruencia a izquierda* determinadas por un subgrupo de G .

Recordemos que en \mathbb{Z} , la relación de congruencia módulo m es una relación de equivalencia que permite inducir la suma de \mathbb{Z} al cociente $\mathbb{Z}_m = (\mathbb{Z}/\equiv (m))$. Si $H = \langle m \rangle$ es el subgrupo cíclico de \mathbb{Z} generado por m , es decir, el subgrupo formado por los múltiplos de m , entonces

$$\begin{aligned} x \equiv y (m) &\iff x - y \text{ es múltiplo de } m \\ &\iff x - y \in H \\ &\iff -x + y = -(x - y) \in H \end{aligned}$$

Observemos que en este caso $-y$ es el inverso de y para la suma en \mathbb{Z} . Intentaremos generalizar esta relación en \mathbb{Z} a cualquier grupo G y a cualquier subgrupo H de G . Observemos primero que si G es un grupo arbitrario, la condición “ $x - y \in H$ ” se traduce en la condición $xy^{-1} \in H$. En este caso, dado que H es un subgrupo, esta condición es equivalente a que $yx^{-1} = (xy^{-1})^{-1} \in H$. Sin embargo, la condición “ $-x + y \in H$ ”, en un grupo genérico se traduce como $x^{-1}y \in H$, y, como es posible intuir, si G no es

abeliano, en general se tiene que $yx^{-1} \neq x^{-1}y$. Luego existen dos formas de generalizar la congruencia módulo m a un grupo cualquiera:

Definición 5.1.1. Sea G un grupo y H un subgrupo de G . Sean $a, b \in G$, decimos que:

- a es **congruente a derecha** con b **módulo** H , y lo denotamos $a \equiv_r b(H)$, si $ab^{-1} \in H$.
- a es **congruente a izquierda** con b **módulo** H , y lo denotamos $a \equiv_l b(H)$, si $a^{-1}b \in H$.

Lema 5.1.2. Sea G un grupo y H un subgrupo de G . Entonces las congruencias a izquierda y a derecha módulo H son relaciones de equivalencia en G . Más aún, para cada $a \in G$,

- la clase de equivalencia de a por \equiv_r es $[a]_r = Ha = \{ha : h \in H\}$
- la clase de equivalencia de a por \equiv_l es $[a]_l = aH = \{ah : h \in H\}$

Demostración. Probaremos el lema para \equiv_r , la prueba para \equiv_l es análoga y se deja como **ejercicio**.

Veamos primero que \equiv_r es una relación de equivalencia. Como H es un subgrupo de G , $e \in H$ y por lo tanto para cada $a \in G$ se verifica $aa^{-1} = e \in H$, con lo cual $a \equiv_r a(H)$ y \equiv_r es reflexiva.

Si ahora tenemos $a, b \in G$ tales que $a \equiv_r b(H)$, o sea $ab^{-1} \in H$, nuevamente como H es un subgrupo el inverso de este elemento debe estar en H . Por lo tanto $(ab^{-1})^{-1} = ba^{-1} \in H$ con lo cual $b \equiv_r a(H)$ y entonces \equiv_r es simétrica.

Finalmente, si $a \equiv_r b(H)$ y $b \equiv_r c(H)$, entonces $ab^{-1} \in H$, $bc^{-1} \in H$ y como la operación en H es cerrada, resulta $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$. Luego $a \equiv_r c(H)$ y por lo tanto \equiv_r es transitiva.

Veamos ahora que $[a]_r = Ha$ para cada $a \in G$. Sea $b \in [a]_r$ y pongamos $h = ab^{-1}$, entonces $h \in H$ pues $a \equiv_r b(H)$. Pero $b = h^{-1}a \in Ha$, de donde $[a]_r \subset Ha$.

Sea ahora $b \in Ha$. Existirá $h \in H$, tal que $b = ha$. Entonces $ab^{-1} = a(ha)^{-1} = h^{-1} \in H$, con lo cual $a \equiv_r (ha)(H)$. Esto es, $Ha \subset [a]_r$. □

Definición 5.1.3. Sea G un grupo y H un subgrupo de G . Para cada $a \in G$, la clase de equivalencia $[a]_r = Ha$ se denomina **coclase a derecha** de a módulo H y la clase de equivalencia $[a]_l = aH$ se denomina **coclase a izquierda** de a módulo H .

Ejemplo 5.1.4. En \mathbb{Z} un subgrupo H es siempre de la forma $H = \langle m \rangle$ (Teorema 4.6.10). La congruencia a derecha y a izquierda módulo H coinciden entre sí. En efecto

$$\begin{aligned} a \equiv_r b(H) &\iff a + (-b) \in H \iff a - b \text{ es múltiplo de } m \\ &\iff b - a \text{ es múltiplo de } m \iff (-a) + b \in H \\ &\iff a \equiv_l b(H). \end{aligned}$$

Más aún, tenemos que $a \equiv_r b(H)$ (o $a \equiv_l b(H)$) si y sólo si $a \equiv b(m)$. En particular, las coclases a derecha e izquierda módulo $H = \langle m \rangle$ de un elemento $k \in \mathbb{Z}$ coinciden entre sí y con la clase de congruencia módulo m de k . Esto es, $[k]_r = [k]_l = \bar{k} = \{k + jm : j \in \mathbb{Z}\}$. ■

Ejemplo 5.1.5. Sea G un grupo abeliano y H un subgrupo cualquiera de G . Entonces

$$\begin{aligned} a \equiv_r b(H) &\iff ab^{-1} \in H \iff (ab^{-1})^{-1} \in H \iff ba^{-1} \in H \\ &\iff a^{-1}b \in H \iff a \equiv_l b(H). \end{aligned}$$

Es decir la congruencia a derecha e izquierda módulo H coinciden. ■

Los ejemplos anteriores pueden inducirnos a pensar que para cualquier subgrupo H de un grupo G las congruencias a derecha e izquierda módulo H coinciden. Sin embargo esto no necesariamente es cierto si G no es abeliano:

Ejemplo 5.1.6. Consideremos el grupo $G = GL(2, \mathbb{R})$ de matrices invertibles 2×2 y el subgrupo

$$SO(2) = \{A \in GL(2, \mathbb{R}) : A^T A = \text{Id}, \det(A) = 1\}$$

de matrices ortogonales de determinante positivo.

Consideremos las matrices $A = \begin{pmatrix} \sqrt{2} & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ en $GL(2, \mathbb{R})$. Tenemos entonces

$$AB^{-1} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \in SO(2), \quad A^{-1}B = \begin{pmatrix} \sqrt{2} & 1/\sqrt{2} \\ -\sqrt{2} & 0 \end{pmatrix} \notin SO(2)$$

con lo cual $A \equiv_r B(SO(2))$ pero A no es congruente a izquierda con B módulo $SO(2)$. ■

Observación 5.1.7. Dado un grupo no abeliano G y un subgrupo H de G en general se tiene que para cada $a \in G$, $[a]_r \neq [a]_l$. Sin embargo,

$$[e]_r = He = H, \quad [e]_l = eH = H$$

es decir, $[e]_r = [e]_l = H$.

En virtud del Lema 5.1.2 todo grupo G es la unión disjunta de las coclases (a derecha o izquierda) dadas por la congruencia módulo H , siendo H un subgrupo cualquiera de G . Como vimos en el Ejemplo 5.1.6, las clases a derecha y a izquierda que determina H pueden ser distintas, pero éstas tienen la misma cantidad de elementos, y además los respectivos conjuntos cociente también tienen la misma cantidad de elementos. Más precisamente:

Teorema 5.1.8. Sea H un subgrupo de un grupo G . Entonces:

1. El cardinal de cada coclase (a derecha o izquierda) módulo H coincide con el cardinal de H .
2. Un subgrupo H de G determina la misma cantidad de coclases a derecha que a izquierda en G (es decir, el cardinal de los conjuntos cociente G/\equiv_r y G/\equiv_l es el mismo).

Demostración. Sea $a \in G$. Veamos que el cardinal de $[a]_r$ coincide con el cardinal de H . Dejamos como **ejercicio** la prueba para $[a]_l$. Debemos probar que existe una función biyectiva de $[a]_r$ en H . Consideremos la función

$$\varphi : [a]_r \rightarrow H, \text{ tal que } \varphi(b) = ba^{-1}.$$

Observemos primero que φ está bien definida. En efecto, cada $b \in [a]_r$ es de la forma $b = ha$ para algún $h \in H$. Luego $\varphi(b) = ba^{-1} = (ha)a^{-1} \in H$.

Además φ es sobre, pues para cada $h \in H$, $ha \in [a]_r$ es tal que $\varphi(ha) = h$.

Finalmente, φ es inyectiva: si $\varphi(b) = \varphi(c)$, entonces $ba^{-1} = ca^{-1}$ y entonces $b = c$. Luego φ es una biyección y por lo tanto el cardinal de $[a]_r$ coincide con el cardinal de H .

Para probar el punto 2 pongamos $G/\equiv_r = (G/\equiv_r(H))$ y $G/\equiv_l = (G/\equiv_l(H))$ y consideremos la función

$$\Psi : G/\equiv_r \rightarrow G/\equiv_l \quad \text{dada por } \Psi([a]_r) = [a^{-1}]_l.$$

Veamos primero que Ψ está bien definida. Sean $a, b \in G$ tales que $[a]_r = [b]_r$. Es decir, $a \equiv_r b(H)$, o sea, $ab^{-1} \in H$. Como H es un subgrupo de G , $(ab^{-1})^{-1} \in H$ con lo cual $ba^{-1} \in H$. Pero

$$ba^{-1} = (b^{-1})^{-1}(a^{-1}) \implies b^{-1} \equiv_l a^{-1}(H)$$

Es decir, si $[a]_r = [b]_r$ entonces $[a^{-1}]_l = [b^{-1}]_l$ y Ψ está bien definida.

Veamos que Ψ es biyectiva. Sea $[a]_l \in G/\equiv_l$. Entonces $[a^{-1}]_r \in G/\equiv_r$ es tal que $\Psi([a^{-1}]_r) = [a]_l$. Luego Ψ es sobreyectiva.

Si ahora $\Psi([a]_r) = \Psi([b]_r)$, entonces $[a^{-1}]_l = [b^{-1}]_l$, es decir, $a^{-1} \equiv_l b^{-1}(H)$. Con el mismo razonamiento que antes resulta $a \equiv_r b(H)$, es decir $[a]_r = [b]_r$ y Ψ es inyectiva.

Como Ψ es biyectiva, G/\equiv_r y G/\equiv_l tienen el mismo cardinal. □

Definición 5.1.9. Sea G un grupo y H un subgrupo de G . El número de coclases distintas (a derecha o izquierda) módulo H se denomina **índice de H en G** y se denota $[G : H]$.

El siguiente resultado establece una relación entre el orden de un grupo G y de un subgrupo H con el índice $[G : H]$. En particular, nos permitirá hacer una previsión sencilla sobre los posibles órdenes de los elementos de G :

Teorema 5.1.10 (Teorema de Lagrange). Sea H un subgrupo de un grupo G . Entonces

$$o(G) = [G : H]o(H).$$

Demostración. Elijamos un representante a_i de cada clase de congruencia a derecha módulo H , donde $i \in I$, siendo I un conjunto de índices cuyo cardinal es $[G : H]$. Luego

$$G = \bigcup_{i \in I} Ha_i.$$

Como a_i y a_j son representantes de clases distintas si $i \neq j$, se tiene que en este caso $Ha_i \cap Ha_j = \emptyset$. Luego

$$o(G) = \sum_{i \in I} \#(Ha_i)$$

Además, por el Teorema 5.1.8, el cardinal de cada Ha_i coincide con el cardinal de H , es decir, $\#(Ha_i) = \#H = o(H)$ para cada $i \in I$. Luego

$$o(G) = \sum_{i \in I} \#(Ha_i) = \sum_{i \in I} o(H) = \#I \cdot o(H) = [G : H]o(H)$$

como queríamos probar. \square

Como consecuencia inmediata del Teorema de Lagrange obtenemos el siguiente resultado:

Corolario 5.1.11. *Sea G un grupo finito. Entonces para cada subgrupo H de G , $o(H) \mid o(G)$. En particular, para cada $a \in G$, $o(a) \mid o(G)$.*

Ejemplo 5.1.12. Si p es primo, $(\mathbb{Z}_p, +)$ no tiene subgrupos propios. En efecto, si H es un subgrupo de \mathbb{Z}_p , entonces $o(H) \mid o(\mathbb{Z}_p) = p$. Luego $o(H) = 1$, en cuyo caso $H = \{\bar{0}\}$ o bien $o(H) = p$, en cuyo caso $H = \mathbb{Z}_p$. Con el mismo argumento puede probarse que todo grupo de orden primo no tiene subgrupos propios. \blacksquare

Ejemplo 5.1.13. Consideremos el grupo $G = (\mathbb{Z}_4, +)$. G tiene orden 4 y por lo tanto cualquier elemento de G tiene orden 1, 2 o 4. El único elemento de orden 1 es la identidad, en este caso $\bar{0}$. Observemos que por el Lema 4.6.9, $\bar{1}$ y $\bar{3}$ son generadores de \mathbb{Z}_4 , y por lo tanto tienen orden 4. Luego como $\bar{2}$ no es un generador, debe ser $o(\bar{2}) = 2$ y por lo tanto $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$. \blacksquare

5.2. Subgrupos normales y grupo cociente

Volveremos ahora a estudiar los posibles grupos cociente que pueden obtenerse a partir de un grupo G . Comencemos analizando cuándo es posible inducir la operación de G al cociente de G por las congruencias a derecha o izquierda módulo un subgrupo H de G .

Teorema 5.2.1. *Sea G un grupo y H un subgrupo de G . Denotemos por \equiv_r y \equiv_l la congruencia a derecha e izquierda módulo H respectivamente. Entonces:*

1. *La operación de G se induce al cociente G/\equiv_r si y sólo si \equiv_r y \equiv_l coinciden.*
2. *La operación de G se induce al cociente G/\equiv_l si y sólo si \equiv_r y \equiv_l coinciden.*

Demostración. Probaremos sólo el ítem (1), la prueba del ítem (2) es análoga y se deja como **ejercicio**. Supongamos que la operación de G se induce al cociente G/\equiv_r , esto es,

$$(5.1) \quad \left. \begin{array}{l} x \equiv_r x' \\ y \equiv_r y' \end{array} \right\} \implies xy \equiv_r x'y'.$$

Supongamos que $a \equiv_r b$ y veamos que $a \equiv_l b$. Recordemos que $[e]_r = [e]_l = H$ (ver Observación 5.1.7). Observemos que como \equiv_r es reflexiva, entonces $a^{-1} \equiv_r a^{-1}$. Luego por la condición (5.1), tenemos:

$$\left. \begin{array}{l} a^{-1} \equiv_r a^{-1} \\ a \equiv_r b \end{array} \right\} \implies a^{-1}a \equiv_r a^{-1}b \implies e \equiv_r a^{-1}b.$$

Luego $a^{-1}b \in [e]_r$, y por lo tanto $a^{-1}b \in H$, es decir, $a \equiv_l b$.

Veamos ahora que si $a \equiv_l b$ entonces $a \equiv_r b$. Si $a \equiv_l b$, entonces $a^{-1}b \in H = [e]_r$, y por lo tanto $a^{-1}b \equiv_r e$. Como $a \equiv_r a$, de la condición (5.1), tenemos:

$$\left. \begin{array}{l} a \equiv_r a \\ a^{-1}b \equiv_r e \end{array} \right\} \implies a(a^{-1}b) \equiv_r ae \implies b \equiv_r a.$$

Concluimos que $a \equiv_r b$ si y sólo si $a \equiv_l b$, y por lo tanto \equiv_r y \equiv_l coinciden, como queríamos probar.

Supongamos ahora que las congruencias a derecha e izquierda módulo H coinciden y veamos que la operación de G se induce al cociente G/\equiv_r . Sean $x, x', y, y' \in G$ tales que $x \equiv_r x'$, $y \equiv_r y'$. Debemos ver que $xy \equiv_r x'y'$. Pongamos $h_1 = x(x')^{-1} \in H$ y $h_2 = y(y')^{-1} \in H$. Como $(x')^{-1} = x^{-1}h_1$, resulta

$$(xy)(x'y')^{-1} = xy(y')^{-1}(x')^{-1} = xh_2(x')^{-1} = xh_2x^{-1}h_1.$$

Ahora bien, $h_2x^{-1} \in [x^{-1}]_r$, y por hipótesis $[x^{-1}]_r = [x^{-1}]_l = x^{-1}H$, dado que las congruencias a derecha e izquierda módulo H coinciden. Luego existirá $h' \in H$ tal que $h_2x^{-1} = x^{-1}h'$ con lo cual

$$(xy)(x'y')^{-1} = xh_2x^{-1}h_1 = xx^{-1}h'h_1 = h'h_1 \in H$$

como queríamos probar. □

Definición 5.2.2. Sea G un grupo. Un subgrupo N de G se dice un **subgrupo normal** si las congruencias a derecha e izquierda módulo N coinciden. En ese caso hablamos directamente de **congruencia módulo N** y denotamos $a \equiv b(N)$ para indicar las condiciones equivalentes $a \equiv_r b(N)$ o $a \equiv_l b(N)$. Si N es un subgrupo normal de G , lo denotamos $N \triangleleft G$.

Hemos probado en el Ejemplo 5.1.5 que si G es abeliano entonces para cualquier subgrupo H de G las congruencias a derecha e izquierda módulo H coinciden. Es decir:

Lema 5.2.3. Sea G un grupo abeliano. Entonces todo subgrupo de G es un subgrupo normal de G .

Como una relación de equivalencia está completamente determinada por sus clases de equivalencia, es decir, dos relaciones de equivalencia son iguales si y sólo si las clases de cualquier elemento respecto de cada una de ellas coinciden, tenemos por el Lema 5.1.2:

Lema 5.2.4. Sea G un grupo y N un subgrupo de G . Entonces $N \triangleleft G$ si y sólo si $aN = Na$ para cada $a \in G$.

Del Teorema 4.3.12 sabemos que si la operación de un grupo G se induce al cociente G/\sim de G por una relación de equivalencia \sim , entonces G/\sim con la operación inducida es un grupo. Por lo tanto obtenemos como consecuencia inmediata del Teorema 5.2.1 que:

Corolario 5.2.5. Sea G un grupo y $N \triangleleft G$. Sea $\equiv(N)$ la congruencia módulo N . Entonces la operación de G se induce al cociente $G/\equiv(N)$ y $G/\equiv(N)$ es un grupo.

Definición 5.2.6. Sea G un grupo y N un subgrupo normal de G . El grupo $G/\equiv (N)$ se denomina **cociente** de G por N y se denota como G/N . Denotamos por $[a]$ a las coclases $[a]_r = [a]_l$ de la congruencia módulo N .

Ejemplo 5.2.7. Del Ejemplo 5.1.6 podemos afirmar que $SO(2)$ no es un subgrupo normal de $GL(2, \mathbb{R})$. Es fácil verificar que $SO(2)$ es un grupo abeliano. Esto muestra que un subgrupo abeliano de un grupo G **no necesariamente** es normal en G . ■

Ejemplo 5.2.8. Consideremos el subgrupo cíclico N generado por $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ en S_3 (el grupo de biyecciones de $\{1, 2, 3\}$ en sí mismo). Tenemos

$$a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$a^3 = a^2 \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{Id}$$

y a partir de ahí las potencias se empiezan a repetir: por ejemplo, $a^4 = a^3 \circ a = a$, $a^5 = a^3 \circ a^2 = a^2$, $a^6 = a^3 \circ a^3 = a^3 = \text{Id}$, etc. Luego $N = \{\text{Id}, a, a^2\}$. Veamos que N es un subgrupo normal de S_3 . Sea $x \in S_3$. Hemos visto en la Observación 5.1.7 que $N = [e]_r = [e]_l$. Luego si $x \in N$, $[x]_r = [e]_r = [e]_l = [x]_l$.

Tomemos ahora $x \in S_3$ tal que $x \notin N$. Estos elementos son:

$$x_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Probaremos que $[x_i]_r = Nx_i = x_iN = [x_i]_l$ para cada $i = 1, 2, 3$.

Comencemos con x_1 . Observemos que $[x_1]_r = Nx_1 = \{x_1, a \circ x_1, a^2 \circ x_1\}$. Tenemos

$$a \circ x_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = x_2$$

$$a^2 \circ x_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = x_3.$$

Concluimos que $[x_1]_r = \{x_1, x_2, x_3\}$, y por lo tanto $[x_1]_r = [x_2]_r = [x_3]_r$. Es decir, el cociente S_3/\equiv_r tiene dos elementos (hay sólo dos clases de equivalencia), $[e]_r = N$ y $[x_1]_r$. Por el Teorema 5.1.8, S_3/\equiv_l también consta de dos elementos, y como $x_1 \notin [e]_l = N$, la otra clase debe ser $[x_1]_l = \{x_1, x_2, x_3\}$. Luego $[x_i]_r = [x_i]_l = \{x_1, x_2, x_3\}$ para cada $i = 1, 2, 3$ y $N \triangleleft S_3$. ■

Veremos a continuación algunas caracterizaciones de un subgrupo normal que nos permitirán demostrar de manera más sencilla cuándo un subgrupo N de un grupo G es normal.

Teorema 5.2.9. *Sea G un grupo y N un subgrupo de G . Entonces son equivalentes:*

1. N es un subgrupo normal de G .
2. para cada $a \in G$, $aN = Na$.
3. para cada $a \in G$, $aNa^{-1} \subset N$, donde $aNa^{-1} = \{ana^{-1} : n \in N\}$.
4. para cada $a \in G$, $aNa^{-1} = N$.

Demostración. La equivalencia entre el punto 1 y el punto 2 ya fue probada en el Lema 5.2.4.

Veamos ahora que el punto 2 implica el punto 3. Sea $n \in N$, como $aN = Na$, existe $n' \in N$ tal que $an = n'a$, de donde $ana^{-1} = n' \in N$. O sea, para $n \in N$ arbitrario, $ana^{-1} \in N$, de donde $aNa^{-1} \subset N$.

Supongamos ahora que vale el punto 3 y veamos que vale el punto 4. Sólo resta probar que $N \subset aNa^{-1}$ para cada $a \in G$. Fijemos por lo tanto $a \in G$ y sea $n \in N$ cualquiera. Pongamos $n' = a^{-1}na$. Observemos que $n' = bnb^{-1}$, para $b = a^{-1} \in G$. Como por hipótesis $bNb^{-1} \subset N$ para cualquier $b \in G$, concluimos que $n' \in N$. Luego $n = an'a^{-1} \in aNa^{-1}$ como queríamos ver.

Veamos finalmente que el punto 4 implica el punto 2. Supongamos que $aNa^{-1} = N$ para cada $a \in G$ y veamos que $aN = Na$ para cada $a \in G$. Sea $x = an \in aN$, con $n \in N$. Entonces por hipótesis, existe $n' \in N$ tal que $ana^{-1} = n' \in N$, de donde $an = n'a \in Na$. Luego $x \in Na$ y por lo tanto $aN \subset Na$.

Con un razonamiento análogo (aplicando la hipótesis a a^{-1} en vez de a), se obtiene $Na \subset aN$, lo que completa la prueba. \square

Ejemplo 5.2.10. A partir del Teorema 5.2.9 podemos verificar inmediatamente que todo subgrupo de un grupo abeliano es un subgrupo normal (Lema 5.2.3).

Supongamos que G es un grupo abeliano y N es un subgrupo cualquiera de G . Sea $a \in G$. Entonces para cada $n \in N$, $an = na$, con lo cual $ana^{-1} = n \in N$. Esto es, $aNa^{-1} \subset N$ y por lo tanto $N \triangleleft G$. \blacksquare

Ejemplo 5.2.11. El grupo lineal, el grupo de traslaciones y el grupo afín. Consideremos el grupo $(\mathcal{B}(\mathbb{R}^n), \circ)$ de biyecciones de \mathbb{R}^n . Sea $\mathcal{L}(\mathbb{R}^n)$ el conjunto de isomorfismos lineales $L : \mathbb{R}^n \rightarrow \mathbb{R}^n$. Como es bien sabido, la composición de isomorfismos lineales es un isomorfismo lineal. Por lo tanto $\mathcal{L}(\mathbb{R}^n)$ es un subconjunto cerrado de $\mathcal{B}(\mathbb{R}^n)$ para la composición de funciones.

Además, la identidad es un isomorfismo lineal y si $L : \mathbb{R}^n \rightarrow \mathbb{R}^n$ es un isomorfismo lineal, entonces $L^{-1} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ también lo es. Por lo tanto $(\mathcal{L}(\mathbb{R}^n), \circ)$ es un subgrupo de $(\mathcal{B}(\mathbb{R}^n), \circ)$, denominado **grupo lineal** de \mathbb{R}^n .

Consideremos ahora el subconjunto $\mathcal{T}(\mathbb{R}^n)$ de traslaciones de \mathbb{R}^n , es decir, transformaciones de la forma $T_v : \mathbb{R}^n \rightarrow \mathbb{R}^n$ tal que $T_v(x) = x + v$ para algún vector fijo $v \in \mathbb{R}^n$. Es inmediato verificar que $T_v \circ T_w = T_{v+w} \in \mathcal{T}(\mathbb{R}^n)$, $\text{Id} = T_0 \in \mathcal{T}(\mathbb{R}^n)$, donde 0 es el vector nulo, y $T_v^{-1} = T_{-v} \in \mathcal{T}(\mathbb{R}^n)$. Luego $\mathcal{T}(\mathbb{R}^n)$ es un subgrupo de $\mathcal{B}(\mathbb{R}^n)$ denominado **grupo de traslaciones** de \mathbb{R}^n .

Consideremos finalmente el subconjunto $\text{Aff}(\mathbb{R}^n)$ de funciones $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ de la forma

$$f = T_v \circ L$$

donde $T_v \in \mathcal{T}(\mathbb{R}^n)$ y $L \in \mathcal{L}(\mathbb{R}^n)$. Una función de este tipo se denomina una **transformación afín** de \mathbb{R}^n . Observemos que $Aff(\mathbb{R}^n) \subseteq \mathcal{B}(\mathbb{R}^n)$. En efecto, sea $f = T_v \circ L \in Aff(\mathbb{R}^n)$. Entonces:

- f es inyectiva: si $x, y \in \mathbb{R}^n$ son tales que $f(x) = f(y)$, entonces

$$L(x) + v = L(y) + v \implies L(x) = L(y) \xrightarrow{L \text{ isomorfismo}} x = y$$

- f es sobreyectiva: sea $y \in \mathbb{R}^n$ y pongamos $x = L^{-1}(y - v)$. Entonces

$$(5.2) \quad f(x) = L(L^{-1}(y - v)) + v = y - v + v = y.$$

Luego f es biyectiva como queríamos probar.

Veamos ahora que $Aff(\mathbb{R}^n)$ es un subconjunto cerrado de $\mathcal{B}(\mathbb{R}^n)$ para la composición de funciones. Supongamos que $f = T_v \circ L$ y $g = T_w \circ S$ son dos transformaciones afines de \mathbb{R}^n . Entonces:

$$\begin{aligned} g \circ f(x) &= (T_w \circ S) \circ (T_v \circ L)(x) = (T_w \circ S)(L(x) + v) \\ &= S(L(x) + v) + w \stackrel{(*)}{=} S(L(x)) + S(v) + w \end{aligned}$$

donde $(*)$ vale pues S es una transformación lineal. Como $S \circ L \in \mathcal{L}(\mathbb{R}^n)$, resulta

$$g \circ f = \underbrace{T_{S(v)+w}}_{\in \mathcal{T}(\mathbb{R}^n)} \circ \underbrace{(S \circ L)}_{\in \mathcal{L}(\mathbb{R}^n)} \in Aff(\mathbb{R}^n)$$

Ahora bien, $\text{Id} = T_0 \circ \text{Id}$ es una transformación afín, y de (5.2) resulta que si $f = T_v \circ L \in Aff(\mathbb{R}^n)$ entonces

$$(5.3) \quad f^{-1} = T_{-L^{-1}(v)} \circ L^{-1} \in Aff(\mathbb{R}^n).$$

Luego $Aff(\mathbb{R}^n)$ es un subgrupo de $\mathcal{B}(\mathbb{R}^n)$ denominado **grupo afín** de \mathbb{R}^n .

Observemos que $\mathcal{L}(\mathbb{R}^n) \subseteq Aff(\mathbb{R}^n)$, dado que si $L \in \mathcal{L}(\mathbb{R}^n)$, L puede expresarse como $L = T_0 \circ L$. De manera similar, si $T_v \in \mathcal{T}(\mathbb{R}^n)$, entonces $T_v = T_v \circ \text{Id}$, con lo cual $\mathcal{T}(\mathbb{R}^n) \subseteq Aff(\mathbb{R}^n)$. Luego $\mathcal{L}(\mathbb{R}^n)$ y $\mathcal{T}(\mathbb{R}^n)$ son subgrupos de $Aff(\mathbb{R}^n)$.

Veamos que $\mathcal{T}(\mathbb{R}^n)$ es un subgrupo normal de $Aff(\mathbb{R}^n)$. Sea $f = T_v \circ L \in Aff(\mathbb{R}^n)$ una transformación afín cualquiera y sea $T_w \in \mathcal{T}(\mathbb{R}^n)$ cualquiera. Entonces de (5.3) resulta:

$$\begin{aligned} f \circ T_w \circ f^{-1}(x) &= (T_v \circ L) \circ T_w \circ (T_{-L^{-1}(v)} \circ L^{-1})(x) \\ &= (T_v \circ L) \circ T_w(L^{-1}(x) - L^{-1}(v)) = (T_v \circ L)(L^{-1}(x) - L^{-1}(v) + w) \\ &= T_v(L(L^{-1}(x)) - L(L^{-1}(v)) + L(w)) = (x - v + L(w) + v) = x + L(w). \end{aligned}$$

Luego $f \circ T_w \circ f^{-1} = T_{L(w)} \in \mathcal{T}(\mathbb{R}^n)$.

Concluimos que $f \mathcal{T}(\mathbb{R}^n) f^{-1} \subset \mathcal{T}(\mathbb{R}^n)$ y por lo tanto $\mathcal{T}(\mathbb{R}^n) \triangleleft Aff(\mathbb{R}^n)$. En este caso se trata de un subgrupo normal que además es un subgrupo abeliano de $Aff(\mathbb{R}^n)$. ■

Volvamos al problema general de determinar qué relaciones de equivalencia \sim en un grupo G permiten inducir la operación de G al cociente G/\sim . Hasta aquí hemos visto que en el caso de las congruencias (a derecha o izquierda) módulo un subgrupo H de G , el cociente G/\equiv_r (o G/\equiv_l) es un grupo si y sólo si H es un subgrupo normal de G . Veremos a continuación que estos no son casos particulares, sino que una relación de equivalencia permite definir un grupo cociente si y sólo si se trata de la congruencia módulo un subgrupo normal:

Teorema 5.2.12. *Sea G un grupo y \sim una relación de equivalencia en G . Entonces la operación de G se induce al cociente G/\sim si y sólo si la clase de equivalencia de la identidad, $N = [e]$, es un subgrupo normal de G y \sim es la congruencia módulo N .*

Demostración. Ya hemos visto en el Corolario 5.2.5 que si $N \triangleleft G$ y \sim es la congruencia módulo N , entonces $[e] = N$ y G/\sim es un grupo con la operación inducida de G .

Supongamos ahora que \sim es una relación de equivalencia en un grupo G tal que la operación de G se induce al cociente G/\sim . Sea $N = [e]$ y veamos que $N \triangleleft G$. Observemos que $e \in N$ y que si $k_1, k_2 \in N$, entonces $k_1 \sim e$, $k_2 \sim e$ y por lo tanto

$$k_1 k_2 \sim e \cdot e = e \implies k_1 k_2 \in N.$$

Luego N es cerrado para la operación de G y contiene a la identidad. Finalmente, si $k \in N$, $k \sim e$, y como $k^{-1} \sim k^{-1}$ resulta

$$k \cdot k^{-1} \sim e \cdot k^{-1} \implies e \sim k^{-1} \implies k^{-1} \in N.$$

Concluimos que N es un subgrupo de G .

Sea ahora $a \in G$ cualquiera y $n \in N$. Tenemos $a \sim a$, $n \sim e$, $a^{-1} \sim a^{-1}$, con lo cual

$$ana^{-1} \sim aea^{-1} = e \implies ana^{-1} \in N.$$

Por lo tanto $N \triangleleft G$. Veamos finalmente que \sim coincide con la congruencia módulo N . Para ello supongamos que $x \sim y$. Entonces como $y^{-1} \sim y^{-1}$, resulta $xy^{-1} \sim y \cdot y^{-1} = e$, con lo cual $xy^{-1} \in N$, o sea $x \equiv y(N)$.

Recíprocamente, si $x \equiv y(N)$, entonces $xy^{-1} \in N$. Luego $xy^{-1} \sim e$ y como $y \sim y$, resulta $(xy^{-1})y \sim e \cdot y$, o sea $x \sim y$. \square

5.3. Primer Teorema de Isomorfismo

El título de esta sección hace referencia a un resultado fundamental de la teoría de grupos que nos permite identificar cuándo un grupo dado es en realidad un grupo cociente. Este título también indica que hay *otros* teoremas de isomorfismo (de hecho hay un segundo y un tercer teorema de isomorfismos). Estos resultados se deducen del primero y no son de interés para el tratamiento que haremos aquí. Los interesados pueden consultarlos en [9] o [12].

Comenzaremos estudiando la relación entre homomorfismos y subgrupos normales.

Lema 5.3.1. Sean G y H grupos y $f : G \rightarrow H$ un homomorfismo de grupos. Entonces $\ker(f) \triangleleft G$.

Demostración. Por el Teorema 4.7.22, $\ker(f)$ es un subgrupo de G . En efecto, $\{e_H\}$ es un subgrupo de H y $\ker(f) = \{a \in G : f(a) = e\} = f^{-1}(e_H)$. Veamos que es un subgrupo normal. Sea $a \in G$ y $n \in \ker(f)$ cualquiera. Entonces $f(n) = e$ y por lo tanto

$$f(ana^{-1}) = f(a)f(n)f(a)^{-1} = f(a)f(a)^{-1} = e.$$

Luego $ana^{-1} \in \ker(f)$ de donde $a \ker(f) a^{-1} \subset \ker(f)$ y entonces $\ker(f) \triangleleft G$. □

Lema 5.3.2. Sea G un grupo y $N \triangleleft G$. Entonces la proyección $\pi : G \rightarrow G/N$ dada por

$$\pi(a) = [a] = aN = Na$$

es un homomorfismo de grupos y $\ker(\pi) = N$.

Demostración. Veamos primero que π es un homomorfismo de grupos. En efecto, sean $x, y \in G$. Entonces como la operación en G/N es la operación de G inducida al cociente, resulta $[x] \cdot [y] = [xy]$. Es decir,

$$\pi(xy) = [xy] = [x] \cdot [y] = \pi(x)\pi(y).$$

Del Teorema 4.3.12 resulta que la identidad en G/N es $[e] = N$. Luego $a \in \ker(\pi)$ si y sólo si $\pi(a) = [a] = [e]$, lo que ocurre si y sólo si $a \in [e] = N$, es decir, $\ker(\pi) = N$. □

Definición 5.3.3. Sea G un grupo y $N \triangleleft G$. El homomorfismo $\pi : G \rightarrow G/N$, $\pi(a) = [a]$ se denomina **proyección (canónica)** de G al cociente G/N .

A partir de los Lemas 5.3.1 y 5.3.2 tenemos que:

Teorema 5.3.4. Sea G un grupo y N un subgrupo de G . Entonces $N \triangleleft G$ si y sólo si $N = \ker(f)$ para algún homomorfismo de grupos f tal que $\text{Dom}(f) = G$.

Demostración. Por el Lema 5.3.1, si $f : G \rightarrow H$ es un homomorfismo de grupos, $\ker(f)$ es un subgrupo normal de G . Sea ahora N un subgrupo normal de G cualquiera. Entonces, por el Lema 5.3.2, $N = \ker(\pi)$, donde $\pi : G \rightarrow G/N$ es un homomorfismo de grupos con dominio G . □

Veremos ahora que todos los subgrupos del cociente G/N se obtienen como imagen via la proyección π de algún subgrupo de G .

Lema 5.3.5. Sea G un grupo, $N \triangleleft G$ y $\pi : G \rightarrow G/N$ la proyección al cociente. Entonces:

1. $\pi(H)$ es un subgrupo de G/N para cada $H < G$.
2. Si $\tilde{H} < G/N$, existe $H < G$ tal que $\tilde{H} = \pi(H)$ y $N \triangleleft H$.

Demostración. El punto 1 es inmediato del Teorema 4.7.22.

Veamos el punto 2. Sea \tilde{H} un subgrupo de G/N y sea $H = \pi^{-1}(\tilde{H})$. Entonces por el Teorema 4.7.22 H es un subgrupo de G y como π es sobre, $\pi(H) = \pi(\pi^{-1}(\tilde{H})) = \tilde{H}$. Además $[e] \in \tilde{H}$, luego $N = \pi^{-1}([e]) \subset \pi^{-1}(\tilde{H})$, con lo cual $N \subset H$. En particular, del Lema 4.5.11 resulta N un subgrupo de H . Como $aNa^{-1} \subseteq N$ para cada $a \in G$, resulta en particular que $hNh^{-1} \subseteq N$ para cada $h \in H \subseteq G$. Luego $N \triangleleft H$. \square

Como consecuencia del Lema 5.3.5 podemos describir todos los subgrupos de $(\mathbb{Z}_m, +)$:

Teorema 5.3.6 (Subgrupos de $(\mathbb{Z}_m, +)$). *Todos los subgrupos de $(\mathbb{Z}_m, +)$ son cíclicos. Es decir, $\tilde{H} < \mathbb{Z}_m$ si y sólo si $\tilde{H} = \langle \bar{k} \rangle$ para algún $k = 0, \dots, m-1$.*

Demostración. Por el Lema 5.3.5, todo subgrupo de \mathbb{Z}_m es de la forma $\pi(H)$ para algún subgrupo H de \mathbb{Z} . Por el Teorema 4.6.10, los subgrupos de H son subgrupos cíclicos de la forma $H = \langle k \rangle$ para algún $k \in \mathbb{Z}$. Luego del Ejercicio 28 del Capítulo 4 resulta $\tilde{H} = \langle \pi(k) \rangle = \langle \bar{k} \rangle$. \square

Así como la operación de un grupo G puede inducirse al cociente G/N de G por un subgrupo normal N , estudiaremos a continuación bajo qué condiciones podemos inducir al cociente G/N un homomorfismo f con dominio G :

Lema 5.3.7 (Lema de factorización). *Sea $f : G \rightarrow H$ un homomorfismo de grupos y $N \triangleleft G$ tal que $N \subset \ker(f)$. Entonces existe un único homomorfismo $\bar{f} : G/N \rightarrow H$ tal que $\bar{f} \circ \pi = f$, donde $\pi : G \rightarrow G/N$ es la proyección al cociente.*

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow f & \downarrow \bar{f} \\ & & H \end{array}$$

Demostración. Para probar la existencia de \bar{f} , observemos que para que se cumpla la condición $\bar{f} \circ \pi = f$, debemos tener $\bar{f}([a]) = f(a)$ para cada $a \in G$. Por lo tanto comenzaremos probando que $\bar{f} : G/N \rightarrow H$ dado por $\bar{f}([a]) = f(a)$ está bien definido.

En efecto, sean $a, a' \in G$ tales que $a \equiv a' (N)$, es decir, $[a] = [a']$. Entonces $a(a')^{-1} \in N$ y como $N \subset \ker(f)$, resulta

$$f(a)f(a')^{-1} = f(a(a')^{-1}) = e \implies f(a) = f(a')$$

como queríamos probar. Veamos ahora que \bar{f} es un homomorfismo de grupos. Para ello sean $[a], [b] \in G/N$. Entonces

$$\bar{f}([a][b]) = \bar{f}([ab]) = f(ab) = f(a)f(b) = \bar{f}([a])\bar{f}([b])$$

Concluimos que existe un homomorfismo de grupos $\bar{f} : G/N \rightarrow H$ tal que para cada $a \in G$, $f(a) = \bar{f}([a]) = \bar{f}(\pi(a))$, es decir, $\bar{f} \circ \pi = f$.

Si $\varphi : G/N \rightarrow H$ es un homomorfismo tal que $\varphi \circ \pi = f$, entonces para cada $[a] \in G/N$, $\varphi([a]) = \varphi(\pi(a)) = f(a) = \bar{f}([a])$. Luego $\varphi = \bar{f}$ y por lo tanto \bar{f} es único. \square

Definición 5.3.8. Sea $f : G \rightarrow H$ un homomorfismo de grupos y $N \triangleleft G$ tal que $N \subset \ker(f)$. El homomorfismo $\bar{f} : G/N \rightarrow H$ dado en el Lema 5.3.7 se denomina **homomorfismo inducido** por f al cociente G/N .

Teorema 5.3.9 (Primer Teorema de Isomorfismo). Si $f : G \rightarrow H$ es un epimorfismo, entonces el homomorfismo inducido por f a $G/\ker(f)$ es un isomorfismo. En particular, $G/\ker(f) \simeq H$.

Demostración. Supongamos que $f : G \rightarrow H$ es un epimorfismo y consideremos el homomorfismo \bar{f} inducido por f a $G/\ker(f)$, esto es,

$$\bar{f} : G/\ker(f) \rightarrow H, \quad \bar{f}([a]) = f(a).$$

Como f es un epimorfismo, dado $h \in H$ existe $a \in G$ es tal que $f(a) = h$. Luego $\bar{f}([a]) = f(a) = h$ y por lo tanto \bar{f} es un epimorfismo. Veamos entonces que \bar{f} es un monomorfismo. Sea $[a] \in \ker(\bar{f})$. Entonces

$$\bar{f}([a]) = f(a) = e_H \implies a \in \ker(f) = [e] \implies [a] = [e].$$

Luego $\ker(\bar{f}) = \{[e]\}$ como queríamos ver. \square

Corolario 5.3.10. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Entonces $G/\ker(f) \simeq \text{Im}(f)$.

Ejemplo 5.3.11. Sea G un grupo y $N \triangleleft G$. Consideremos la proyección al cociente $\pi : G \rightarrow G/N$. Entonces π es un epimorfismo tal que $\ker(\pi) = N$. Es fácil verificar que el isomorfismo inducido $\bar{\pi} : G/N \rightarrow G/N$ es la identidad. \blacksquare

Ejemplo 5.3.12. Sea $H = \langle i \rangle$ el subgrupo cíclico de (\mathbb{C}^*, \cdot) generado por la unidad imaginaria i . Consideremos la función $f : \mathbb{Z} \rightarrow H$ dada por $f(k) = i^k$. Entonces es claro que f es sobreyectiva. Más aún, f es un homomorfismo de grupos. En efecto,

$$f(k_1 + k_2) = i^{k_1 + k_2} = i^{k_1} i^{k_2} = f(k_1) f(k_2).$$

Luego f es un epimorfismo y $\ker(f) = \{k \in \mathbb{Z} : i^k = 1\} = \{4k : k \in \mathbb{Z}\} = \langle 4 \rangle$. Luego $\langle i \rangle \simeq \mathbb{Z}/\langle 4 \rangle = \mathbb{Z}_4$. \blacksquare

Ejemplo 5.3.13. Consideremos la aplicación $\varphi : \mathbb{R} \rightarrow \mathbb{C}^*$ dada por $\varphi(\theta) = 1_{2\pi\theta} = \cos(2\pi\theta) + i \sin(2\pi\theta)$. Observemos que φ es un homomorfismo de $(\mathbb{R}, +)$ en (\mathbb{C}^*, \cdot) . En efecto, sean $\theta, \rho \in \mathbb{R}$. Entonces

$$\varphi(\theta + \rho) = 1_{2\pi(\theta + \rho)} = 1_{2\pi\theta + 2\pi\rho} = 1_{2\pi\theta} \cdot 1_{2\pi\rho} = \varphi(\theta) \cdot \varphi(\rho).$$

Ahora bien, $\theta \in \ker(\varphi)$ si y sólo si $\cos(2\pi\theta) + i \sin(2\pi\theta) = 1$, lo que ocurre si y sólo si $\theta = k$ para $k \in \mathbb{Z}$. Luego $\ker(\varphi) = \mathbb{Z}$ y por lo tanto $\text{Im}(\varphi) \simeq \mathbb{R}/\mathbb{Z}$. Observemos finalmente que

$$\text{Im}(\varphi) = \{z \in \mathbb{C} : \|z\| = 1\} = S^1.$$

Luego el círculo S^1 con el producto inducido de \mathbb{C}^* es un grupo isomorfo a \mathbb{R}/\mathbb{Z} . \blacksquare

Ejemplo 5.3.14. Consideremos la aplicación $\varphi : Aff(n, \mathbb{R}) \rightarrow \mathcal{L}(\mathbb{R}^n)$ del grupo afin en el grupo lineal de \mathbb{R}^n dada por $\varphi(f) = L_f$, donde $f = T_v \circ L_f$ (ver Ejemplo 5.2.11). Observemos que φ es un homomorfismo. En efecto, si $f = T_v \circ L_f$ y $g = T_w \circ L_g$, entonces

$$f \circ g = T_{L_f(w)+v} \circ (L_f \circ L_g)$$

y por lo tanto $\varphi(f \circ g) = L_f \circ L_g = \varphi(f) \circ \varphi(g)$. Claramente φ es un epimorfismo, pues dada $L \in \mathcal{L}(\mathbb{R}^n)$, poniendo $f = T_0 \circ L \in Aff(n, \mathbb{R})$ resulta $\varphi(f) = L$. Finalmente, si $f = T_v \circ L_f$ tenemos que

$$f \in \ker(\varphi) \iff \varphi(f) = L_f = \text{Id} \iff f = T_v$$

o sea, $\ker(\varphi) = \mathcal{T}(\mathbb{R}^n)$. Luego $\mathcal{L}(\mathbb{R}^n) \simeq Aff(n, \mathbb{R})/\mathcal{T}(\mathbb{R}^n)$. ■

5.4. Propiedades y clasificación de los grupos cíclicos

En esta sección afrontaremos nuevamente un problema de clasificación (ya lo hemos hecho con las álgebras de Boole finitas). En el estudio de cualquier estructura algebraica la noción de isomorfismo nos permite clasificar estas estructuras, es decir, dividir las en clases de equivalencia cuyos elementos comparten propiedades comunes. Sin embargo en general es un problema muy difícil (si no imposible) describir un representante particular de cada una de estas clases. En el caso de los grupos cíclicos el problema es relativamente sencillo. Como veremos a continuación, un grupo cíclico es isomorfo a \mathbb{Z} o a algún \mathbb{Z}_m .

Teorema 5.4.1. *Sea $f : G \rightarrow G'$ un homomorfismo de grupos con G cíclico. Entonces:*

1. *$f(G)$ es un subgrupo cíclico de G' . Más aún, si $a \in G$ es un generador de G , entonces $f(a)$ es un generador de $f(G)$.*
2. *Si f es un monomorfismo, entonces b' es un generador de $f(G)$ si y sólo si $b' = f(b)$ para algún generador b de G .*

Demostración. Supongamos que G es cíclico y a es un generador de G . Por el Teorema 4.7.22, $f(G) = \text{Im}(f)$ es un subgrupo de G' . Veamos que $f(G) = \langle f(a) \rangle$.

Un elemento genérico de $\langle f(a) \rangle$ es de la forma $f(a)^k$ para algún $k \in \mathbb{Z}$. Como f es un homomorfismo, $f(a)^k = f(a^k) \in f(G)$ (ver Ejercicio 27 del Capítulo 4). Luego $\langle f(a) \rangle \subset f(G)$.

Recíprocamente, si $g' \in f(G)$ existe $g \in G$ tal que $f(g) = g'$. Pero como $G = \langle a \rangle$, existirá $k \in \mathbb{Z}$ tal que $g = a^k$. Luego $g' = f(a^k) = f(a)^k \in \langle f(a) \rangle$.

Si ahora f es un monomorfismo, entonces $f : G \rightarrow f(G)$ es un isomorfismo. El resultado es entonces consecuencia del Ejercicio 28 del Capítulo 4. □

Lema 5.4.2. *Sea G un grupo cíclico y $a \in G$ un generador de G . Entonces $f : \mathbb{Z} \rightarrow G$, $f(k) = a^k$ es un epimorfismo.*

Demostración. Observemos que $f(k_1 + k_2) = a^{k_1+k_2} = a^{k_1}a^{k_2}$ con lo cual f es un homomorfismo de grupos. Si ahora $g \in G$, existirá $k \in \mathbb{Z}$ tal que $g = a^k$, con lo cual $f(k) = g$. Luego f es un epimorfismo. □

Teorema 5.4.3 (Clasificación de grupos cíclicos). *Sea G un grupo cíclico. Entonces G es isomorfo a alguno de los siguientes grupos:*

1. $(\mathbb{Z}, +)$ si $o(G)$ es infinito.
2. $(\mathbb{Z}_m, +)$, para algún $m \in \mathbb{N}$, si $o(G) = m$.

Demostración. Sea G un grupo cíclico y sea a un generador de G . Consideremos el epimorfismo $f : \mathbb{Z} \rightarrow G$, $f(a) = a^k$, dado en el Lema 5.4.2.

Si $\ker(f) = \{0\}$, entonces f es un monomorfismo y por lo tanto un isomorfismo. Es decir, $G \simeq \mathbb{Z}$.

Supongamos entonces que $\ker(f)$ no es trivial. Como $\ker(f)$ es un subgrupo de \mathbb{Z} , por el Teorema 4.6.10, $\ker f = \langle m \rangle$ para algún $m \in \mathbb{Z}$. Luego por el Teorema 5.3.9, $G \simeq \mathbb{Z}/\langle m \rangle = \mathbb{Z}_m$. \square

Observación 5.4.4. *Sea $G = \langle a \rangle$ y $f : \mathbb{Z} \rightarrow G$, $f(k) = a^k$. Si $\ker(f) = \{0\}$, entonces f es un isomorfismo. Supongamos que $\ker(f) = \langle m \rangle$. Entonces el Teorema 5.3.9 nos proporciona el isomorfismo entre G y \mathbb{Z}_m : se trata del isomorfismo inducido por f ,*

$$\bar{f} : \mathbb{Z}_m \rightarrow G, \quad \bar{f}(\bar{k}) = a^k.$$

Observemos además que a es un generador arbitrario de G . En particular, para cada generador $a \in G$, si $G \simeq \mathbb{Z}$, existe un isomorfismo $f : \mathbb{Z} \rightarrow G$ tal que $f(1) = a$. Y si $G \simeq \mathbb{Z}_m$, existe un isomorfismo $\bar{f} : \mathbb{Z}_m \rightarrow G$ tal que $\bar{f}(\bar{1}) = \bar{a}$.

Corolario 5.4.5. *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Supongamos que G es cíclico, a es un generador de G y consideremos el epimorfismo $f : \mathbb{Z} \rightarrow G$ dado por $f(k) = a^k$. Si $S < G$ es un subgrupo de G , entonces por el Teorema 4.7.22, $S' = f^{-1}(S)$ es un subgrupo de \mathbb{Z} . Como $S = f(S')$ y S' es cíclico por el Teorema 4.6.10, S debe ser un subgrupo cíclico de G por el Teorema 5.4.1. \square

Corolario 5.4.6. *Si G es un grupo de orden p , con p primo, entonces $G \simeq \mathbb{Z}_p$.*

Demostración. Sea G un grupo de orden p y sea $a \in G$ cualquiera, con $a \neq e$. Entonces por el Teorema de Lagrange $o(a) \mid p$. Como $a \neq e$, $o(a) \neq 1$, y por lo tanto $o(a) = p$. Concluimos que $\langle a \rangle = G$. Luego G es un grupo cíclico de orden finito p , y por el Teorema 5.4.3, $G \simeq \mathbb{Z}_p$. \square

Ya hemos notado que un grupo cíclico puede tener más de un generador. Estudiaremos el problema de establecer los posibles generadores de un grupo cíclico a la luz del isomorfismo con $(\mathbb{Z}, +)$ o $(\mathbb{Z}_m, +)$. Recordemos que del Lema 4.6.9:

- En \mathbb{Z} , los únicos generadores son 1 y -1 .
- En \mathbb{Z}_m , \bar{k} es un generador si y sólo si $(k : m) = 1$.

Teorema 5.4.7. *Sea $G = \langle a \rangle$ un grupo cíclico. Entonces*

1. *Si G es infinito, a y a^{-1} son los únicos generadores de G .*
2. *Si G es finito de orden m , entonces a^k es un generador de G si y sólo si $\text{m.c.d.}(k, m) = 1$.*

Demostración. Supongamos que $G = \langle a \rangle$ es un grupo cíclico de orden infinito generado por $a \in G$. Entonces $f : \mathbb{Z} \rightarrow G$ dado por $f(k) = a^k$ es un isomorfismo. Por el Teorema 5.4.1, los únicos generadores de G son $f(1)$ y $f(-1)$. Como $a = f(1)$, el otro generador es $f(-1) = f(1)^{-1} = a^{-1}$.

Supongamos ahora que $G = \langle a \rangle$ es un grupo cíclico de orden finito m . Nuevamente, tenemos un isomorfismo $f : \mathbb{Z}_m \rightarrow G$ dado por $f(\bar{k}) = a^k$. Por el Teorema 5.4.1, los generadores de G son $f(\bar{k})$ tales que $\text{m.c.d.}(k, m) = 1$. En particular, como $a = f(\bar{1})$, los generadores de G son los elementos de la forma a^k con $\text{m.c.d.}(k, m) = 1$. \square

El análisis desarrollado hasta acá debería habernos convencido que para estudiar cualquier propiedad de un grupo cíclico basta conocer las propiedades de los grupos aditivos \mathbb{Z} y \mathbb{Z}_m .

Nos interesa ahora caracterizar el orden de un elemento a de un grupo G cualquiera, no necesariamente cíclico. Por definición, $o(a)$ es el orden del subgrupo cíclico generado por a , $H = \langle a \rangle \subset G$. Tenemos:

Teorema 5.4.8. *Sea G un grupo y $a \in G$.*

1. *a tiene orden infinito si y sólo si vale: $[a^k = e \text{ si y sólo si } k = 0]$. En ese caso, los elementos a^k con $k \in \mathbb{Z}$ son todos distintos entre sí.*
2. *a tiene orden finito si y sólo si existe $m \in \mathbb{N}$ tal que $a^m = e$. En este caso,*

$$(5.4) \quad o(a) = \min\{k \in \mathbb{N} : a^k = e\}$$

y $a^r = a^s$ si y sólo si $r \equiv s \pmod{m}$. Es decir, $\langle a \rangle = \{e, a, a^2, \dots, a^{o(a)-1}\}$.

Demostración. Supongamos que $a \in G$ tiene orden infinito. Entonces $H = \langle a \rangle$ es un grupo cíclico de orden infinito y existe un isomorfismo $f : \mathbb{Z} \rightarrow H$ tal que $f(1) = a$. En particular, $\ker(f) = \{0\}$.

Observemos que como $f(1) = a$, tenemos que $a^k = f(1)^k = f(k1) = f(k)$. Luego

$$a^k = e \iff f(k) = e \iff k \in \ker(f) = \{0\} \iff k = 0.$$

Supongamos ahora que $a \in G$ es tal que $a^k = e$ si y sólo si $k = 0$. Veamos que a tiene orden infinito. Supongamos por el contrario que a tiene orden finito m . Entonces $H = \langle a \rangle$ es isomorfo a \mathbb{Z}_m y existe un isomorfismo $f : \mathbb{Z}_m \rightarrow H$ tal que $f(\bar{1}) = a$. Como $m\bar{1} = \bar{m} = \bar{0}$, tenemos $a^m = f(m\bar{1}) = f(\bar{0}) = e$, lo que contradice la hipótesis. Luego $o(a)$ es infinito.

Finalmente, como $a^k = f(k)$ para el isomorfismo $f : \mathbb{Z} \rightarrow H$, resulta

$$a^k = a^j \iff f(k) = f(j) \iff k = j.$$

En particular, si $k \neq j$, $a^k \neq a^j$ como queríamos ver. Esto concluye la prueba de 1.

Veamos la prueba del punto 2. A partir del punto 1 (negando ambas proposiciones) tenemos que a tiene orden finito si y sólo si existe $k \in \mathbb{N}$ tal que $a^k = e$.

Supongamos entonces que $a \in G$ es un elemento de orden m y veamos que vale (5.4). Consideremos el isomorfismo $f : \mathbb{Z}_m \rightarrow \langle a \rangle$ tal que $f(\bar{1}) = a$. Como $k\bar{1} = \bar{0}$ si y sólo si k es un múltiplo de m , tendremos que $a^k = e$ si y sólo si k es un múltiplo de m . En particular, cualquier valor $k \in \mathbb{N}$ tal que $a^k = e$ verifica $k \geq m$ y por lo tanto $m = o(m) = \min\{k \in \mathbb{N} : a^k = e\}$. La última afirmación es inmediata del isomorfismo entre $\langle a \rangle$ y \mathbb{Z}_m . Dejamos los detalles como **ejercicio**. \square

Ejemplo 5.4.9. Consideremos el grupo $(\mathbb{Z}_{10}, +)$. Entonces \bar{k} será un generador de \mathbb{Z}_{10} si y sólo si $\text{m.c.d.}(k, 10) = 1$. O sea, los generadores de \mathbb{Z}_{10} son $\bar{1}, \bar{3}, \bar{7}$ y $\bar{9}$. Por lo tanto los posibles subgrupos propios de \mathbb{Z}_{10} son los subgrupos cíclicos generados por $\bar{2}, \bar{4}, \bar{5}, \bar{6}$ y $\bar{8}$.

Por el Teorema de Lagrange, los elementos de \mathbb{Z}_{10} tienen orden 1, 2, 5 o 10. El único elemento de orden 1 es la identidad $\bar{1}$, y los elementos de orden 10 son los generadores de \mathbb{Z}_{10} .

Observemos que $o(\bar{2}) = 5$. En efecto, $1 \cdot \bar{2} = \bar{2}, 2 \cdot \bar{2} = \bar{4}, 3 \cdot \bar{2} = \bar{6}, 4 \cdot \bar{2} = \bar{8}$ y $5 \cdot \bar{2} = \bar{10} = \bar{0}$. O sea 5 es el menor entero k tal que $k\bar{2} = \bar{0}$. Por lo tanto, en \mathbb{Z}_{10} , $\langle \bar{2} \rangle \simeq \mathbb{Z}_5$. En particular, como 5 es primo, de este isomorfismo concluimos que cualquier elemento en $\langle \bar{2} \rangle$ es un generador de $\langle \bar{2} \rangle$. En particular, como $\bar{4}, \bar{6}, \bar{8} \in \langle \bar{2} \rangle$, tendremos que

$$\langle \bar{2} \rangle = \langle \bar{4} \rangle = \langle \bar{6} \rangle = \langle \bar{8} \rangle \simeq \mathbb{Z}_5.$$

Sólo nos queda explorar qué ocurre $\bar{5}$. Aquí tendremos $2 \cdot \bar{5} = \bar{0}$ y por lo tanto $o(\bar{5}) = 2$. En este caso, $\langle \bar{5} \rangle = \{\bar{0}, \bar{5}\} \simeq \mathbb{Z}_2$.

Concluimos que cualquier subgrupo propio de \mathbb{Z}_{10} es isomorfo a \mathbb{Z}_5 o a \mathbb{Z}_2 . \blacksquare

Ejemplo 5.4.10. Consideremos el grupo $\text{Aut}(\mathbb{Z})$ de automorfismos de \mathbb{Z} . Sea $f \in \text{Aut}(\mathbb{Z})$. Como \mathbb{Z} es un grupo cíclico generado por ± 1 y un automorfismo envía generadores en generadores, tendremos que $f(1) = 1$ o $f(1) = -1$. Observemos que el valor de $f(1)$ determina completamente f , pues $f(k) = f(k \cdot 1) = kf(1)$. Es decir, si conocemos $f(1)$ sabemos quién es f (ver Ejercicio 27 del Capítulo 4).

Por lo tanto hay sólo dos automorfismos posibles, f_1 tal que $f_1(1) = 1$, en cuyo caso $f_1(k) = k$ y por lo tanto $f_1 = \text{Id}$, o f_2 tal que $f_2(1) = -1$, en cuyo caso $f_2(k) = -k$, o sea $f_2 = -\text{Id}$. Observemos que $f_2 \circ f_2 = f_1$ y por lo tanto $\text{Aut}(\mathbb{Z})$ es un grupo cíclico de orden 2, cuyo generador es $f_2 = -\text{Id}$. Concluimos que $\text{Aut}(\mathbb{Z}) \simeq \mathbb{Z}_2$.

Observemos que un grupo con dos elementos, digamos $G = \{e, a\}$ debe ser automáticamente isomorfo a \mathbb{Z}_2 , pues $a^2 = e$ (no puede ser $a^2 = a$ pues podríamos cancelar y obtendríamos $a = e$). \blacksquare

Ejemplo 5.4.11. Consideremos ahora el grupo $\text{Aut}(\mathbb{Z}_4)$. Nuevamente f queda determinado por $f(\bar{1})$. Como $\bar{1}$ es un generador de \mathbb{Z}_4 , $f(\bar{1})$ también debe ser un generador, y por lo tanto tenemos nuevamente dos opciones: $f_1(\bar{1}) = \bar{1}$, o sea $f_1 = \text{Id}$, o $f_2(\bar{1}) = \bar{3}$. Luego $\text{Aut}(\mathbb{Z}_4) = \{\text{Id}, f_2\} \simeq \mathbb{Z}_2$. \blacksquare

Ejemplo 5.4.12. Consideremos finalmente el grupo $\text{Aut}(\mathbb{Z}_5)$. Aquí cualquier elemento es un generador, y por lo tanto tenemos cuatro posibles automorfismos: $f_1 = \text{Id}$, f_j , $j = 2, 3, 4$ tal que $f_j(\bar{1}) = \bar{j}$. Tomemos f_3 e intentemos determinar f_3^k . Tendremos

1. $f_3^2(\bar{1}) = f_3 \circ f_3(\bar{1}) = f_3(\bar{3}) = f_3(3 \cdot \bar{1}) = 3 \cdot f_3(\bar{1}) = \bar{9} = \bar{4}$. Como f_3^2 es un automorfismo, está determinado por su valor en $\bar{1}$ y por lo tanto $f_3^2 = f_4$.
2. $f_3^3(\bar{1}) = f_3 \circ f_4(\bar{1}) = f_3(\bar{4}) = 4 \cdot f_3(\bar{1}) = \bar{12} = \bar{2}$. Luego $f_3^3 = f_2$.
3. Finalmente, $f_3^4(\bar{1}) = f_3 \circ f_2(\bar{1}) = f_3(\bar{2}) = 2 \cdot f_3(\bar{1}) = \bar{6} = \bar{1}$, luego $f_3^4 = \text{Id} = f_1$.

Concluimos que f_3 es un elemento de orden 4, y $\langle f_3 \rangle = \text{Aut}(\mathbb{Z}_5)$, con lo cual $\text{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_4$. ■

5.5. Producto directo y producto libre de grupos

Hemos visto que si G y H son grupos, entonces $G \times H$ es un grupo con la operación

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2).$$

Siempre que denotemos simplemente $G \times H$ sin aclarar cuál es la operación, entenderemos esta estructura de grupo. En este caso hablamos del **producto directo** de G y H , o de **suma directa** en el caso que $(G, +)$ y $(H, +)$ sean grupos abelianos, en cuyo caso lo denotamos $G \oplus H$.

Un grupo puede ser isomorfo un producto directo aunque no esté presentado como tal:

Ejemplo 5.5.1. Consideremos el grupo multiplicativo (\mathbb{C}^*, \cdot) . Entonces (\mathbb{R}^+, \cdot) y (S^1, \cdot) son subgrupos de (\mathbb{C}^*, \cdot) (ver ejemplo 5.3.13) y sea $\varphi : (\mathbb{R}^+, \cdot) \times (S^1, \cdot) \rightarrow (\mathbb{C}^*, \cdot)$ dado por

$$\varphi(r, z) = rz.$$

Observemos que φ es un homomorfismo de grupos. En efecto

$$\varphi((r, z) \cdot (r', z')) = \varphi((rr', zz')) = (rr')(zz') = (rz)(rz') = \varphi(r, z) \cdot \varphi(r', z').$$

Además φ es un monomorfismo:

$$(r, z) \in \ker(\varphi) \iff rz = 1 \iff z = \frac{1}{r} \in \mathbb{R}^+ \xrightarrow{z \in S^1} r = 1, z = 1.$$

Luego $\ker(\varphi) = \{(1, 1)\}$. Finalmente φ es un epimorfismo, pues dado $w \in \mathbb{C}^*$, $w = \varphi(|w|, \frac{w}{|w|})$. Concluimos que φ es un isomorfismo de grupos. ■

Veremos ahora cómo determinar cuando un grupo es efectivamente el producto directo de dos subgrupos. En el Ejemplo 5.5.1 detectamos dos subgrupos $N = (\mathbb{R}^+, \cdot)$ y $K = (S^1, \cdot)$ tales que

$$\mathbb{C}^* = NK = \{nk : n \in N, k \in K\}$$

y $N \cap K = \{1\}$. Además N y K son subgrupos normales, dado que (\mathbb{C}^*, \cdot) es abeliano.

Esto no debería sorprendernos, dado que vimos en el Ejercicio 29 del Capítulo 4 que si $G = N \times K$ es el producto de dos grupos, entonces $N \times \{e_K\}$ y $\{e_N\} \times K$ son subgrupos G , isomorfos a N y K respectivamente, tales que todo elemento de G es el producto de un elemento del primero por un elemento del segundo. Además es fácil ver que se trata de subgrupos normales. Por ejemplo, dado $(n, e_K) \in N \times \{e_K\}$ y $(m, k) \in G$ cualesquiera, se tiene

$$(m, k) \cdot (n, e_K) \cdot (m, k)^{-1} = (mnm^{-1}, kk^{-1}) = (mnm^{-1}, e_K) \in N \times \{e_K\}.$$

Además

$$(N \times \{e_K\}) \cap (\{e_N\} \times K) = \{e = (e_N, e_K)\}.$$

Luego, si un grupo G es isomorfo al producto de dos subgrupos N y K , éstos deben ser subgrupos normales con intersección trivial, y cada elemento de G debe poder describirse como el producto de un elemento de N y un elemento de K . Más precisamente:

Teorema 5.5.2. *Sea G un grupo y sean N y K dos subgrupos de G tales que:*

1. N y K son subgrupos normales de G ;
2. $G = NK = \{nk : n \in N, k \in K\}$;
3. $N \cap K = \{e\}$.

Entonces $G \simeq N \times K$.

Demostración. Consideremos la función $f : N \times K \rightarrow G$ dada por $f(n, k) = nk$. Como $G = NK$, f es sobreyectiva. Veamos que es un homomorfismo de grupos. Por el Ejercicio 9 de este capítulo tenemos que $nk = kn$ para cada $n \in N$ y cada $k \in K$. Luego

$$\begin{aligned} f((n_1, k_1)(n_2, k_2)) &= f(n_1 n_2, k_1 k_2) = (n_1 n_2)(k_1 k_2) = n_1(n_2 k_1)k_2 \\ &= n_1(k_1 n_2)k_2 = (n_1 k_1)(n_2 k_2) = f(n_1, k_1)f(n_2, k_2). \end{aligned}$$

Concluimos que f es un epimorfismo. Por otra parte,

$$(n, k) \in \ker(f) \iff nk = e \iff n = k^{-1} \in N \cap K.$$

Como $N \cap K = \{e\}$ resulta $\ker(f) = \{e\}$ y por lo tanto f es un isomorfismo. \square

Ejemplo 5.5.3. Sean p y q números primos relativos (es decir, m. c. d. $(p, q) = 1$). Probaremos que

$$\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \oplus \mathbb{Z}_q$$

Para ello consideremos los subgrupos normales $N = \langle \bar{p} \rangle$ y $K = \langle \bar{q} \rangle$ de \mathbb{Z}_{pq} . Veamos que $\mathbb{Z}_{pq} = N + K$. Como p y q son coprimos, existen $k_1, k_2 \in \mathbb{Z}$ tales que $k_1 p + k_2 q = 1$. Luego cualquiera sea $k \in \mathbb{Z}$ se tiene $k = (k k_1)p + (k k_2)q$, con lo cual, proyectando a \mathbb{Z}_{pq} , resulta

$$\bar{k} = (k k_1)\bar{p} + (k k_2)\bar{q} \in N + K,$$

es decir, $\mathbb{Z}_{pq} \subset N + K$ y la otra contención es trivial.

Veamos ahora que $N \cap K = \{\bar{0}\}$. Supongamos que $\bar{k} \in N \cap K$. Entonces existen $l, r \in \mathbb{Z}$ tales que $k \equiv lp \pmod{pq}$ y $k \equiv rq \pmod{pq}$. Restando ambas ecuaciones, tenemos que $lp - rq \equiv 0 \pmod{pq}$. Es decir, $lp - rq$ es múltiplo de pq . Ahora, $p \mid lp$ y $p \mid pq$, con lo cual $p \mid rq$, pero como $p \nmid q$ debe ser $p \mid r$. Luego $r = sp$ para algún $s \in \mathbb{Z}$ y por lo tanto $k \equiv spq \equiv 0 \pmod{pq}$. Es decir, $\bar{k} = \bar{0}$ en \mathbb{Z}_{pq} . Concluimos del Teorema 5.5.2 que $\mathbb{Z}_{pq} \simeq N \oplus K$.

Veamos ahora que $N \simeq \mathbb{Z}_q$ y $K \simeq \mathbb{Z}_p$. Como $p\bar{q} = \overline{pq} = \bar{0}$, y para cada $0 < k < p$, $0 < kq < pq$, resulta que $k\bar{q} \neq \bar{0}$. Luego $p = \min\{k \in \mathbb{N}_0 : k\bar{q} = \bar{0}\}$ y por el Teorema 5.4.8 tenemos que $o(K) = o(\bar{q}) = p$. Luego $K \simeq \mathbb{Z}_p$, dado que K es cíclico. De manera análoga resulta $o(N) = q$ y $N \simeq \mathbb{Z}_q$.

Más aún, de la demostración del Teorema 5.5.2 tenemos que $f : N \times K \rightarrow \mathbb{Z}_{pq}$ dada por $f(n, k) = nk$ es un isomorfismo. Como \bar{p} (en \mathbb{Z}_p) $g : \mathbb{Z}_p \rightarrow N$ dado por $g(\bar{j}) = j\bar{p}$. En el Ejercicio 22 de este capítulo veremos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no es cíclico y por lo tanto no es isomorfo a \mathbb{Z}_4 . Luego este resultado no es válido si p y q no son coprimos. ■

Podemos generalizar el Ejemplo 5.5.3 de la siguiente manera.

Teorema 5.5.4. Sean $m_1, m_2, \dots, m_n \in \mathbb{N}$ coprimos dos a dos. Entonces si $m = m_1 \cdots m_n$, entonces

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$$

Más aún, el isomorfismo viene dado por $f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_n})$ donde $[a]_m$ y $[a]_{m_i}$ denotan las clases de $a \in \mathbb{Z}$ en \mathbb{Z}_m o en los respectivos \mathbb{Z}_{m_i} , $i = 1, \dots, n$.

Demostración. Haremos la prueba por inducción sobre n . Claramente para $n = 1$ es trivial, y para $n = 2$ es el Ejemplo 5.5.3. Supongamos que si m_1, \dots, m_n son primos relativos entonces

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$$

Sean entonces m_1, \dots, m_n, m_{n+1} primos relativos y pongamos $m = m_1 m_2 \cdots m_{n+1}$ y $m' = m_1 \cdots m_n$. Entonces m' y m_{n+1} son primos relativos y por el Ejemplo 5.5.3, $\mathbb{Z}_m \simeq \mathbb{Z}_{m'} \oplus \mathbb{Z}_{m_{n+1}}$. Por la hipótesis inductiva $\mathbb{Z}_{m'} \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$, de donde se obtiene el resultado (recordemos que si $G \simeq G'$ y $K \simeq K'$, entonces $G \times K \simeq G' \times K'$).

En particular tenemos que $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ es un grupo cíclico. Veamos que $b = ([1]_{m_1}, \dots, [1]_{m_n})$ es un generador. En efecto, $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ es un grupo de orden m y por lo tanto $mb = ([0]_{m_1}, \dots, [0]_{m_n})$. Sea $r \in \mathbb{N}$ tal que $rb = ([0]_{m_1}, \dots, [0]_{m_n})$. Entonces, como $rb = ([r]_{m_1}, \dots, [r]_{m_n})$, resulta $[r]_{m_i} = [0]_{m_i}$ para cada $i = 1, \dots, n$. Luego r es un múltiplo de m_i para cada $i = 1, \dots, n$. Pero, al ser coprimos dos a dos, el mínimo común múltiplo de m_1, \dots, m_n es m . Luego debe ser $m \leq r$, y por el Teorema 5.4.8, $o(b) = m$. Concluimos que b es un generador de $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ y por la Observación 5.4.4 existe un isomorfismo $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ tal que $f([1]_m) = b$, de donde

$$f([a]_m) = f(a[1]_m) = af([1]_m) = a([1]_{m_1}, \dots, [1]_{m_n}) = (a[1]_{m_1}, \dots, a[1]_{m_n}) = ([a]_{m_1}, \dots, [a]_{m_n})$$

como queríamos probar. □

Ya hemos mencionado (ver el Ejercicio 29 del Capítulo 4) que si G y H son grupos, entonces $G \times \{e_H\}$ y $\{e_G\} \times H$ son subgrupos de $G \times H$ isomorfos a G y H respectivamente. Por otra parte, los grupos G y H se pueden “recuperar” del producto $G \times H$ a partir de las proyecciones canónicas a cada factor. Enunciaremos a continuación con más precisión estas propiedades. La prueba es standard y la dejamos como **ejercicio**.

Teorema 5.5.5. Sean G y H grupos con identidades e_G y e_H respectivamente y sea $G \times H$ el producto directo de G y H . Entonces:

1. Las funciones $i_G : G \rightarrow G \times H$ y $i_H : H \rightarrow G \times H$ dadas por $i_G(g) = (g, e_H)$ y $i_H(h) = (e_G, h)$ son monomorfismos de grupos.

2. Las funciones $\pi_G : G \times H \rightarrow G$ y $\pi_H : G \times H \rightarrow H$ dadas por $\pi_G(g, h) = g$ y $\pi_H(g, h) = h$ son epimorfismos de grupos.

Además de la propiedad enunciada en el Teorema 5.5.2, existe otra forma de caracterizar cuándo un grupo es (isomorfo a) el producto de dos grupos. Consideremos los grupos G y H y sea $G \times H$ su producto directo. Sea ahora K un grupo cualquiera para el cual existen homomorfismos $\varphi : K \rightarrow G$ y $\rho : K \rightarrow H$. Definamos $\Psi : K \rightarrow G \times H$ dado por

$$\Psi(k) = (\varphi(k), \rho(k))$$

Entonces $\Psi = \varphi \times \rho$ es un homomorfismo de grupos (ver Ejercicio 29 del Capítulo 4) y verifica trivialmente que $\pi_G \circ \Psi = \varphi$ y $\pi_H \circ \Psi = \rho$, es decir, Ψ hace conmutativo el siguiente diagrama:

$$(5.5) \quad \begin{array}{ccccc} & & K & & \\ & \swarrow \varphi & \downarrow \Psi & \searrow \rho & \\ G & \xleftarrow{\pi_G} & G \times H & \xrightarrow{\pi_H} & H \end{array}$$

Supongamos que $\tilde{\Psi} : K \rightarrow G \times H$ es un homomorfismo que también hace conmutativo el diagrama 6.7, y $\tilde{\Psi}(k) = (\tilde{\Psi}_G(k), \tilde{\Psi}_H(k))$. Entonces:

$$\tilde{\Psi}_G(k) = \pi_G \circ \tilde{\Psi}(k) = \varphi(k)$$

y de manera análoga $\tilde{\Psi}_H(k) = \rho(k)$. Luego $\tilde{\Psi} = \varphi \times \rho = \Psi$. Es decir, Ψ es el único homomorfismo que hace conmutativo el diagrama (6.7). Esta propiedad caracteriza completamente el producto directo de grupos:

Teorema 5.5.6. Sean G, H, P grupos tales que existen homomorfismos $\tilde{\pi}_G : P \rightarrow G$ y $\tilde{\pi}_H : P \rightarrow H$ de modo que si K es un grupo cualquiera y $\varphi : K \rightarrow G$ y $\rho : K \rightarrow H$ son homomorfismos de grupos, entonces existe un único homomorfismo $\Psi : K \rightarrow P$ tal que $\tilde{\pi}_G \circ \Psi = \varphi$ y $\tilde{\pi}_H \circ \Psi = \rho$:

$$(5.6) \quad \begin{array}{ccccc} & & K & & \\ & \swarrow \varphi & \downarrow \Psi & \searrow \rho & \\ G & \xleftarrow{\tilde{\pi}_G} & P & \xrightarrow{\tilde{\pi}_H} & H \end{array}$$

Entonces P es isomorfo al producto directo $G \times H$.

Demostración. Por hipótesis el diagrama (5.6) conmuta para cualquier grupo K y cualquier par de homomorfismos φ y ρ . En particular, como $\pi_G : G \times H \rightarrow H$ y $\pi_H : G \times H \rightarrow H$ son homomorfismos de grupos, poniendo $K = G \times H$ en (5.6) deberá existir un único homomorfismo $\Psi : G \times H \rightarrow P$ de modo que el siguiente diagrama conmuta:

$$\begin{array}{ccccc} & & G \times H & & \\ & \swarrow \pi_G & \downarrow \Psi & \searrow \pi_H & \\ G & \xleftarrow{\tilde{\pi}_G} & P & \xrightarrow{\tilde{\pi}_H} & H \end{array}$$

Por otra parte, podemos reemplazar K por P en el diagrama (6.7) y obtenemos que existe un único homomorfismo $\theta : P \rightarrow G \times H$ tal que el siguiente diagrama también conmuta:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \tilde{\pi}_G & \downarrow \theta & \searrow \tilde{\pi}_H & \\ G & \xleftarrow{\pi_G} & G \times H & \xrightarrow{\pi_H} & H \end{array}$$

Tenemos entonces que los homomorfismos $\Psi \circ \theta$ y $\theta \circ \Psi$ hacen conmutar los diagramas:

$$\begin{array}{ccccc} & & G \times H & & \\ & \swarrow \pi_G & \downarrow \theta \circ \Psi & \searrow \pi_H & \\ G & \xleftarrow{\pi_G} & G \times H & \xrightarrow{\pi_H} & H \end{array} \quad \begin{array}{ccccc} & & P & & \\ & \swarrow \tilde{\pi}_G & \downarrow \Psi \circ \theta & \searrow \tilde{\pi}_H & \\ G & \xleftarrow{\tilde{\pi}_G} & P & \xrightarrow{\tilde{\pi}_H} & H \end{array}$$

Como $\text{Id}_{G \times H} : G \times H \rightarrow G \times H$ y $\text{Id}_P : P \rightarrow P$ también son homomorfismos que hacen conmutar trivialmente estos diagramas, de la unicidad dada en las hipótesis, resulta que $\theta \circ \Psi = \text{Id}_{G \times H}$ y $\Psi \circ \theta = \text{Id}_P$. Concluimos que Ψ y θ son isomorfismos de grupos, uno inverso del otro. \square

Observación 5.5.7. Las propiedades el tipo de las enunciadas en el Teorema 5.5.6, es decir, que caracterizan una cierta estructura a partir de la existencia de un diagrama conmutativo bajo ciertas hipótesis, se denominan propiedades universales. Las estudiaremos en más detalle en el capítulo siguiente.

Finalizaremos esta sección introduciendo una nueva operación entre grupos, el denominado *producto libre* de grupos. Realizar formalmente esta construcción puede resultar complicado, pero se basa en un principio muy simple: supongamos que tenemos una familia $\{G_\alpha\}_{\alpha \in A}$ de grupos. Los elementos de los grupos G_α son *letras* y el producto libre de todos ellos consiste en todas las *palabras* que se pueden formar “listando” alternativamente elementos de los grupos G_α . La operación entre dos palabras es simplemente la yuxtaposición de palabras, con la salvedad que si la última letra g_n de una palabra y la primera letra h_1 de la siguiente pertenecen al mismo grupo, debemos reemplazar el par de letras $g_n h_1$ por la letra $g = g_n \cdot h_1$.

Comenzaremos haciendo una serie de definiciones y estableciendo la nomenclatura que utilizaremos.

Definición 5.5.8. Sea $\{X_\alpha\}_{\alpha \in A}$ una familia indexada de conjuntos. Se denomina **unión disjunta** de la familia $\{X_\alpha\}_{\alpha \in A}$ a

$$\bigsqcup_{\alpha \in A} X_\alpha := \bigcup_{\alpha \in A} X_\alpha \times \{\alpha\} = \{(x, \alpha) : x \in X_\alpha, \alpha \in A\}.$$

Es decir, en la unión disjunta los elementos están etiquetados para distinguir de qué conjunto provienen, y los conjuntos que intervienen son considerados distintos aunque formalmente sean el mismo. Por ejemplo, para la unión usual, $\mathbb{R} \cup \mathbb{R} = \mathbb{R}$ y tenemos que $3 \in \mathbb{R} \cup \mathbb{R}$, $\pi \in \mathbb{R} \cup \mathbb{R}$, etc. Sin embargo, en la unión disjunta $\mathbb{R} \sqcup \mathbb{R}$ debemos indicar a qué copia de \mathbb{R} pertenecen los elementos. Así, un elemento de $\mathbb{R} \sqcup \mathbb{R}$ es $(3, 1)$ o $(\pi, 2)$, para indicar que 3 pertenece a la primer copia de \mathbb{R} y π pertenece a la segunda.

Muchas veces obviaremos las etiquetas e indicaremos a los conjuntos a los que pertenecen los elementos, sobreentendiendo que elementos pertenecientes a conjuntos con índices distintos son distintos. En el ejemplo anterior, si ponemos $X_1 = \mathbb{R}$ y $X_2 = \mathbb{R}$, escribimos $3 \in X_1$, $\pi \in X_2$ en vez de indicar los elementos como $(3, 1)$ o $(\pi, 2)$. De esta manera, en $X_1 \sqcup X_2$, el elemento $3 \in X_1$ es distinto del elemento $3 \in X_2$, dado que formalmente estos elementos son respectivamente $(3, 1)$ y $(3, 2)$.

Definición 5.5.9. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos. Una **palabra** de longitud $m \in \mathbb{N}$ en la familia $\{G_\alpha\}_{\alpha \in A}$ es una m -upla (x_1, x_2, \dots, x_m) de elementos de la unión disjunta $\bigsqcup_{\alpha \in A} G_\alpha$. Denotamos $m = \text{long}(p)$ para indicar que p es una palabra de longitud m . Cada elemento de G_α para algún $\alpha \in A$, se denomina una **letra**.

Se denomina **palabra vacía** a una 0-upla, es decir, una úpla sin elementos, y se denota por $()$. Por definición, $\text{long}(()) = 0$.

Denotamos por \mathcal{W} al conjunto de palabras en la familia $\{G_\alpha\}_{\alpha \in A}$ junto con la palabra vacía.

Dada una palabra $p = (x_1, x_2, \dots, x_m) \in \mathcal{W}$ de longitud m y una palabra $q = (y_1, y_2, \dots, y_k) \in \mathcal{W}$ de longitud k , se define la **concatenación** pq de las palabras p y q como la palabra en \mathcal{W} de longitud $m + k$ dada por

$$pq = (x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_k).$$

La concatenación de una palabra p con la palabra vacía (a derecha o izquierda) se define como la palabra p . Es decir, $p() = ()p = p$.

La concatenación de palabras es claramente asociativa, y por definición $()$ es la identidad en \mathcal{W} para la concatenación de palabras. Por lo tanto:

Teorema 5.5.10. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia (junto con la palabra vacía). Entonces \mathcal{W} con la concatenación de palabras es un monoide con identidad la palabra vacía $()$.

Observemos que hasta el momento la estructura de grupo de los integrantes de la familia $\{G_\alpha\}$ no juega ningún rol particular. De hecho, el conjunto \mathcal{W} de las palabras que pueden formarse tomando letras

en un conjunto X arbitrario, con la concatenación de palabras como operación, es un semigrupo denominado **semigrupo libre** sobre el conjunto X . Si además agregamos la palabra vacía, tenemos un monoide denominado **monoide libre** sobre X .

Nos interesa sin embargo definir un grupo a partir de las palabras en una familia indexada de grupos $\{G_\alpha\}_{\alpha \in A}$. Denotemos para ello e_α la identidad en cada G_α y consideremos dos transformaciones en \mathcal{W} denominadas **reducciones elementales**:

Definición 5.5.11. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia junto con la palabra vacía.

- Si una palabra $p = (x_1, x_2, \dots, x_m) \in \mathcal{W}$ verifica que $x_i, x_{i+1} \in G_\alpha$ para algún $\alpha \in A$, denotamos por $r_i(p)$ a la palabra de longitud $m - 1$ dada por

$$r_i(p) = (x_1, \dots, x_{i-1}, x_i \cdot x_{i+1}, \dots, x_m) \in \mathcal{W}.$$

Es decir, $r_i(p)$ elimina la letra x_{i+1} de p y reemplaza la letra x_i por $x_i \cdot x_{i+1}$, donde \cdot es el producto en el grupo G_α al cual pertenecen tanto x_i como x_{i+1} .

- Si una palabra $p = (x_1, x_2, \dots, x_m) \in \mathcal{W}$ verifica que $x_i = e_\alpha$ para algún $\alpha \in A$, denotamos $s_i(p)$ a la palabra de longitud $m - 1$ dada por

$$s_i(p) = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m).$$

Es decir, en $s_i(p)$ se elimina la letra i -ésima de p si ésta es la identidad en uno de los grupos G_α .

Si $p \in \mathcal{W}$, $r_i(p)$ o $s_i(p)$ se denominan **reducciones elementales** de p . Si q es una reducción elemental de p lo denotamos $p \xrightarrow{1} q$. Si p no admite una reducción elemental, p se denomina una **palabra reducida**.

Dada $p \in \mathcal{W}$, una palabra q que se obtiene tras aplicar sucesivas reducciones elementales de p se denomina una **reducción** de p . Lo denotamos $p \rightarrow q$.

Ejemplo 5.5.12. Consideremos los grupos (\mathbb{Z}_5^*, \cdot) y $(\mathbb{R}, +)$ y sea $p = (\bar{1}, \bar{3}, 7, 5, \bar{4}, \bar{4})$ una palabra en $\mathbb{Z}_5^* \sqcup \mathbb{R}$. Podemos aplicar sucesivamente a p las siguientes reducciones elementales:

$$q_1 = s_1(p) = (\bar{3}, 7, 5, \bar{4}, \bar{4})$$

$$q_2 = r_2(q_1) = (\bar{3}, 7 + 5, \bar{4}, \bar{4}) = (\bar{3}, 12, \bar{4}, \bar{4})$$

$$q_3 = r_3(q_2) = (\bar{3}, 12, \bar{4} \cdot \bar{4}) = (\bar{3}, 12, \bar{16}) = (\bar{3}, 12, \bar{1})$$

$$q_4 = s_3(q_3) = (\bar{3}, 12)$$

Así, q_1 , q_2 , q_3 y q_4 son reducciones de p y tenemos

$$p \xrightarrow{1} q_1 \xrightarrow{1} q_2 \xrightarrow{1} q_3 \xrightarrow{1} q_4, \quad \text{y} \quad p \rightarrow q_4$$

Además, la palabra q_4 es una palabra reducida. ■

Observación 5.5.13. *Es inmediato que la relación en \mathcal{W} dada por $p \mathcal{R} q$ si $p \rightarrow q$ es transitiva. Esto es, si $p \rightarrow q'$ y $q' \rightarrow q$, entonces $p \rightarrow q$.*

Intuitivamente, tras aplicar una cantidad finita de reducciones elementales a una palabra p obtenemos una reducción q de p que es una palabra reducida, es decir, que no admite más reducciones elementales. Más precisamente:

Lema 5.5.14. *Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Si $p \in \mathcal{W}$, entonces p es una palabra reducida o bien existe una palabra reducida $q \in \mathcal{W}$ que es una reducción de p .*

Demostración. Haremos la prueba por inducción sobre la longitud m de las palabras en \mathcal{W} .

Claramente la palabra vacía es una palabra reducida, y si p es una palabra de longitud 1, entonces p es una palabra reducida o bien $p = (e_\alpha)$ para algún $\alpha \in A$, en cuyo caso $s_1(p) = ()$, es decir, $p \xrightarrow{1} ()$.

Supongamos entonces que toda palabra q de longitud $\text{long}(q) \leq m$ es una palabra reducida o bien admite una reducción a una palabra reducida, y sea p una palabra de longitud $m+1$. Si p es una palabra reducida, no hay nada que probar. Si p no es reducida, existe una reducción elemental $p \xrightarrow{1} q_1$, con $\text{long}(q_1) = m$. Por hipótesis inductiva, o bien q_1 es una palabra reducida, en cuyo caso p admite una reducción a una palabra reducida, o bien existe una reducción q de q_1 que es una palabra reducida. En este segundo caso, q es también una reducción de p , lo que concluye la prueba. \square

Nos proponemos probar ahora que toda palabra admite una única reducción a una palabra reducida. Para ello necesitaremos algunos resultados previos.

Lema 5.5.15. *Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Sea $p \in \mathcal{W}$. Si $x, y \in \mathcal{W}$ son tales que $x \neq y$, $p \xrightarrow{1} x$ y $p \xrightarrow{1} y$, entonces existe $z \in \mathcal{W}$ tal que $x \xrightarrow{1} z$ y $y \xrightarrow{1} z$.*

Demostración. Sea $p = (p_1, \dots, p_m)$. Supongamos primero que $x = r_i(p)$, $y = r_j(p)$, con $i \neq j$ dado que $x \neq y$. Podemos suponer sin pérdida de generalidad que $i < j$. Entonces existen $\alpha, \beta \in A$ tales que $p_i, p_{i+1} \in G_\alpha$ y $p_j, p_{j+1} \in G_\beta$.

Si $j = i+1$, entonces necesariamente $\alpha = \beta$ y

$$x = (p_1, \dots, p_{i-1}, p_i \cdot p_j, p_{j+1}, \dots, p_m), \quad y = (p_1, \dots, p_i, p_j \cdot p_{j+1}, p_{j+2}, \dots, p_m).$$

Luego poniendo $z = (p_1, \dots, p_{i-1}, p_i \cdot p_j \cdot p_{j+1}, p_{j+2}, \dots, p_m)$ se tiene $x \xrightarrow{1} z$, $y \xrightarrow{1} z$.

Si $i < i+1 < j < j+1$, entonces

$$x = (p_1, \dots, p_i \cdot p_{i+1}, \dots, p_j, p_{j+1}, \dots, p_m), \quad y = (p_1, \dots, p_i, p_{i+1}, \dots, p_j \cdot p_{j+1}, \dots, p_m).$$

Entonces poniendo $z = (p_1, \dots, p_i \cdot p_{i+1}, \dots, p_j \cdot p_{j+1}, \dots, p_m)$ resulta $x \xrightarrow{1} z$, $y \xrightarrow{1} z$.

Si ahora reemplazamos r_i o r_j por s_i o s_j la prueba es similar. Dejamos los detalles como **ejercicio**. \square

Corolario 5.5.16. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Sea $p \in \mathcal{W}$. Si $x, y \in \mathcal{W}$ son tales que $x \neq y$, $p \rightarrow x$ y $p \rightarrow y$, entonces existe $z \in \mathcal{W}$ tal que $x \rightarrow z$ e $y \rightarrow z$.

Demostración. Escribamos $p \xrightarrow{k} q$ si q se obtiene a partir de p tras k reducciones elementales. Es decir, existen $q_1, \dots, q_k = q \in \mathcal{W}$ tales que

$$p \xrightarrow{1} q_1 \xrightarrow{1} q_2 \xrightarrow{1} \dots \xrightarrow{1} q_k = q.$$

Observemos que en este caso tendremos

$$(5.7) \quad p \xrightarrow{l} q_l, \quad q_l \xrightarrow{k-l} q$$

para cada $1 \leq l < k$.

Probaremos primero por inducción sobre k que dados $p, x, y \in \mathcal{W}$ cualesquiera, entonces

$$\left. \begin{array}{l} p \xrightarrow{1} x \\ p \xrightarrow{k} y \end{array} \right\} \implies \exists z \in \mathcal{W} / x \rightarrow z \wedge y \rightarrow z.$$

Si $k = 1$ el resultado es válido por el Lema 5.5.15. Supongamos que el resultado vale para $k \in \mathbb{N}$ y sea $y \in \mathcal{W}$ tal que $p \xrightarrow{k+1} y$. De (5.7) existirá y' tal que $p \xrightarrow{k} y'$ y $y' \xrightarrow{1} y$. Por hipótesis inductiva tenemos que

$$\left. \begin{array}{l} p \xrightarrow{1} x \\ p \xrightarrow{k} y' \end{array} \right\} \implies \exists z' \in \mathcal{W} / x \rightarrow z' \wedge y' \rightarrow z'.$$

Aplicando nuevamente la hipótesis inductiva tenemos:

$$\left. \begin{array}{l} y' \xrightarrow{1} y \\ y' \xrightarrow{k} z' \end{array} \right\} \implies \exists z \in \mathcal{W} / y \rightarrow z \wedge z' \rightarrow z.$$

Como $x \rightarrow z'$ y $z' \rightarrow z$ resulta $x \rightarrow z$. Concluimos que dados $p, x, y \in \mathcal{W}$ cualesquiera, entonces

$$(5.8) \quad \left. \begin{array}{l} p \xrightarrow{1} x \\ p \rightarrow y \end{array} \right\} \implies \exists z \in \mathcal{W} / x \rightarrow z \wedge y \rightarrow z.$$

Probaremos ahora por inducción sobre $m \in \mathbb{N}$ que dados $p, x, y \in \mathcal{W}$ cualesquiera, entonces

$$(5.9) \quad \left. \begin{array}{l} p \xrightarrow{m} x \\ p \rightarrow y \end{array} \right\} \implies \exists z \in \mathcal{W} / x \rightarrow z \wedge y \rightarrow z.$$

Si $m = 1$, el resultado sigue de (5.8). Si $m > 1$, entonces existe $x' \in \mathcal{W}$ tal que $p \xrightarrow{m-1} x' \xrightarrow{1} x$. Aplicando la hipótesis inductiva a $p \xrightarrow{m-1} x'$ y $p \rightarrow y$, existirá $z' \in \mathcal{W}$ tal que $x' \rightarrow z'$ y $y \rightarrow z'$. Ahora podemos aplicar (5.8) a $x' \xrightarrow{1} x$, $x' \rightarrow z'$, y existirá $z \in \mathcal{W}$ tal que $x \rightarrow z$, $z' \rightarrow z$. Finalmente, como $y \rightarrow z'$ y $z' \rightarrow z$ tendremos también $y \rightarrow z$ como queríamos ver. \square

Teorema 5.5.17. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Si $p \in \mathcal{W}$, entonces p es una palabra reducida o bien existe una única palabra reducida $q \in \mathcal{W}$ que es una reducción de p .

Demostración. La existencia de q fue probada en el Lema 5.5.14. Supongamos que $p \in \mathcal{W}$ sea tal que existen palabras reducidas $x, y \in \mathcal{W}$ tales que $p \rightarrow x$ y $p \rightarrow y$. Si $x \neq y$, del Corolario 5.5.16 existe $z \in \mathcal{W}$ tal que $x \rightarrow z$ y $y \rightarrow z$. Pero esto no puede ocurrir, pues x e y son palabras reducidas y, por definición, no admiten ninguna reducción. Luego debe ser $x = y$. \square

Definición 5.5.18. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Si $p \in \mathcal{W}$, denotamos por $r(p)$ a $r(p) = p$ si p es una palabra reducida, o $r(p) = q$ donde q es la única palabra reducida en \mathcal{W} tal que $p \rightarrow q$.

El conjunto de todas las palabras reducidas en \mathcal{W} se denomina **producto libre** de la familia $\{G_\alpha\}_{\alpha \in A}$ y se denota $\bigstar_{\alpha \in A} G_\alpha$.

En función del Teorema 5.5.17, queda bien definida la función

$$r : \mathcal{W} \rightarrow \bigstar_{\alpha \in A} G_\alpha, \quad p \mapsto r(p)$$

del conjunto de palabras en la familia $\{G_\alpha\}_{\alpha \in A}$ en el producto libre de esta familia.

Lema 5.5.19. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y sea \mathcal{W} el conjunto de palabras en esta familia, junto con la palabra vacía. Entonces la función $r : \mathcal{W} \rightarrow \bigstar_{\alpha \in A} G_\alpha$ verifica que

$$r(pq) = r(r(p)r(q))$$

para cada $p, q \in \mathcal{W}$.

Demostración. Supondremos que p y q no son palabras reducidas (en caso que lo fueran, la prueba es similar, basta con considerar los diferentes casos, y la dejamos como **ejercicio**).

Es inmediato que $r(p)r(q)$ es una reducción de pq , dado que es la concatenación de una reducción de p con una reducción de q . Esto es, $pq \rightarrow r(p)r(q)$. Si $r(p)r(q)$ es una palabra reducida, entonces $r(r(p)r(q)) = r(p)r(q)$. Si no, tenemos que $r(p)r(q) \rightarrow r(r(p)r(q))$. En cualquier caso, $pq \rightarrow r(r(p)r(q))$, es decir, $r(r(p)r(q))$ es una palabra reducida que es una reducción de pq . Por la unicidad dada en el Teorema 5.5.17, resulta que $r(r(p)r(q)) = r(pq)$. \square

Ejemplo 5.5.20. Consideremos los grupos $G_1 = (\mathbb{Z}_5^*, \cdot)$ y $G_2 = (\mathbb{R}, +)$. Sean $p = (\bar{1}, \bar{3}, 7, 5, \bar{4}, \bar{4})$ y $q = (3, \bar{2}, \bar{3})$.

Vimos en el Ejemplo 5.5.12 que $r(p) = (\bar{3}, 12)$. Por otra parte, tenemos

$$q \xrightarrow{1} (3, \bar{6}) = (3, \bar{1}) \xrightarrow{1} (3)$$

Luego $r(q) = (3)$. Además $pq = (\bar{1}, \bar{3}, 7, 5, \bar{4}, \bar{4}, 3, \bar{2}, \bar{3})$. Luego

$$pq \rightarrow (\bar{3}, 12, \bar{16}, 3, \bar{6}) \rightarrow (\bar{3}, 12, 3) \rightarrow (\bar{3}, 15)$$

con lo cual $r(pq) = (\bar{3}, 15)$. Por otra parte, $r(p)r(q) = (\bar{3}, 12, 3)$ (que no es una palabra reducida) y $r(r(p)r(q)) = (\bar{3}, 15) = r(pq)$. \blacksquare

Teorema 5.5.21. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia indexada de grupos y consideremos la operación \cdot en $\bigstar_{\alpha \in A} G_\alpha$ dada por

$$p \cdot q = r(pq)$$

donde pq es la concatenación de las palabras p y q . Entonces $\left(\bigstar_{\alpha \in A} G_\alpha, \cdot\right)$ es un grupo tal que la palabra vacía $()$ es la identidad y si $p = (x_1, \dots, x_m)$ es una palabra reducida, entonces $p^{-1} = (x_m^{-1}, \dots, x_1^{-1})$

Demostración. Veamos primero que la operación es asociativa. Sean $x, y, z \in \bigstar_{\alpha \in A} G_\alpha$. Observemos que $r(x) = x$, $r(y) = y$ y $r(z) = z$, dado que se trata de palabras reducidas. Entonces por el Lema 5.5.19 resulta

$$\begin{aligned} (x \cdot y) \cdot z &= r(xy) \cdot z = r(r(xy)z) = r(r(xy)r(z)) = r((xy)z) \\ &= r(x(yz)) = r(r(x)r(yz)) = r(xr(yz)) = x \cdot r(yz) \\ &= x \cdot (y \cdot z). \end{aligned}$$

Por otra parte, como $p \cdot () = ()p = p$ para cualquier palabra p , esto vale en particular si p es una palabra reducida, con lo cual

$$p \cdot () = r(p()) = r(p) = p$$

y de la misma manera $() \cdot p = p$. Luego $()$ es la identidad de $\bigstar_{\alpha \in A} G_\alpha$.

Finalmente, veamos por inducción sobre la longitud de las palabras reducidas que si $p = (x_1, \dots, x_m)$, entonces $q = (x_m^{-1}, \dots, x_1^{-1})$ es el inverso de p . Observemos primero que si p es una palabra reducida, también lo es q . En efecto, ningún x_i es la identidad de alguno de los grupos G_α , y por lo tanto tampoco lo es x_i^{-1} . Como además en p no hay letras consecutivas en un mismo grupo, tampoco las hay en q .

Si $\text{long}(p) = 1$, es decir, $p = (x_1)$, sea $q = (x_1^{-1})$. Supongamos que $x_1 \in G_\alpha$, con lo cual $x_1^{-1} \in G_\alpha$. Entonces $pq = (x_1, x_1^{-1})$ y tenemos que

$$r_1(pq) = (x_1 x_1^{-1}) = (e_\alpha) \implies s_1(r_1(pq)) = ()$$

Luego $pq \rightarrow ()$ y por lo tanto $p \cdot q = r(pq) = ()$. De manera análoga resulta $s_1(r_1(qp)) = ()$ y por lo tanto $r(qp) = ()$ y $q \cdot p = ()$.

Supongamos ahora que el resultado vale para todas las palabras de longitud m y sea $p = (x_1, \dots, x_{m+1})$ una palabra de longitud $m+1$. Sea $q = (x_{m+1}^{-1}, \dots, x_1^{-1})$ y pongamos $y = (x_1, \dots, x_m)$, $z = (x_m^{-1}, \dots, x_1^{-1})$. Por hipótesis inductiva, $z = y^{-1}$. Además $pq = (x_1, \dots, x_m, x_{m+1}, x_{m+1}^{-1}, x_m^{-1}, \dots, x_1)$. Luego

$$r_{m+1}(pq) = (x_1, \dots, x_m, x_{m+1} x_{m+1}^{-1}, x_m^{-1} \dots, x_1^{-1}) \implies s_{m+1}(r_{m+1}(pq)) = (x_1, \dots, x_m, x_m^{-1}, \dots, x_1^{-1}) = yz$$

Tenemos entonces que

$$pq \rightarrow yz \rightarrow ()$$

con lo cual $p \cdot q = ()$. De manera análoga se prueba que $q \cdot p = ()$. □

Al igual que ocurre en el producto directo de grupos, cada uno de los grupos de la familia $\{G_\alpha\}_{\alpha \in A}$ puede identificarse con un subgrupo del producto libre. Más precisamente:

Teorema 5.5.22. Sea $\{G_\alpha\}_{\alpha \in A}$ una familia de grupos. Para cada $\gamma \in A$ sea $i_\gamma : G_\gamma \rightarrow \ast_{\alpha \in A} G_\alpha$ dada por

$$i_\gamma(x) = \begin{cases} (x) & \text{si } x \neq e_\gamma \\ () & \text{si } x = e_\gamma \end{cases}.$$

Entonces i_γ es un monomorfismo de grupos.

Demostración. Observemos que la definición de i_γ puede resumirse poniendo $i_\gamma(x) = r((x))$, dado que $r((x)) = ()$ si y sólo si $x = e_\gamma$. Sean $x, y \in G_\gamma$. Entonces

$$i_\gamma(x) \cdot i_\gamma(y) = r((x)(y)) = r((xy)) = i_\gamma(xy).$$

Luego i_γ es un homomorfismo. Por la apreciación que hicimos al principio resulta inmediato que $\ker(i_\gamma) = \{e_\gamma\}$ y por lo tanto i_γ es un monomorfismo. \square

El producto libre también puede caracterizarse por una propiedad universal. En lo que sigue, para simplificar la exposición, y porque es suficiente para nuestro objetivo (que es introducir la suma en una categoría, algo que veremos en el capítulo siguiente) trabajaremos con el producto libre de dos grupos. Los resultados sin embargo pueden generalizarse a una familia arbitraria de grupos.

Teorema 5.5.23. Sean G y H grupos y consideremos los homomorfismos $i_G : G \rightarrow G * H$ y $i_H : H \rightarrow G * H$, donde $G * H$ denota el producto libre de G y H . Supongamos que K es un grupo para el cual existen homomorfismos $\varphi : G \rightarrow K$ y $\rho : H \rightarrow K$, y pongamos $F : G \sqcup H \rightarrow K$ dada por

$$F(x) = \begin{cases} \varphi(x) & \text{si } x \in G \\ \rho(x) & \text{si } x \in H \end{cases}$$

Pongamos $\Psi := \varphi * \rho : G * H \rightarrow K$ dada por

$$\Psi(()) = e_K, \quad \Psi((x_1, x_2, \dots, x_m)) = F(x_1)F(x_2) \cdots F(x_m).$$

Entonces Ψ es el único homomorfismo de grupos tal que $\Psi \circ i_G = \varphi$ y $\Psi \circ i_H = \rho$.

$$(5.10) \quad \begin{array}{ccccc} G & \xrightarrow{i_G} & G * H & \xleftarrow{i_H} & H \\ & \searrow \varphi & \downarrow \Psi & \swarrow \rho & \\ & & K & & \end{array}$$

Demostración. Veamos que Ψ es un homomorfismo de grupos. Observemos primero que si $q = ()$, entonces para cualquier palabra reducida $p \in \ast_{\alpha \in A} G_\alpha$ se tiene

$$\Psi(p \cdot ()) = \Psi(p) = \Psi(p)e_K = \Psi(p)\Psi(())$$

y de manera análoga $\Psi(() \cdot p) = \Psi(())\Psi(p)$. Además si $p = (x_1, \dots, x_m)$, $q = (y_1, \dots, y_n)$ y x_m e y_1 pertenecen a grupos distintos, entonces $p \cdot q = pq = (x_1, \dots, x_m, y_1, \dots, y_n)$ es una palabra reducida y

$$\Psi(p \cdot q) = F(x_1) \cdots F(x_m)F(y_1) \cdots F(y_n) = \Psi(p)\Psi(q).$$

Para continuar la prueba haremos, como es usual, una doble inducción sobre la longitud de las palabras.

Supongamos que p es una palabra de longitud 1 y probemos por inducción sobre $m = \text{long}(q)$ que $\Psi(p \cdot q) = \Psi(p)\Psi(q)$.

Supongamos entonces que $\text{long}(q) = 1$. Si pq es una palabra reducida, el resultado ya fue probado. Si pq no es una palabra reducida y $p = (x)$ con $x \in G$ (si $x \in H$ el razonamiento es análogo), entonces deberá ser $q = (y)$ con $y \in G$. Luego $xy \in G$, y como φ es un homomorfismo, resulta

$$\Psi(p \cdot q) = \Psi((xy)) = F(xy) = \varphi(xy) = \varphi(x)\varphi(y) = F(x)F(y) = \Psi(p)\Psi(q).$$

Supongamos ahora que para cada palabra p de longitud 1 y cada palabra reducida q de longitud m vale $\Psi(p \cdot q) = \Psi(p)\Psi(q)$. Sea $p = (x)$ y sea $w = (w_1, \dots, w_{m+1})$ una palabra reducida de longitud $m+1$. Nuevamente si pw es una palabra reducida, no hay nada que probar. Si pw no es reducida, entonces x y w_1 pertenecen al mismo grupo (digamos G , la prueba para el caso en que ambos pertenezcan a H es análoga).

Si $xw_1 \neq e_G$, entonces $p \cdot w = (xw_1, w_2, \dots, w_{m+1}) = (xw_1) \cdot w'$, donde $w' = (w_2, \dots, w_{m+1})$ es una palabra reducida. Además $w = (w_1) \cdot w'$. Luego por hipótesis inductiva,

$$\Psi(p \cdot w) = \Psi((xw_1) \cdot w') = \Psi((xw_1))\Psi(w')$$

Por el caso base, $\Psi(xw_1) = \Psi((x))\Psi((w_1))$ y por la hipótesis inductiva $\Psi(w) = \Psi((w_1) \cdot w') = \Psi((w_1))\Psi(w')$. Finalmente, resulta

$$\Psi(p \cdot w) = \Psi((xw_1))\Psi(w') = \Psi((x))\Psi((w_1))\Psi(w') = \Psi((x))\Psi(w) = \Psi(p)\Psi(w)$$

como queríamos probar.

Si $xw_1 = e_G$, es decir, $w_1 = x^{-1}$, entonces $p \cdot w = w'$. Como además $w = (w_1) \cdot w'$, por hipótesis inductiva $\Psi(w) = \Psi((w_1))\Psi(w')$ y resulta

$$\begin{aligned} \Psi(p \cdot w) &= \Psi(w') = e_K \Psi(w') = \varphi(e_G) \Psi(w') = \varphi(xw_1) \Psi(w') = \varphi(x) \varphi(w_1) \Psi(w') \\ &= \Psi((x)) \Psi((w_1)) \Psi(w') = \Psi(p) \Psi(w) \end{aligned}$$

Concluimos que si p es una palabra de longitud 1, entonces para cualquier palabra reducida w , $\Psi(p \cdot w) = \Psi(p)\Psi(w)$.

Probemos ahora por inducción sobre $\text{long}(p) = m$ que para cualquier palabra reducida q , $\Psi(p \cdot q) = \Psi(p)\Psi(q)$. El caso $m = 1$ es el prueba anterior. Supongamos que el resultado vale para una palabra reducida p de longitud m y una palabra reducida q cualquiera.

Si ahora $w = (w_1, w_2, \dots, w_{m+1})$ es una palabra reducida de longitud $m+1$, entonces $p = (w_1) \cdot w'$ donde $w' = (w_2, \dots, w_m)$ es una palabra reducida de longitud m . Luego, $w \cdot q = (w_1) \cdot w' \cdot q$. Por hipótesis inductiva $\Psi(w' \cdot q) = \Psi(w')\Psi(q)$ y por el caso base $\Psi(w \cdot q) = \Psi((w_1) \cdot (w' \cdot q)) = \Psi(w_1)\Psi(w' \cdot q)$. Luego

$$\Psi(w \cdot q) = \Psi((w_1))\Psi(w' \cdot q) = \Psi((w_1))\Psi(w')\Psi(q)$$

Nuevamente aplicando el caso base resulta $\Psi(w) = \Psi((w_1) \cdot w') = \Psi((w_1))\Psi(w')$ y por lo tanto $\Psi(w \cdot q) = \Psi(w)\Psi(q)$ como queríamos probar.

Por como está definido Ψ resulta inmediato que $\Psi \circ i_G = \varphi$ y $\Psi \circ i_H = \rho$.

Supongamos que $\Psi' : G * H \rightarrow K$ es un homomorfismo que también verifica $\Psi' \circ i_G = \varphi$ y $\Psi' \circ i_H = \rho$. Probaremos, nuevamente por inducción sobre la longitud de una palabra reducida, que $\Psi' = \Psi$.

Si $p = ()$, como Ψ' es un homomorfismo debe ser $\Psi'(()) = e_K = \Psi(())$. Supongamos que $\text{long}(p) = 1$, o sea $p = (x)$ con $x \in G$ o $x \in H$. Si $x \in G$, $p = i_G(x)$ y por lo tanto

$$\Psi'(p) = \Psi'(i_G(x)) = \varphi(x) = \Psi(x)$$

y lo mismo ocurre si $x \in H$.

Supongamos ahora que Ψ' y Ψ coinciden sobre todas las palabras reducidas de longitud m , y sea $p = (x_1, \dots, x_{m+1})$ una palabra reducida de longitud $m+1$. Entonces $p = (x_1) \cdot p'$ donde $p' = (x_2, \dots, x_{m+1})$ es una palabra reducida de longitud m . Como Ψ y Ψ' son homomorfismos y $\Psi = \Psi'$ sobre las palabras de longitud 1 y longitud m , resulta

$$\Psi'(p) = \Psi'((x_1))\Psi'(p') = \Psi((x_1))\Psi(p') = \Psi((x_1) \cdot p') = \Psi(p)$$

lo que concluye la prueba. □

Con los mismos argumentos que en el Teorema 5.5.23 y con las mismas técnicas que en la prueba 5.5.6, puede demostrarse el siguiente resultado. Dejamos los detalles como **ejercicio**.

Teorema 5.5.24. Sean G , H y L grupos, tales que existen dos homomorfismos $\tilde{i}_G : G \rightarrow L$ y $\tilde{i}_H : H \rightarrow L$, de modo que para cualquier grupo K y cualquier par de homomorfismos $\varphi : H \rightarrow K$ y $\rho : G \rightarrow K$, existe un único homomorfismo $\Psi : L \rightarrow K$ tal que $\Psi \circ \tilde{i}_G = \varphi$ y $\Psi \circ \tilde{i}_H = \rho$. Entonces L es isomorfo al producto libre $G * H$.

5.6. Aplicaciones a la aritmética modular

Para finalizar este Capítulo analizaremos algunas aplicaciones de la teoría de grupos a la teoría de números analizando algunas propiedades de la aritmética modular.

Teorema 5.6.1 (Pequeño Teorema de Fermat). Sea p un número primo. Entonces para todo entero a no divisible por p resulta $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Si a no es divisible por p , entonces $\bar{a} \neq \bar{0}$. Luego \bar{a} es un elemento del grupo multiplicativo (\mathbb{Z}_p^*, \cdot) , que es un grupo de orden $p-1$. Por el Teorema de Lagrange (Teorema 5.1.10), $o(\bar{a})$ divide a $p-1$, es decir, existe $k \in \mathbb{N}$ tal que $p-1 = ko(\bar{a})$. Como $\bar{a}^{o(\bar{a})} = \bar{1}$, tenemos $a^{o(\bar{a})} \equiv 1 \pmod{p}$ y por lo tanto $(a^{o(\bar{a})})^k \equiv 1 \pmod{p}$ o sea $a^{p-1} \equiv 1 \pmod{p}$. □

Como consecuencia inmediata del Teorema 5.6.1 obtenemos el siguiente corolario. Es interesante notar que ambos enunciados son en realidad equivalentes. Dejamos la prueba como **ejercicio**.

Corolario 5.6.2. Sea p un número primo y $a \in \mathbb{Z}$ cualquiera. Entonces $a^p \equiv a \pmod{p}$.

Ejemplo 5.6.3. Aplicaremos el Pequeño Teorema de Fermat (PTF) para calcular de manera sencilla el resto de dividir 27^{2154} por 11. Observemos que como 11 es primo y $11 \nmid 27 = 3^3$, del PTF tendremos que $27^{10} \equiv 1 \pmod{11}$. Pero entonces $27^{k10} \equiv 1^k \pmod{11}$ para cualquier $k \in \mathbb{Z}$. Escribamos 2154 como $2154 = 215 \cdot 10 + 4$. Luego $27^{2154} = 27^{215 \cdot 10} \cdot 27^4$. Como $27^{215 \cdot 10} \equiv 1 \pmod{11}$, resulta $27^{2154} \equiv 27^4 \pmod{11}$. Ahora bien, $r_{11}(27) = 5$ y por lo tanto $27^4 \equiv 5^4 \pmod{11}$. Ahora, $5^4 = 25^2$ y como $25 \equiv 3 \pmod{11}$ tenemos

$$27^{2154} \equiv 27^4 \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \pmod{11}.$$

Concluimos que $r_{11}(27^{2154}) = 9$. ■

Un segundo resultado fundamental de la aritmética modular es el denominado *Teorema Chino del Resto*. Este resultado permite resolver sistemas de ecuaciones lineales en congruencia:

$$(5.11) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

No es de esperar que estos sistemas tengan siempre solución. Consideremos por ejemplo el siguiente sistema simple:

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 7 \pmod{10} \end{cases}$$

Si un tal x existiese, debería ser de la forma $x = 4k_1 + 2$ y $x = 10k_2 + 7$ para algún par de enteros k_1 y k_2 . Esto implica que existen enteros tales que

$$4k_1 + 2 = 10k_2 + 7 \Leftrightarrow 2(2k_1 - 5k_2) = 5$$

lo cual claramente no puede ocurrir, puesto que el lado izquierdo de la igualdad es siempre un número par, y el lado derecho es siempre impar.

Intentaremos desarrollar primeramente un criterio para determinar cuándo el sistema tiene solución. Más aún, a nivel de la aritmética modular, encontrar una solución de este sistema no significa simplemente encontrar un entero x que las satisfaga a todas, sino que nuestro objetivo será determinarlo unívocamente módulo algún entero m . Esto es, pretendemos reducir el sistema de ecuaciones a una ecuación lineal del tipo

$$x \equiv x_0 \pmod{m}$$

para algún x_0 y algún m .

Teorema 5.6.4 (Teorema Chino del Resto). *Sean m_1, m_2, \dots, m_r números naturales coprimos dos a dos y sea m su producto. Si a_1, a_2, \dots, a_r son números enteros cualesquiera, existe solución al sistema (5.11) y está unívocamente determinada módulo m . Esto es, si x_0 es una solución cualquiera de 5.11, entonces x satisface $x \equiv x_0 \pmod{m}$. En particular, existe un único $x_0 \in \mathbb{Z}$ solución de (5.11) tal que $0 \leq x_0 < m$.*

Demostración. Como m_1, \dots, m_r son primos relativos, por el Teorema 5.5.4 existe un isomorfismo $f : \mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_r}$ tal que $f([a]_m) = ([a]_{m_1}, \dots, [a]_{m_r})$ para cada $a \in \mathbb{Z}$. En particular, f es biyectivo, y por lo tanto dados $a_1, \dots, a_r \in \mathbb{Z}$, deberá existir un único $a \in \mathbb{Z}$ tal que $f([a]_m) = ([a_1]_{m_1}, \dots, [a_r]_{m_r})$. Por lo tanto $a \in \mathbb{Z}$ verifica que $[a]_{m_j} = [a_j]_{m_j}$ para cada $j = 1, \dots, r$, es decir, $a \equiv a_j (m_j)$ para cada $j = 1, \dots, r$, con lo cual $x_0 = a$ es solución de (5.11). \square

La demostración del Teorema Chino del Resto tiene el problema que no nos indica cómo encontrar la solución x_0 que estamos buscando. Presentaremos a continuación un algoritmo que, además de dar una prueba alternativa del Teorema 5.6.4 nos indica como construirla.

Comencemos suponiendo que en (5.11), $a_2 = a_3 = \dots = a_r = 0$. Es decir, tenemos un sistema

$$S_1) \begin{cases} x \equiv a_1 (m_1) \\ x \equiv 0 (m_2) \\ \vdots \\ x \equiv 0 (m_r) \end{cases}$$

Veamos que S_1 tiene solución. Sea $m' = m_2 \cdot m_3 \cdot \dots \cdot m_r$. Observemos que $\text{m. c. d.}(m', m_1) = 1$, pues de otra manera un divisor común debería dividir simultáneamente a m_1 y a alguno de los otros m_j , $j \geq 2$, (dado que los m_j son coprimos dos a dos), y esto no puede ocurrir pues $\text{mcd}(m_1, m_j) = 1$ para cada $j = 2, \dots, r$.

En particular, m' es invertible en $(\mathbb{Z}_{m_1}^*, \cdot)$. Por lo tanto existirá $v' \in \mathbb{Z}$ tal que $m'v' \equiv 1 (m_1)$. Observemos que $m_j \mid m'v'$ para cada $j \geq 2$ pues $m_j \mid m'$. Luego $m'v' \equiv 0 (m_j)$ para cada $j \geq 2$. Pongamos $x_1 = a_1 m'v'$. Tendemos entonces

$$m'v' \equiv 0 (m_j) \Rightarrow x_1 \equiv 0 (m_j), \quad \text{para todo } j = 2, \dots, r.$$

Además

$$m'v' \equiv 1 (m_1) \Rightarrow x_1 = a_1 m'v' \equiv a_1 (m_1).$$

Luego x_1 es una solución de S_1 .

De manera análoga podemos encontrar una solución x_j de cada uno de los sistemas S_j dados por

$$S_j) \begin{cases} x \equiv a_j (m_j) \\ x \equiv 0 (m_i) \quad \forall i \neq j \end{cases}$$

Si ahora ponemos

$$x_0 = \sum_{j=1}^r x_j$$

tenemos que

$$x_j \equiv a_j (m_j), \quad x_i \equiv 0 (m_j) \quad \forall i \neq j \Rightarrow x_0 \equiv a_j (m_j).$$

Como esto es válido para cada j , tenemos que x_0 es solución de (5.11).

Ejemplo 5.6.5. Consideremos el sistema

$$S) \begin{cases} x \equiv 4 (8) \\ x \equiv 10 (35) \\ x \equiv 1 (3) \end{cases}$$

La demostración del Teorema Chino del Resto nos da un modo de obtener una solución particular, y a partir de ella todas las soluciones del sistema S . Debemos considerar tres sistemas:

$$S_1) \begin{cases} x \equiv 4 (8) \\ x \equiv 0 (35) \\ x \equiv 0 (3) \end{cases}, \quad S_2) \begin{cases} x \equiv 0 (8) \\ x \equiv 10 (35) \\ x \equiv 0 (3) \end{cases}, \quad S_3) \begin{cases} x \equiv 0 (8) \\ x \equiv 0 (35) \\ x \equiv 1 (3) \end{cases}$$

Sea $m'_1 = 35 \cdot 3 = 105$. Tenemos que encontrar v'_1 tal que $m'_1 v'_1 \equiv 1 (8)$. Comencemos observando que $105 = 13 \cdot 8 + 1$ y entonces $105 \equiv 1 (8)$. Por lo tanto $v'_1 = 1$ y $x_1 = m'_1 v'_1 a_1 = 105 \cdot 4 = 420$. Observemos que efectivamente

$$420 = 12 \cdot 35, \quad 420 = 140 \cdot 3, \quad 420 = 52 \cdot 8 + 4$$

y por lo tanto $x_1 \equiv 4 (8)$, $x_1 \equiv 0 (35)$, $x_1 \equiv 0 (3)$. O sea que x_1 es solución de S_1 . Para hallar las soluciones de S_2 consideremos $m'_2 = 8 \cdot 3 = 24$. Encontremos v'_2 tal que $24v'_2 \equiv 1(35)$. Recordemos que v'_2 es el coeficiente de 24 que se obtiene aplicando el algoritmo de Euclides para encontrar $\text{mcd}(24, 35)$. Tenemos:

$$35 = 24 \cdot 1 + 11$$

$$24 = 11 \cdot 2 + 2$$

$$11 = 5 \cdot 2 + 1$$

de donde

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (24 - 11 \cdot 2) = -5 \cdot 24 + 11 \cdot 11 = -5 \cdot 24 + 11 \cdot (35 - 24) = -16 \cdot 24 + 11 \cdot 35.$$

Luego $v'_2 = -16$ y $x_2 = 24 \cdot (-16) \cdot 10 = -3840$. De manera análoga se obtiene una solución $x_3 = 280$ de S_3 . Luego una solución x_0 de S es

$$x_0 = 420 - 3840 + 280 = -3140.$$

Ahora bien, $m = 8 \cdot 25 \cdot 3 = 840$, y por lo tanto la única solución x'_0 con $0 \leq x'_0 < m$ es $r_{840}(-3140) = 220$. Concluimos finalmente que las soluciones de S están caracterizadas por $x \equiv 220 (840)$. ■

Ejemplo 5.6.6. Para vender una enciclopedia cuyo precio es menor a \$10.000 una librería ofrece los siguientes planes de pago:

1. anticipo de \$200 y cuotas mensuales de \$180.
2. anticipo de \$300 y cuotas mensuales de \$250.
3. anticipo de \$370 y cuotas mensuales de \$490.

¿Cuál es el precio total de la enciclopedia?

Solución: Supongamos que P es el precio de la obra. Entonces cualquiera de los planes se calcula mediante la fórmula $P = a + cn$, donde a es el anticipo, c es el monto de cada cuota y n es el número de cuotas,

que claramente varía de plan a plan. Por lo tanto nuestras incógnitas son P y n_1, n_2, n_3 , donde n_i es el número de cuotas del plan i . En principio pareciera que tenemos un sistema de ecuaciones a coeficientes enteros (denominadas *ecuaciones diofánticas*) en las incógnitas P, n_1, n_2, n_3 . Pero si observamos mejor, vemos que

$$P - a = cn \Leftrightarrow P \equiv a (c).$$

Es decir, reduciendo el problema a un sistema de ecuaciones en congruencia podemos obviar las incógnitas n_i , cuyo valor estará determinado una vez que conozcamos P (aunque en el enunciado del problema no se pide hallar la cantidad de cuotas de cada plan). Debemos entonces resolver

$$S) \begin{cases} P \equiv 200 (180) \\ P \equiv 300 (250) \\ P \equiv 370 (490) \end{cases}$$

Lo primero que debemos observar es que 180, 250 y 490 no son coprimos dos a dos (pues 10 es un divisor común de todos). Sin embargo, observemos que

$$y \equiv kn (km) \Leftrightarrow y - kn = lkm \Leftrightarrow \frac{y}{k} - n = lm \Leftrightarrow \frac{y}{k} \equiv n (m)$$

Pongamos entonces $x = P/10$. Tenemos que P será solución de S si y sólo si x es solución de

$$S') \begin{cases} x \equiv 20 (18) \\ x \equiv 30 (25) \\ x \equiv 37 (49) \end{cases}$$

En este caso 18, 25 y 49 sí son primos relativos dos a dos, pues $18 = 2 \cdot 3^2$, $25 = 5 \cdot 5$, $49 = 7 \cdot 7$. Siguiendo el procedimiento del ejemplo anterior obtenemos que 22430 es una solución de S' . En este caso $m = 22050$ y es fácil comprobar que $22430 \equiv 380 (22050)$. Con lo cual $x_0 = 380$ es la solución más pequeña que podemos encontrar. Observemos que cualquier otra solución diferirá de x_0 en un múltiplo de 22050 y por lo tanto x_0 es la única solución menor que 1000. Luego $P = 3800$ es la única solución de S menor que 10000 ■

Ejemplo 5.6.7. El algoritmo de encriptación RSA. El algoritmo RSA es una forma muy sencilla de encriptar datos que se utiliza aún hoy. Se basa en la existencia de dos claves: una clave pública que todos conocen y con la cual pueden cifrar sus mensajes, y una clave privada que se utiliza para descifrarlos.

Supongamos que una persona A decide mandar un mensaje a una persona B , y quiere que sólo B lo pueda leer. La persona B elige dos números primos p y q y considera un número $e < (p-1)(q-1)$ que sea coprimo con $(p-1)(q-1)$. En un principio sólo B conoce estos tres números, pero comunica a A los números e y $n = pq$. El par (n, e) constituye la clave pública, a la que todos tienen acceso. A los fines prácticos, para que el algoritmo sea eficiente, los números p , q y e deben ser muy grandes (en general se utilizan números de más de 170 cifras). Para ejemplificarlo, tomemos los siguientes números:

$$p = 3, q = 11, n = pq = 33, (p-1)(q-1) = 20, e = 7.$$

Ahora A convierte su mensaje en un número $M < n$ y lo transforma en el único número $c < n$ tal que $c \equiv M^e (n)$. En vez de enviar el mensaje M completo, envía sólo el número c que B deberá descifrar.

Supongamos siguiendo con el ejemplo que el mensaje sin cifrar es $M = 15$. Entonces

$$M^e = 15^7 \equiv 27 \pmod{33}$$

con lo cual el mensaje cifrado es $c = 27$.

Observemos que en el camino alguien podría hacker el mensaje, y así tendría acceso al número c . No entendería lo que A efectivamente está enviando porque el mensaje está cifrado. Aún teniendo acceso a la clave pública (n, e) , debería hallar M tal que $c \equiv M^e \pmod{n}$. Ahora bien, si este problema en una ecuación normal se resuelve de manera sencilla aplicando la raíz e -ésima a c para recuperar M , en la aritmética modular esto no es cierto. Como ejemplo podemos observar que $1 \equiv 2^2 \pmod{3}$, pero no es cierto que $\sqrt{1} \equiv 2 \pmod{3}$. En nuestro ejemplo, $\sqrt[7]{27}$ ni siquiera es un número entero.

Para descifrar el mensaje B utiliza la clave privada, que está dada por el único $d < ((p-1)(q-1))$ tal que $ed \equiv 1 \pmod{((p-1)(q-1))}$. Observemos que como el e elegido originalmente es coprimo con el módulo, el número d buscado siempre existe. En nuestro ejemplo, $d = 3$, pues $de = 21 \equiv 1 \pmod{20}$.

Ahora bien, como $de \equiv 1 \pmod{((p-1)(q-1))}$ tenemos que

$$de = \lambda(p-1)(q-1) + 1 = \lambda_1(p-1) + 1 = \lambda_2(q-1) + 1$$

donde $\lambda_1 = \lambda(q-1)$ y $\lambda_2 = \lambda(p-1)$. Por lo tanto

$$c^d = M^{de} = (M^{p-1})^{\lambda} M \equiv M \pmod{p}$$

pues por el Pequeño Teorema de Fermat $M^{p-1} \equiv 1 \pmod{p}$. Con el mismo argumento resulta $c^d \equiv M \pmod{q}$. Es decir que M es solución del sistema

$$\begin{cases} x = c^d \pmod{p} \\ x = c^d \pmod{q} \end{cases}$$

que por el Teorema Chino del resto es única módulo $n = pq$.

En nuestro ejemplo, $c^d = 27^3 = 19683 \equiv 15 \pmod{33}$.

Observemos que como $n = pq$ y la factorización en números primos es única, conociendo n debería ser sencillo recuperar los primos p y q . La eficacia de este algoritmo se basa en que en realidad es muy difícil factorizar un número muy grande en factores primos. ■

5.7. Ejercicios

1. Probar que todo grupo cíclico G es un grupo abeliano.
2. Sea G un grupo abeliano. Mostrar que para todo n natural, $H = \{g \in G : g^n = e\}$ constituye un subgrupo de G .
3. Sea G un grupo abeliano y sea T el conjunto de los elementos de G de orden finito. Probar que T es un subgrupo de G . Mostrar con un ejemplo que esto es falso si G no es abeliano.
4. **Diffie-Hellman.** Alice y Bob desean ponerse de acuerdo en un número secreto. Sin embargo, saben que sus comunicaciones son monitoreadas por Eve, lo cual parece imposibilitar esta tarea. Sabiendo que existe un grupo cíclico finito G con generador g para el cual resulta computacionalmente costoso

- resolver el problema de Diffie-Hellman (dados g^a y g^b , computar g^{ab}); proponer un protocolo que les permita a Alice y Bob establecer una clave en común y secreta.
5. Probar que $\mathbb{Z} \times \mathbb{Z}$ no es un grupo cíclico, pero que puede ser generado por un subconjunto finito. ¿Es cierto que un conjunto finito siempre genera grupos finitos y que un conjunto infinito siempre genera conjuntos infinitos?
 6. Sea S_3 el grupo de biyecciones de $\{1, 2, 3\}$ en sí mismo.
 - a) Sea H el grupo cíclico de S_3 generado por $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Probar que ninguna clase a derecha (excepto el mismo H que es la clase de la identidad) es también una clase a izquierda módulo H .
 - b) Probar que existe $a \in S_3$ tal que $aH \cap Ha = \{a\}$.
 - c) Sea K el grupo cíclico de S_3 generado por $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Probar K es normal en S_3 .
 - d) Probar que S_n no es cíclico para $n \geq 3$.
 7. Sea N el subconjunto de S_4 que consiste de aquellas permutaciones tales que $f(4) = 4$. ¿Es N un subgrupo normal de S_4 ?
 8. Sean K y N subgrupos de G , con $N \triangleleft G$. Probar que:
 - a) $N \cap K$ es un subgrupo normal de K .
 - b) $\langle N \cup K \rangle = NK = KN$, donde $NK = \{nk : n \in N, k \in K\}$ y lo mismo para KN .
 - c) Si K es un subgrupo normal de G y $K \cap N = \{e\}$, entonces $kn = nk$ para cada $k \in K$ y cada $n \in N$.
 - d) La composición $\pi \circ i$, donde $i : K \rightarrow G$ es la inclusión canónica y $\pi : G \rightarrow G/N$ es la proyección al cociente, es un isomorfismo de K en G/N .
 9. Probar que si $N_1 \triangleleft G$ y $N_2 \triangleleft G$, entonces
 - a) $N_1 \cap N_2 \triangleleft G$.
 - b) Si $N_1 \cap N_2 = \{e\}$, entonces $n_1 n_2 = n_2 n_1$ para cada $n_1 \in N_1$ y cada $n_2 \in N_2$.
 10. Probar que D_4 posee subgrupos A y B tales que $A \triangleleft B$ y $B \triangleleft D_4$ pero A no es normal en D_4 .
 11. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Probar que
 - a) si $N \triangleleft G$, $f(N)$ no necesariamente es un subgrupo normal de H .
 - b) Si H es abeliano y $N \subset \ker(f)$, entonces $N \triangleleft G$.
 12. Sea N un subgrupo normal de G tales que N y G/N son grupos finitamente generados (es decir, en ambos casos son el grupo generado por una cantidad finita de elementos). Probar que G es finitamente generado.
 13. El *centro* de un grupo G se define como $Z(G) = \{g \in G : gx = xg \ \forall x \in G\}$ (ver Ejercicio 19 de del Capítulo 4). Mostrar que:
 - a) El centro de S_n con $n \geq 2$ es $\{1\}$.
 - b) $Z(G) \triangleleft G$ para todo grupo G .

c) $Z(G/Z(G))$ es trivial.

14. Sean $a, b \in \mathbb{R}$, definimos:

$$\tau_{a,b} : \mathbb{R} \rightarrow \mathbb{R}, \tau_{a,b}(x) = ax + b$$

Probar que

- a) $G = \{\tau_{a,b} : a \in \mathbb{R} - \{0\}, b \in \mathbb{R}\}$ es un grupo bajo la operación de composición.
- b) $H = \{\tau_{a,b} \in G : a \in \mathbb{Q}\}$ es un subgrupo de G .
- c) $N = \{\tau_{1,b} \in G\}$ es un subgrupo normal de G .
- d) $G/N \simeq (\mathbb{R} - \{0\}, *)$.

15. Sea $X = \{z \in \mathbb{C} : z^n = 1 \text{ p.a. } n \in \mathbb{N}\}$. Probar que X es un subgrupo de $(\mathbb{C} - \{0\}, \cdot)$ y $X \simeq \mathbb{Q}/\mathbb{Z}$.

16. Sean $k, m \in \mathbb{Z}$. Probar que $\langle km \rangle$ es un subgrupo normal de $\langle k \rangle$ y que $\langle k \rangle / \langle km \rangle$ es isomorfo a \mathbb{Z}_m .

17. Sea $\mathcal{N}(G)$ el conjunto de subgrupos normales de un grupo G . Probar que $(\mathcal{N}(G), \subseteq)$ es un retículo. Describir las operaciones join y meet.

18. Sean A, B grupos y consideremos el grupo producto $A \times B$. Sean $\pi_A : A \times B \rightarrow A$ y $\pi_B : A \times B \rightarrow B$ las proyecciones sobre cada factor. Probar que

- a) $A \times \{e_B\} \triangleleft A \times B$ y $\{e_A\} \times B \triangleleft A \times B$
- b) π_A y π_B son epimorfismos.
- c) $\ker(\pi_A) = \{e_A\} \times B$ y $\ker(\pi_B) = A \times \{e_B\}$.
- d) $(A \times B) / (A \times \{e_B\}) \simeq B$
- e) Si $N \triangleleft A$ y $M \triangleleft B$ entonces $N \times M \triangleleft A \times B$ y $(A \times B) / (N \times M) \simeq (A/N) \times (B/M)$.

19. Probar que si un grupo tiene una cantidad finita de subgrupos, debe ser un grupo finito.

20. Probar que si G es un grupo infinito, entonces G tiene al menos un subgrupo propio.

21. Determinar el grupo $\text{Aut}(\mathbb{Z}_8)$.

22. Probar que $(\mathbb{Z}_2, +) \oplus (\mathbb{Z}_2, +)$ no es cíclico. Concluir que todo grupo de orden 4 es isomorfo a $(\mathbb{Z}_4, +)$ o a $(\mathbb{Z}_2, +) \oplus (\mathbb{Z}_2, +)$.

23. Sea G grupo y H subgrupo de G , demostrar que $H \triangleleft G$ si se cumple al menos una de las siguientes condiciones:

- a) G es abeliano.
- b) $[G : H] = 2$.
- c) $\varphi : G \rightarrow G'$ es un morfismo de grupos, G' es abeliano y H es un subgrupo de G tal que $\ker(\varphi) \subseteq H$.

24. Sean G y H grupos, $N \triangleleft G$, $K \triangleleft H$. Probar que $(N \times K) \triangleleft (G \times H)$.

25. Sean G, H_1, H_2 grupos y $\varphi : G \rightarrow H_1$, $\Psi : G \rightarrow H_2$ dos homomorfismos tales que $\ker(\varphi) \subset \ker(\Psi)$. Probar que existe un único homomorfismo $f : H_1 \rightarrow H_2$ tal que $f \circ \varphi = \Psi$.

26. Sea G un grupo y H un subgrupo de G . H se dice un *subgrupo característico* de G si para cada automorfismo $\varphi : G \rightarrow G$, $\varphi(H) \subset H$.

- a) Probar que si H es un subgrupo característico de un grupo G entonces $H \triangleleft G$.

- b) Probar que H es un subgrupo característico de G si y sólo si para cada grupo K que contiene a G como un subgrupo normal, resulta $H \triangleleft K$.
- c) Sea H un subgrupo característico de un grupo G y sea $\varphi : G \rightarrow G$ un automorfismo. Probar que φ se induce a un automorfismo $\bar{\varphi} : G/H \rightarrow G/H$ y que la asignación $\varphi \mapsto \bar{\varphi}$ es un homomorfismo de $\text{Aut}(G)$ en $\text{Aut}(G/H)$.
- d) Probar que si $H = \langle a \rangle$ es el grupo cíclico generado por $a \in G$ entonces H es un subgrupo característico de G .
- e) Encontrar un subgrupo normal de $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ que no sea un subgrupo característico (lo que prueba que la recíproca del item 26a es falsa).
27. Sean $m, n \in \mathbb{N}$ con $n \mid m$ y $H = \langle \bar{n} \rangle \subset \mathbb{Z}_m$, probar que $\mathbb{Z}_m/H \simeq \mathbb{Z}_n$
28. Sea G un grupo cíclico y $f : G \rightarrow G'$ un homomorfismo de grupos. Probar que $f(G)$ puede tener generadores que no sean la imagen de un generador de G . Es decir, puede existir $b' \in f(G)$ tal que $f(G) = \langle b' \rangle$, pero $b' = f(b)$ y $\langle b \rangle \neq G$.
29. Probar que si $G \simeq G'$ y $H \simeq H'$, entonces $G * H \simeq G' * H'$.
30. Sea p un número primo y $a \in \mathbb{Z}$ tal que $p \nmid a$. Probar que:
- Si $n \equiv r \pmod{p-1}$, entonces $a^n \equiv a^r \pmod{p}$.
 - Concluir en particular que $a^n \equiv a^{r_{p-1}(n)} \pmod{p}$.
31. Probar que para todo $a \in \mathbb{Z}$, $7 \mid a^{362} - a^{62}$.
32. Resolver los siguientes sistemas en congruencia:

$$\begin{array}{lll}
 a) \ S) \begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{7} \end{cases} & b) \ S) \begin{cases} x \equiv 3 \pmod{22} \\ x \equiv 5 \pmod{8} \\ x \equiv 17 \pmod{20} \end{cases} & c) \ S) \begin{cases} 3x \equiv 2 \pmod{7} \\ 7x \equiv 5 \pmod{8} \\ 6x \equiv 8 \pmod{10} \end{cases}
 \end{array}$$

33. La producción diaria de huevos en una granja es inferior a 75. Cierta día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz dijo que eso era imposible. ¿Quién tiene razón?
34. Una banda de 13 piratas asaltó un barco mercantil y se hizo con una gran cantidad de monedas de oro, todas idénticas entre sí. Cuando trataron de distribuirlas equitativamente entre ellos, les sobraron 8 monedas. Por lo tanto, decidieron no repartirlas. Imprevistamente, dos de ellos contrajeron sarampión y murieron. Al volver a intentar repartir las monedas, les sobraron 3, y por lo tanto volvieron a cancelar la distribución. Posteriormente murieron otros 3 piratas ahogados. Los restantes volvieron a intentar distribuir las monedas, pero les sobraron 5. Cansados de tanto intentar distribuir sin poder ser equitativos, optaron por guardar las monedas hasta que se les ocurriese una solución. Tiempo después, los piratas se arrepintieron de todas sus fechorías y decidieron hacer un acto caritativo a modo de redención. Se dirigieron a un pueblo muy pobre en el que había exactamente 1136 personas viviendo, y decidieron integrarse al pueblo para iniciar una nueva vida. Más aún, decidieron que repartirían equitativamente todas las monedas entre todos los habitantes

del pueblo, incluyéndose a ellos. Pero, para su sorpresa, volvieron a sobrar monedas. ¿Cuántas monedas sobraron?

Categorías

6.1. Breve digresión sobre la Teoría de Conjuntos

La teoría de categorías constituye un campo relativamente reciente de estudio. Su primer aparición data de los años 40 del siglo pasado en los trabajos de los matemáticos Samuel Eilenberg y Saunders Mac Lane relativos a investigaciones en topología algebraica. Esta teoría, sin embargo, constituye una especie de teoría general de las estructuras matemáticas y sus relaciones, y muy pronto resultó evidente que podía aplicarse a otras áreas de la matemática o de la informática. Por ejemplo, dos pruebas en áreas diferentes de la matemática pueden utilizar métodos “similares”, y la teoría de categorías proporciona una forma de expresar de manera precisa estas similitudes. De esta forma, es posible dar una prueba en el contexto de las categorías y obtener estos resultados conocidos en áreas diferentes como casos particulares. Esta capacidad unificadora de la teoría hace que sea altamente abstracta. Introduciremos en este capítulo las nociones básicas y veremos a través de ejemplos concretos cómo las estructuras que hemos estudiado se enmarcan en la teoría. Para un tratamiento inicial sobre la teoría de categorías, recomendamos [17] o [18]. Para un tratamiento más avanzado (y completo), puede consultarse [1], [2] o [14].

Antes de empezar debemos hacer una mención al uso que daremos de los conceptos de *conjunto* y *clase*. Hasta el momento hemos usado el concepto de conjunto simplemente como una colección de objetos (esta es la noción que propone Cantor en la teoría original de conjuntos). Esta definición intuitiva es suficiente para el desarrollo de casi la totalidad de las teorías matemáticas, pero como es bien sabido, a nivel más abstracto puede dar lugar a contradicciones y paradojas.

Cabe mencionar la paradoja de Russel, que tiene múltiples enunciaciones equivalentes. Una de ellas es la siguiente: dado un conjunto X , existen dos posibilidades mutuamente excluyentes, $X \in X$ o $X \notin X$. Digamos que X es un conjunto *ordinario* si $X \notin X$, y *extraordinario* si $X \in X$. Es decir, un conjunto ordinario no se tiene a sí mismo como elemento, caso contrario es extraordinario. Claramente, todo conjunto es ordinario o extraordinario. Si ahora consideramos el conjunto Y de todos los conjuntos ordinarios, ¿se trata de un conjunto ordinario o extraordinario? Si Y fuese ordinario, entonces por como lo hemos definido

$Y \in Y$, pero a su vez, al ser ordinario tendríamos $Y \notin Y$. Esto da lugar a una contradicción, y por lo tanto una definición consistente de conjunto no debería ser tan ambigua como la que propuso Cantor.

Para corregir estos problemas Ernst Zermelo y Adolf Fraenkel elaboraron una teoría axiomática de conjuntos que se basa en una serie de “estratificaciones” donde cada conjunto puede definirse sólo a partir de conceptos previamente definidos, con lo cual las nociones de conjunto ordinario o extraordinario no serían admisibles. A los efectos de permitir justamente colecciones de conjuntos o elementos que no necesariamente sean conjuntos pero que comparten una cierta propiedad se introduce el concepto de *clase*. Este concepto no forma parte de la teoría de Zermelo Fraenkel (ZF), se trata de colecciones de objetos demasiado grandes como para ser considerados conjuntos, como por ejemplo la clase de todos los conjuntos, de todos los grupos, etc. (veremos por qué estas “colecciones” no pueden ser conjuntos en seguida).

Existen varias teorías que generalizan la axiomática de ZF (que tampoco incluye el axioma de elección, ver la sección 2.6), y permiten trabajar con clases. Entre ellas, la teoría de von Neumann-Bernays-Gödel (NBG), que fue desarrollada sucesivamente por los matemáticos John von Neumann (1925), Paul Bernays (1937) y Kurt Gödel (1940). A pesar de las dificultades de desarrollar formalmente esta teoría (que ocuparía un curso en sí mismo) las ideas intuitivas que tenemos de conjunto y clase bastarán para el desarrollo de este capítulo (una presentación formal del tema puede consultarse en [3] o [5]).

Básicamente, las clases se comportan esencialmente como conjuntos. Es decir, usaremos la palabra *clase* en vez de *conjunto*, y nos podemos quedar tranquilos que las paradojas que aparecen en la teoría de Cantor desaparecen. Los conjuntos son casos particulares de clases, denominadas *clases pequeñas*. Una clase que no es un conjunto se denomina una *clase propia*. Hablamos en general de *objetos* de una clase, y utilizaremos frecuentemente la notación que usamos en la teoría de conjuntos también para clases. Más precisamente

- Si \mathcal{C} es una clase y A es un objeto de esa clase, escribiremos $A \in \mathcal{C}$.
- Los objetos de una clase sólo pueden ser conjuntos (aquí debemos observar que lo que usualmente llamamos elementos de un conjunto, y los distinguimos de los conjuntos propiamente dichos, tanto en ZF como en NBG son conjuntos).
- Muchas veces definiremos una clase por comprensión, es decir, con una expresión de la forma $\mathcal{C} = \{\text{objetos que cumplen cierta propiedad}\}$.
- Hablaremos de *subclase* de una clase \mathcal{C} cuando tengamos una clase \mathcal{C}' que verifique que todos los objetos de \mathcal{C}' son objetos de \mathcal{C} . Lo denotaremos $\mathcal{C}' \subseteq \mathcal{C}$.
- Dos clases \mathcal{C} y \mathcal{D} son iguales si y sólo si $\mathcal{C} \subseteq \mathcal{D}$ y $\mathcal{D} \subseteq \mathcal{C}$.
- Podemos también definir el producto cartesiano de clases como $\mathcal{C} \times \mathcal{D} = \{(A, B) : A \in \mathcal{C} \wedge B \in \mathcal{D}\}$.
- Una *función de clase*, denotada $f : \mathcal{C} \rightarrow \mathcal{D}$ es una subclase $f \subseteq \mathcal{C} \times \mathcal{D}$ que verifica:

$$\text{i) } \forall A \in \mathcal{C} \exists B \in \mathcal{D} / (A, B) \in f \quad \text{ii) } (A, B), (A, C) \in f \implies B = C.$$

Si $(A, B) \in f$, lo denotamos $B = f(A)$. Dos funciones de clase pueden componerse de la manera usual, y la composición es asociativa.

- Los conjuntos son clases y si \mathcal{C} es un conjunto, entonces una subclase de \mathcal{C} también es un conjunto. Si X es un conjunto, $\mathcal{P}(X)$ es un conjunto. Más aún, si I es un conjunto y $\{X_\alpha\}_{\alpha \in I}$ es una familia de conjuntos (o una clase de conjuntos), la unión, la intersección y el producto cartesiano de los miembros de esta familia es nuevamente un conjunto.

Ahora bien, hemos mencionado que “la colección de todos los conjuntos ordinarios” no es un conjunto. Pero, ¿por qué no puede existir el conjunto de todos los conjuntos? Básicamente, porque la colección de todos los conjuntos ordinarios sería una subclase, y por lo tanto un subconjunto, lo que no puede ocurrir. Una razón tal vez más intuitiva tiene que ver con que la colección de todos los conjuntos es “demasiado grande” para ser un conjunto: si X es un conjunto, entonces $\mathcal{P}(X)$ es un conjunto y $\#X < \#\mathcal{P}(X)$ (aquí $\#$ simboliza el cardinal). Además si X e Y son conjuntos y $X \subseteq Y$, entonces $\#X \leq \#Y$. Supongamos que la colección \mathcal{C} de todos los conjuntos fuese un conjunto. Entonces $\mathcal{P}(\mathcal{C})$ sería un conjunto cuyos elementos son subconjuntos de \mathcal{C} , es decir, en particular son conjuntos y por lo tanto $\mathcal{P}(\mathcal{C}) \subseteq \mathcal{C}$. Pero entonces $\#\mathcal{P}(\mathcal{C}) \leq \#\mathcal{C}$ lo que conduce a un absurdo. Concluimos que \mathcal{C} no es un conjunto, pero sí es una clase.

De manera similar puede probarse que la colección \mathcal{G} de todos los grupos no puede ser un conjunto. En efecto, veamos que *todo conjunto no vacío X admite una operación \cdot de modo que (X, \cdot) es un grupo*. En efecto, si X es un conjunto finito, existe una biyección $f : X \rightarrow \{0, \dots, m-1\}$ para algún $m \in \mathbb{N}$. El conjunto $\{0, \dots, m-1\}$ admite una estructura de grupo identificándolo con \mathbb{Z}_m . Es decir, la biyección f puede pensarse como $f : X \rightarrow \{\bar{0}, \dots, \overline{m-1}\}$ y podemos “copiar” la estructura de grupo de \mathbb{Z}_m de modo que f sea un isomorfismo de grupos. Más precisamente, definimos

$$x \cdot y = f^{-1}(f(x) \cdot f(y))$$

(dejamos como **ejercicio** probar que efectivamente (X, \cdot) es un grupo para quienes no se convenzan del todo del argumento).

Si ahora X es un conjunto infinito, un resultado importante de ZFC (es decir, en la teoría ZF más el axioma de elección, y que vale en NBG) establece que existe una biyección $f : X \rightarrow \mathcal{P}_f(X)$ entre el conjunto X y el conjunto $\mathcal{P}_f(X)$ de subconjuntos finitos de X (ya hemos utilizado este argumento en el Ejemplo 3.7.13 del Capítulo 4). Podemos dar estructura de grupo a $\mathcal{P}_f(X)$ recurriendo a la diferencia simétrica, es decir, si $Y, Z \in \mathcal{P}_f(X)$,

$$Y \triangle Z = (Y \cup Z) - (Y \cap Z).$$

Dejamos como **ejercicio** verificar que efectivamente $(\mathcal{P}_f(X), \triangle)$ es un grupo, con identidad el conjunto vacío \emptyset y tal que $A^{-1} = A$ para cada $A \in \mathcal{P}_f(X)$.

A través de la biyección f podemos copiar la operación a X , poniendo nuevamente $f(x \cdot y) = f^{-1}(f(x) \triangle f(y))$, y con el mismo argumento que antes tendremos que (X, \cdot) es un grupo.

Por lo tanto la clase \mathcal{C} de todos los conjuntos se identifica con una subclase de \mathcal{G} , la colección de todos los grupos. Si \mathcal{G} fuese un conjunto, también debería serlo \mathcal{C} , lo que no puede ocurrir.

Como todo grupo es un monoide, y todo monoide es un semigrupo, con este mismo argumento resulta que la clase de todos los monoides o la clase de todos los semigrupos no son conjuntos.

6.2. Primeras definiciones y ejemplos

Introduciremos en esta sección la definición de una categoría y una serie de ejemplos que aparezcan frecuentemente en el resto del capítulo y en el capítulo siguiente.

Definición 6.2.1. Una categoría \mathcal{C} comprende:

- una clase de **objetos** que denotamos $\text{ob } \mathcal{C}$, cuyos elementos se denotan por A, B, C , etc.
- una clase de **morfismo** o **flechas** que denotamos $\text{mor } \mathcal{C}$, cuyos elementos se denotan por f, g, h , etc.
- dos funciones de clase:
 - $\text{dom} : \text{mor } \mathcal{C} \rightarrow \text{ob } \mathcal{C}$, denominada **dominio**
 - $\text{codom} : \text{mor } \mathcal{C} \rightarrow \text{ob } \mathcal{C}$ denominada **codominio**.

Si $f \in \text{mor } \mathcal{C}$ es tal que $\text{dom}(f) = A \in \text{ob } \mathcal{C}$ y $\text{codom}(f) = B \in \text{ob } \mathcal{C}$, se denota $f : A \rightarrow B$. Denotamos también por $\text{Hom}(A, B) := \{f \in \text{mor } \mathcal{C} : f : A \rightarrow B\}$.

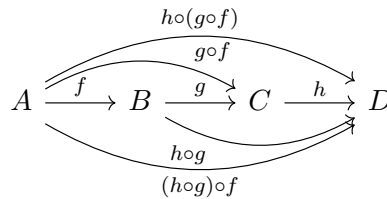
- una función \circ para cada $A, B, C \in \text{ob } \mathcal{C}$, denominada **composición** tal que

$$\circ : \text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C), \quad \circ(f, g) = g \circ f$$

que verifica:

- para cada $A, B, C, D \in \text{ob } \mathcal{C}$, $f \in \text{Hom}(A, B)$, $g \in \text{Hom}(B, C)$ y $h \in \text{Hom}(C, D)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$



Nos referiremos a esta propiedad como **asociatividad** de la composición.

- Para cada $A \in \text{ob } \mathcal{C}$ existe un morfismo $\text{id}_A \in \text{Hom}(A, A)$ denominado **morfismo identidad** tal que:
 - para cada $B \in \text{ob } \mathcal{C}$ y cada $f \in \text{Hom}(A, B)$, $f \circ \text{id}_A = f$;
 - para cada $C \in \text{ob } \mathcal{C}$ y cada $g \in \text{Hom}(C, A)$, $\text{id}_A \circ g = g$.

$$\begin{array}{ccccc} & & \text{id}_A & & \\ & & \downarrow & & \\ C & \xrightarrow{g} & A & \xrightarrow{f} & B \end{array}$$

Observación 6.2.2. La existencia de las funciones dom y codom permite probar que si $A, B, C, D \in \text{ob } \mathcal{C}$ son objetos distintos, entonces $\text{Hom}(A, B) \cap \text{Hom}(C, D) = \emptyset$, pues en efecto, si f fuese un morfismo en $\text{Hom}(A, B) \cap \text{Hom}(C, D)$, tendríamos $\text{dom } f = A = C$ y $\text{codom } f = B = D$. En muchos textos esta condición aparece en la definición de una categoría.

Definición 6.2.3. Una categoría \mathcal{C} se dice una **categoría pequeña** si $\text{ob } \mathcal{C}$ y $\text{mor } \mathcal{C}$ son conjuntos. Si no es pequeña la categoría se dice **grande**. \mathcal{C} se dice **localmente pequeña** si para cada $A, B \in \text{ob } \mathcal{C}$, $\text{Hom}(A, B)$ es un conjunto. En ese caso, $\text{Hom}(A, B)$ se denomina un **hom-set**.

Ejemplo 6.2.4. La categoría Set. Definiremos la categoría $\mathcal{C} = \text{Set}$ donde:

- ob Set es la clase de todos los conjuntos;
- mor Set es la clase de todas las funciones entre conjuntos. En particular, $\text{Hom}(A, B)$ es el conjunto de funciones de A en B .
- dom y codom son las funciones de clase que a cada función entre conjuntos le asigna el dominio y el codominio de cada función, respectivamente.
- La composición en Set es la composición usual de funciones, y para cada conjunto A , id_A es la función identidad $\text{Id} : A \rightarrow A$.

Es inmediato verificar que Set así definido es una categoría, denominada la **categoría de conjuntos**.

Un morfismo de particular interés, que normalmente suele ignorarse cuando trabajamos con funciones, es la denominada **función vacía**. En realidad, existe una (única) función vacía $\emptyset_A : \emptyset \rightarrow A$ para cada conjunto A , que no es más que la relación funcional trivial $\emptyset \subset \emptyset \times A$. Esto implica que $\text{Hom}(\emptyset, A)$ consta de un único morfismo.

Por otra parte, para cada conjunto $\{x\}$ de un único elemento, $\text{Hom}(A, \{x\})$ también consta de un único morfismo, dado que es posible definir una única función (la función constante $f(a) = x$ para cada $a \in A$) de A en $\{x\}$. ■

Ejemplo 6.2.5. De manera similar a la categoría Set podemos construir categorías cuyos objetos sean las distintas estructuras que estudiamos hasta el momento. Las enunciamos en la siguiente tabla y haremos referencia frecuentemente a ellas. En todos los casos, los morfismos son funciones en el sentido usual, las funciones dominio y codominio son el dominio y codominio de la respectiva función, la función composición es la composición usual de funciones, y el morfismo identidad será la función identidad usual. Dejamos como ejercicio verificar que se cumple la Definición 6.2.1:

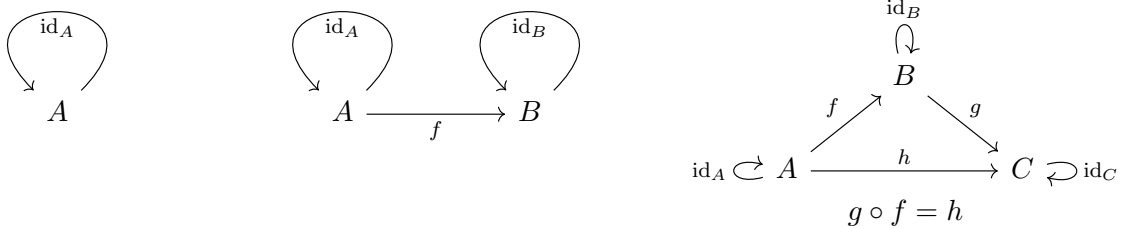
\mathcal{C}	$\text{ob } \mathcal{C}$	$\text{mor } \mathcal{C}$
Set	conjuntos	funciones
FinSet	conjuntos finitos	funciones
Poset	posets	morfismos de posets
Ret	retículos	morfismos de retículos
Sgrp	semigrupos	morfismos de semigrupos
Mon	monoides	morfismos de monoides
Grp	grupos	homomorfismos de grupos
Ab	grupos abelianos	homomorfismos de grupos abelianos
Vect	espacios vectoriales reales	transformaciones lineales

Claramente podríamos seguir definiendo categorías para cada estructura para la cual haya definido algún tipo de morfismos, como la categoría de las álgebras de Boole, de los grupos cíclicos, etc. Se trata en todos los casos de categorías grandes, localmente pequeñas, dado que $\text{ob } \mathcal{C}$ es siempre una clase propia, y $\text{Hom}(A, B) \subset A \times B$ es siempre un conjunto. ■

Ejemplo 6.2.6. Por conveniencia, denotaremos por **0** a la categoría sin objetos ni morfismos. Claramente las propiedades de la función composición y la existencia de identidad se satisfacen por vacuidad, ya que no hay objetos ni morfismos a las cuales aplicarlas.

1 es una categoría donde $\text{ob } \mathbf{1}$ está formado por un único objeto A y $\text{mor } \mathbf{1}$ por un único morfismo, que debe ser necesariamente id_A .

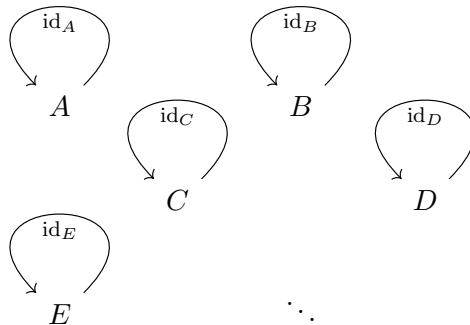
La categoría **2** se define de modo que $\text{ob } \mathbf{2} = \{A, B\}$, $\text{mor } \mathbf{2} = \{\text{id}_A, \text{id}_B, f : A \rightarrow B\}$, y análogamente la categoría **3** es tal que $\text{ob } \mathbf{3} = \{A, B, C\}$, $\text{mor } \mathbf{3} = \{\text{id}_A, \text{id}_B, \text{id}_C, f : A \rightarrow B, g : B \rightarrow C, h : A \rightarrow C\}$. En todos los casos la composición es tal que id es el morfismo identidad, y en el caso de **3** además se verifica $h = g \circ f$. Estas categorías suelen representarse a través de los siguientes diagramas:



Observemos que para definir estas categorías no hemos precisado quienes son A , B o C ni los morfismos que intervienen. Esto por el momento es irrelevante dado que estas categorías están definidas en modo abstracto. **1**, **2**, **3** son ejemplos de categorías pequeñas.

En los Ejemplos 6.2.5 consideramos categorías dadas por diferentes estructuras. Veremos ahora que una estructura algebraica considerada individualmente también puede definir una categoría.

Ejemplo 6.2.7. Categoría discreta. Dado un conjunto X cualquiera podemos definir una categoría \mathcal{C} tal que $\text{ob } \mathcal{C} = X$ y $\text{mor } \mathcal{C} = \{\text{id}_A : A \in X\}$. La composición se define de modo tal que $\text{id}_A \circ \text{id}_A = \text{id}_A$, con lo cual es inmediato que se verifica la Definición 6.2.1. \mathcal{C} se denomina categoría discreta, y puede representarse mediante el siguiente diagrama:



Ejemplo 6.2.8. Un poset es una categoría. Sea (P, \preceq) un conjunto parcialmente ordenado. Consideremos la categoría \mathcal{C}_P de modo que $\text{ob } \mathcal{C}_P = P$, $\text{mor } \mathcal{C}_P = \{(p, p') : p \preceq p'\}$. Las funciones dominio y codominio están dadas por $\text{dom}(p, p') = p$ y $\text{codom}(p, p') = p'$. La composición está dada por $(p', p'') \circ (p, p') = (p, p'')$ que está bien definida por la transitividad de \preceq , y la identidad es $\text{id}_p = (p, p) \in \text{mor } \mathcal{C}_P$ pues \preceq es reflexiva. La asociatividad de \circ es trivial. En este caso $\text{Hom}(p, p')$ es vacío si $p \not\preceq p'$ y consta del único elemento (p, p') si $p \preceq p'$.

Observemos que no hemos usado en ningún momento la antisimetría de \preceq . En efecto, cualquier conjunto preordenado da lugar a una categoría de este tipo. ■

Ejemplo 6.2.9. Un monoide es una categoría. Sea $(M, *)$ un monoide. Podemos definir una categoría \mathcal{C}_M donde $\text{ob } \mathcal{C}_M = \{\star\}$, un único objeto abstracto, $\text{mor } \mathcal{C}_M = M$. Es claro en este caso que las funciones dom y codom asignan el único elemento \star a cualquier morfismo. La composición se define como $\circ = *$. Es fácil verificar que se cumplen las propiedades que definen una categoría, y en este caso el morfismo id_\star es la identidad del monoide.

Dejamos como ejercicio verificar que si \mathcal{C} es una categoría con un único objeto, entonces $(\text{mor } \mathcal{C}, \circ)$ es un monoide. ■

Las categorías de los ejemplos 6.2.7, 6.2.8 y 6.2.9 son categorías pequeñas.

Ejemplo 6.2.10. Categoría dual. Sea \mathcal{C} una categoría. Se denomina **categoría dual** o **categoría opuesta** de \mathcal{C} , a la categoría \mathcal{C}^{op} tal que:

- $\text{ob } \mathcal{C}^{op} = \text{ob } \mathcal{C}$,
- $\text{mor } \mathcal{C}^{op}$ es tal que $f \in \text{Hom}^{op}(A, B)$ si $f \in \text{Hom}(B, A)$.
- $\text{dom}^{op} = \text{codom}$ y $\text{codom}^{op} = \text{dom}$.
- \circ^{op} es tal que si $f \in \text{Hom}^{op}(A, B)$ y $g \in \text{Hom}^{op}(B, C)$, entonces $g \circ^{op} f = f \circ g$.
- $\text{id}_A^{op} = \text{id}_A$.

Es fácil verificar (y lo dejamos como ejercicio) que \mathcal{C}^{op} es efectivamente una categoría, probaremos sólo a modo de ejemplo la asociatividad de \circ^{op} : Sean $f \in \text{Hom}^{op}(A, B)$, $g \in \text{Hom}^{op}(B, C)$ y $h \in \text{Hom}^{op}(C, D)$. Entonces $f \in \text{Hom}(B, A)$, $g \in \text{Hom}(C, B)$ y $h \in \text{Hom}(D, C)$. Luego:

$$\begin{aligned} (h \circ^{op} g) \circ^{op} f &= (g \circ h) \circ^{op} f = f \circ (g \circ h) = (f \circ g) \circ h \\ &= h \circ^{op} (f \circ g) = h \circ^{op} (g \circ^{op} f). \end{aligned}$$

Observemos que \mathcal{C}^{op} es una categoría pequeña (resp. grande) si y sólo si \mathcal{C} es pequeña (resp. grande), y \mathcal{C}^{op} es localmente pequeña si y sólo si \mathcal{C} es localmente pequeña. ■

Observación 6.2.11. En la categoría dual de una categoría \mathcal{C} muchas veces dejan de tener sentido las nociones de morfismo y composición que tienen en la categoría \mathcal{C} . Por ejemplo, en el Ejemplo 6.2.5 vimos una serie de categorías donde los morfismos son efectivamente funciones entre conjuntos y la composición es la composición usual de funciones. En el caso de las categorías duales de estas categorías los morfismos ya

no son necesariamente funciones entre el conjunto A y el conjunto B (sí lo serán entre B y A), y no debemos confundir un morfismo en $\text{Hom}^{op}(A, B)$ con la función inversa de $f \in \text{Hom}(B, A)$ (que posiblemente no existe). En este caso es más pertinente la denominación de **flechas** en vez de morfismos, y podemos pensar que la categoría dual de \mathcal{C} simplemente se obtiene invirtiendo las flechas de \mathcal{C} y acomodando las demás definiciones para que todo tenga sentido. Sintéticamente estas propiedades pueden resumirse en el siguiente diagrama:

$$\begin{array}{ccc}
 \text{En } \mathcal{C} & & \text{En } \mathcal{C}^{op} \\
 \begin{array}{c} A \\ \downarrow f \\ B \\ \downarrow g \\ C \end{array} & \xrightarrow{g \circ f} & \begin{array}{c} A \\ \uparrow f \\ B \\ \uparrow g \\ C \end{array} \\
 & & f \circ^{op} g := g \circ f
 \end{array}$$

Ejemplo 6.2.12. Consideremos la categoría \mathcal{C}_P asociada a un poset P (ver Ejemplo 6.2.8). ¿Cuál es su categoría opuesta? Tendremos que $\text{ob } \mathcal{C}_P^{op} = \text{ob } \mathcal{C}_P = P$. Por otra parte, si $x, y \in P$, un morfismo $f \in \text{Hom}^{op}(x, y)$ es un morfismo en $\text{Hom}(y, x)$, el cual existe si y sólo si $y \preceq x$. Esto es, un morfismo $f \in \text{Hom}^{op}(x, y)$ es un par $f = (y, x)$ tal que $y \preceq x$.

Si ahora consideramos el poset dual de P , es decir P^* donde $x \preceq^* y$ si $y \preceq x$, entonces $\text{ob } \mathcal{C}_{P^*} = P$ y $f = (x, y) \in \text{Hom}_{\mathcal{C}_{P^*}}(x, y)$ si y sólo si $y \preceq x$, lo que ocurre si y sólo si $(y, x) \in \text{Hom}_{\mathcal{C}_P}(y, x) = \text{Hom}^{op}(x, y)$. Analizaremos más adelante la relación entre \mathcal{C}_{P^*} y \mathcal{C}_P^{op} , pero adelantamos que son “esencialmente” la misma categoría. ■

Ejemplo 6.2.13. Categoría producto. Sean \mathcal{C}_1 y \mathcal{C}_2 dos categorías. Se denomina **categoría producto** a una categoría \mathcal{C} , que se denota $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2$, tal que

- $\text{ob } \mathcal{C} = \{(A, B) : A \in \text{ob } \mathcal{C}_1, B \in \text{ob } \mathcal{C}_2\}$.
- $\text{mor } \mathcal{C} = \{(f, g), : f \in \text{mor } \mathcal{C}_1, g \in \text{mor } \mathcal{C}_2\}$ y las funciones dominio y codominio están dadas por $\text{dom}(f, g) = (\text{dom } f, \text{dom } g)$ y $\text{codom}(f, g) = (\text{codom } f, \text{codom } g)$. De esta manera, si $(A, B), (A', B') \in \text{ob } \mathcal{C}$,

$$\text{Hom}((A, B), (A', B')) = \{(f, g) : (A, B) \rightarrow (A', B') : f \in \text{Hom}(A, A'), g \in \text{Hom}(B, B')\}.$$

- la composición es componente a componente, esto es $(f', g') \circ (f, g) = (f' \circ f, g' \circ g)$. Es fácil ver a partir de la asociatividad de la composición en \mathcal{C}_1 y \mathcal{C}_2 que la composición en \mathcal{C} es asociativa.
- $\text{id}_{(A, B)} = (\text{id}_A, \text{id}_B)$. En efecto, si $(f, g) \in \text{Hom}((A, B), (A', B'))$, se verifica

$$(f, g) \circ \text{id}_{(A, B)} = (f, g) \circ (\text{id}_A, \text{id}_B) = (f \circ \text{id}_A, g \circ \text{id}_B) = (f, g)$$

La otra composición es análoga. ■

En la definición 6.2.1 y en mucho de los ejemplos anteriores hemos recurrido a algunos diagramas para ilustrar la composición entre flechas. Si bien como hemos visto los morfismos o flechas en una categoría no necesariamente son funciones entre conjuntos es siempre útil la utilización de diagramas para representar objetos y flechas.

Definición 6.2.14. Un **diagrama** en una categoría \mathcal{C} es un grafo dirigido etiquetado consistentemente, donde los vértices se etiquetan con objetos de \mathcal{C} , las aristas dirigidas con flechas de \mathcal{C} de modo que si una arista está etiquetada con una flecha f cuyo dominio es A y codominio es B , el nodo inicial y final de esta arista se etiquetan con A y B respectivamente.

Un diagrama en \mathcal{C} se dice **conmutativo** o se dice que **conmuta** si para cualquier par de vértices X e Y del diagrama, todos los caminos del diagrama entre X e Y son equivalentes, en el sentido que determinan una arista dirigida entre X e Y que representa una misma flecha en \mathcal{C} .

Por ejemplo, el siguiente diagrama conmuta, si hay una flecha $h : X \rightarrow Y$ que es a la vez $g \circ f'$ y $f \circ g'$. Es decir, el diagrama es conmutativo si $g' \circ f = f' \circ g$.

$$\begin{array}{ccc} X & \xrightarrow{f} & Z \\ g \downarrow & & \downarrow g' \\ W & \xrightarrow{f'} & Y \end{array}$$

La utilización de diagramas conmutativos para enunciar y demostrar propiedades puede ser muy útil tanto porque ayuda a comprender visualmente las propiedades de una categoría, como porque además permite concluir propiedades que analíticamente pueden ser engorrosas de describir. Probaremos a continuación una propiedad que ilustra la comodidad de trabajar con diagramas conmutativos:

Lema 6.2.15. Si en el siguiente diagrama ambos cuadrados interiores son conmutativos, entonces todo el diagrama es conmutativo:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{f'} & C \\ a \downarrow & & b \downarrow & & \downarrow c \\ A' & \xrightarrow{g} & B' & \xrightarrow{g'} & C' \end{array}$$

Demostración. Por hipótesis tenemos que $g \circ a = b \circ f$ y que $g' \circ b = c \circ f'$. Luego el diagrama conmuta si todos los caminos entre A y C' conmutan. Por un lado,

$$\begin{aligned} (g' \circ g) \circ a &= g' \circ (g \circ a) = g' \circ (b \circ f) = (g' \circ b) \circ f \\ &= (c \circ f') \circ f = c \circ (f' \circ f). \end{aligned}$$

Por otra parte,

$$(g' \circ b) \circ f = (c \circ f') \circ f = (g' \circ g) \circ a.$$

con lo cual el diagrama es conmutativo. \square

Ejemplo 6.2.16. Categoría de flechas. Sea \mathcal{C} una categoría, se denomina **categoría de flechas** de \mathcal{C} a la categoría $\mathcal{C}^{\rightarrow}$ tal que:

- $\text{ob } \mathcal{C}^{\rightarrow} = \text{mor } \mathcal{C}$.
- $\text{mor } \mathcal{C}^{\rightarrow}$ es tal que si $f, f' \in \text{ob } \mathcal{C}^{\rightarrow}$ con $f \in \text{Hom}(A, B)$, $f' \in \text{Hom}(A', B')$, un morfismo en $\mathcal{C}^{\rightarrow}$ es un cuadrado conmutativo

$$(6.1) \quad \begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \end{array}$$

donde $a \in \text{Hom}(A, A')$, $b \in \text{Hom}(B, B')$ y en \mathcal{C} se verifica $b \circ f = f' \circ a$. Para simplificar las definiciones, suele identificarse un morfismo en $\mathcal{C}^{\rightarrow}$ con el par (a, b) de morfismos en \mathcal{C} . Debemos observar sin embargo que el cuadrado 6.1 puede resultar conmutativo para los mismos morfismos (a, b) pero para distintos morfismos f y f' . Por ejemplo, si definimos los morfismos de $\mathcal{C}^{\rightarrow}$ sólo como pares de morfismos en \mathcal{C} que hacen que 6.1 sea conmutativo, el par $(\text{id}_A, \text{id}_A)$ sería un morfismo en $\mathcal{C}^{\rightarrow}$ que pertenece a $\text{Hom}(f, f)$ cualquiera sea $f \in \text{Hom}(A, A)$, lo que haría que las funciones dom y codom no estén bien definidas en $\mathcal{C}^{\rightarrow}$. Para solucionar este problema es que los morfismos en $\mathcal{C}^{\rightarrow}$ se consideran como todo el cuadrado conmutativo. Se denotan como el par (a, b) pero sobreentendiendo que (a, b) representa un cuadrado conmutativo en $\text{Hom}(f, f')$.

- la composición en $\mathcal{C}^{\rightarrow}$ está dada de la siguiente manera: si $(a, b) \in \text{Hom}(f, f')$ y $(a', b') \in \text{Hom}(f', f'')$ entonces $(a', b') \circ (a, b) = (a' \circ a, b' \circ b)$. Si queremos pensarlo como composición de diagramas, tenemos:

$$(6.2) \quad \begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \end{array} \circ \begin{array}{ccc} A' & \xrightarrow{f'} & B' \\ a' \downarrow & & \downarrow b' \\ A'' & \xrightarrow{f''} & B'' \end{array} = \begin{array}{ccc} A & \xrightarrow{f} & B \\ a' \circ a \downarrow & & \downarrow b' \circ b \\ A'' & \xrightarrow{f''} & B'' \end{array}$$

Observemos que la composición está bien definida. En efecto, en el siguiente diagrama los cuadrados interiores son conmutativos

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \\ a' \downarrow & & \downarrow b' \\ A'' & \xrightarrow{f''} & B'' \end{array}$$

Luego del Lema 6.2.15 resulta que el diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & & B' \\ a' \downarrow & & \downarrow b' \\ A'' & \xrightarrow{f''} & B'' \end{array}$$

también es conmutativo. Esto es, $(b' \circ b) \circ f = f'' \circ (a' \circ a)$. Por lo tanto el diagrama de la derecha en 6.2 es conmutativo, con lo cual $(a' \circ a, b' \circ b) \in \text{Hom}(f, f'')$. Veamos que la composición es asociativa. Sean $(a, b) \in \text{Hom}(f, f')$, $(a', b') \in \text{Hom}(f', f'')$, $(a'', b'') \in \text{Hom}(f'', g'')$. Entonces:

$$\left(\begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \end{array} \circ \begin{array}{ccc} A' & \xrightarrow{f'} & B' \\ a' \downarrow & & \downarrow b' \\ A'' & \xrightarrow{f''} & B'' \end{array} \right) \circ \begin{array}{ccc} A'' & \xrightarrow{f''} & B'' \\ a'' \downarrow & & \downarrow b'' \\ A''' & \xrightarrow{f'''} & B''' \end{array} = \begin{array}{ccc} A & \xrightarrow{f} & B \\ a' \circ a \downarrow & & \downarrow b' \circ b \\ A'' & \xrightarrow{f''} & B'' \end{array} \circ \begin{array}{ccc} A'' & \xrightarrow{f''} & B'' \\ a'' \downarrow & & \downarrow b'' \\ A''' & \xrightarrow{f'''} & B''' \end{array} \\ = \begin{array}{ccc} A & \xrightarrow{f} & B \\ a'' \circ (a' \circ a) \downarrow & & \downarrow b'' \circ (b' \circ b) \\ A''' & \xrightarrow{f'''} & B''' \end{array}$$

y se manera análoga

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \end{array} \circ \left(\begin{array}{ccc} A' & \xrightarrow{f'} & B' \\ a' \downarrow & & \downarrow b' \\ A'' & \xrightarrow{f''} & B'' \end{array} \circ \begin{array}{ccc} A'' & \xrightarrow{f''} & B'' \\ a'' \downarrow & & \downarrow b'' \\ A''' & \xrightarrow{f'''} & B''' \end{array} \right) = \begin{array}{ccc} A & \xrightarrow{f} & B \\ a \downarrow & & \downarrow b \\ A' & \xrightarrow{f'} & B' \end{array} \circ \begin{array}{ccc} A' & \xrightarrow{f'} & B' \\ a' \circ a' \downarrow & & \downarrow b' \circ b' \\ A'' & \xrightarrow{f''} & B'' \end{array} \\ = \begin{array}{ccc} A & \xrightarrow{f} & B \\ (a'' \circ a') \circ a \downarrow & & \downarrow (b'' \circ b') \circ b \\ A''' & \xrightarrow{f'''} & B''' \end{array}$$

De la asociatividad en \mathcal{C} , resultan $(a'' \circ a') \circ a = a'' \circ (a' \circ a)$ y $(b'' \circ b') \circ b = b'' \circ (b' \circ b)$. Concluimos que la composición en $\mathcal{C}^{\rightarrow}$ es conmutativa.

- Finalmente, si $f : A \rightarrow B \in \text{ob } \mathcal{C}^{\rightarrow}$, entonces $\text{id}_f = (\text{id}_A, \text{id}_B)$. ■

Definición 6.2.17. Sea \mathcal{C} una categoría. Una **subcategoría** \mathcal{C}' de \mathcal{C} es una categoría \mathcal{C}' tal que:

- Todos los objetos de \mathcal{C}' son objetos de \mathcal{C} (abusando de la notación, $\text{ob } \mathcal{C}' \subseteq \text{ob } \mathcal{C}$).
- Todos los morfismos de \mathcal{C}' son morfismos de \mathcal{C} (o sea, $\text{mor } \mathcal{C}' \subseteq \text{mor } \mathcal{C}$).
- las funciones dominio, codominio así como la composición de morfismos y los morfismos identidad en \mathcal{C}' son los mismos que en \mathcal{C} .

Si \mathcal{C}' es una subcategoría de \mathcal{C} , lo denotamos $\mathcal{C}' \subseteq \mathcal{C}$. Un subcategoría \mathcal{C}' de \mathcal{C} se dice **full** si para cada $A, B \in \mathcal{C}'$, $\text{Hom}_{\mathcal{C}'}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$.

Ejemplo 6.2.18. La categoría FinSet es una subcategoría full de la categoría Set . La categoría Ret es una subcategoría de la categoría Poset , que no es full, pues existen morfismos de posets entre retículos que no son morfismos de retículos (ver Ejemplo 3.4.1). Entre las estructuras algebraicas tenemos $\text{Ab} \subseteq \text{Grp} \subseteq \text{Mon} \subseteq \text{Sgrp}$ (¿qué subcategorías son full?). Observemos que estas categorías no son subcategorías de Set . Por ejemplo, los objetos de Mon son monoides, y no estamos pensando sólo en el conjunto subyacente, sino en la operación que lo acompaña (y hace de ellos un monoide). Así, $(\mathbb{Z}, +)$ y (\mathbb{Z}, \cdot) son objetos distintos en Mon , pero como conjuntos representan el mismo objeto en Set . Para estudiar mejor estas relaciones entre categorías introduciremos el concepto de *functor*. ■

6.3. Funtores

Como en toda estructura algebraica existen morfismos que relacionan unas con otras, necesitamos definir una forma de relacionar dos categorías diferentes y establecer un concepto de *categorías equivalentes*. En todas las estructuras algebraicas que hemos estudiado el concepto de equivalencia está asociado con la existencia de isomorfismos, esto es, funciones biyectivas que asignan los elementos de una estructura en otra y preservan todas las características constitutivas de la estructura en cuestión. Como las categorías están definidas a partir de dos clases fundamentales, $\text{ob } \mathcal{C}$ y $\text{mor } \mathcal{C}$, necesitamos definir una forma de “mapear” objetos y morfismos de una categoría en otra:

Definición 6.3.1. Sean \mathcal{C} y \mathcal{D} categorías. Un **funtor covariante** o simplemente un **funtor** de \mathcal{C} en \mathcal{D} es un par de funciones de clase, ambas denotadas por F ,

$$F : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{D}, \quad F : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{D}$$

tales que:

1. para cada $f \in \text{Hom}_{\mathcal{C}}(A, B)$, $F(f) \in \text{Hom}_{\mathcal{D}}(F(A), F(B))$:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & & \text{en } \mathcal{C} \\ F : & \downarrow & \downarrow & \downarrow & \\ & F(A) & \xrightarrow{F(f)} & F(B) & \text{en } \mathcal{D} \end{array}$$

2. Para cada objeto A de \mathcal{C} , $F(\text{id}_A) = \text{id}_{F(A)}$
3. Para cualesquiera objetos A, B, C de \mathcal{C} y morfismos $f \in \text{Hom}(A, B)$, $g \in \text{Hom}(B, C)$,

$$F(g \circ f) = F(g) \circ F(f).$$

$$\begin{array}{ccc} A \xrightarrow{f} B \xrightarrow{g} C & & F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \\ \searrow \text{ } g \circ f \nearrow & & \searrow \text{ } F(g \circ f) = F(g) \circ F(f) \nearrow \end{array}$$

Si F es un funtor covariante de \mathcal{C} en \mathcal{D} , lo denotamos $F : \mathcal{C} \rightarrow \mathcal{D}$.

Ejemplo 6.3.2. El funtor identidad. Sea \mathcal{C} una categoría. Pongamos $\text{Id} : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{C}$ tal que $\text{Id}(A) = A$ e $\text{Id} : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{C}$ tal que $\text{Id}(f) = f$. Es inmediato verificar que Id es un funtor covariante, denominado funtor identidad. Cuando necesitemos especificar la categoría, lo denotamos $\text{Id}_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$. ■

Ejemplo 6.3.3. El funtor inclusión. Sea \mathcal{C} una categoría y \mathcal{C}' una subcategoría de \mathcal{C} . Entonces $\text{inc} : \mathcal{C}' \rightarrow \mathcal{C}$ tal que $\text{inc}(A) = A$ para cada $A \in \text{ob } \mathcal{C}'$ y $\text{inc}(f) = f$ para cada $f \in \text{mor } \mathcal{C}'$ es trivialmente un funtor, denominado el funtor inclusión de \mathcal{C}' en \mathcal{C} . ■

Ejemplo 6.3.4. El functor olvido. Sea \mathcal{C} una categoría donde los objetos son conjuntos (con alguna estructura adicional), los morfismos son funciones, la composición es la composición usual de funciones y el morfismo identidad es la función identidad (por ejemplo Sgrp , Mon , Grp , Ab , Vect , Ret , etc.). Podemos definir un functor $\text{fgt} : \mathcal{C} \rightarrow \text{Set}$ de modo que si A es un objeto de \mathcal{C} , $\text{fgt}(A) = A$ y si f es un morfismo de \mathcal{C} , $\text{fgt}(f) = f$, es decir, fgt devuelve a cada objeto de \mathcal{C} el conjunto subyacente y a cada morfismo de \mathcal{C} el mismo morfismo visto como función. Es claro que fgt es un functor covariante (dejamos los detalles como ejercicio). Por ejemplo en Mon , podemos considerar los moniodes $(\mathbb{Z}, +)$ y (\mathbb{Z}, \cdot) , y tendremos que $\text{fgt}(\mathbb{Z}, +) = \text{fgt}(\mathbb{Z}, \cdot) = \mathbb{Z}$. ■

Ejemplo 6.3.5. El functor hom_A . Sea \mathcal{C} una categoría localmente pequeña (por ejemplo Set , Grp , Sgrp , Poset , etc.) y sea A un objeto fijo en \mathcal{C} . Definamos $\text{hom}_A : \text{ob } \mathcal{C} \rightarrow \text{ob Set}$ por

$$\text{hom}_A(B) = \text{Hom}_{\mathcal{C}}(A, B).$$

Para ver que hom_A define un functor de \mathcal{C} en Set , debemos definir una función de clase de mor \mathcal{C} en mor Set . Consideremos un morfismo f en mor \mathcal{C} y supongamos que $f \in \text{Hom}_{\mathcal{C}}(B, C)$. Como $\text{hom}_A(B) = \text{Hom}_{\mathcal{C}}(A, B)$ y $\text{hom}_A(C) = \text{Hom}_{\mathcal{C}}(A, C)$, debemos definir una función (un morfismo en Set)

$$(6.3) \quad \text{hom}_A(f) : \text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, C)$$

Para ello basta observar que si $h \in \text{Hom}_{\mathcal{C}}(A, B)$, entonces $h \circ f \in \text{Hom}_{\mathcal{C}}(A, C)$. Por lo tanto, poniendo

$$\text{hom}_A(f)(h) = f \circ h$$

queda bien definida la función (6.3):

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(A, B) & \xrightarrow{\text{hom}_A(f)} & \text{Hom}_{\mathcal{C}}(A, C) \\ h & \longmapsto & f \circ h \end{array} \qquad \begin{array}{ccc} B & \xrightarrow{f} & C \\ \swarrow h & & \nearrow f \circ h \\ & A & \end{array}$$

lo que a su vez permite definir la función de clases

$$\text{hom}_A : \text{mor } \mathcal{C} \rightarrow \text{mor Set}, \quad f \mapsto \text{hom}_A(f)$$

que por construcción verifica la condición 1 de la Definición 6.3.1.

Veamos que se verifican las condiciones 2 y 3. Para ver que se verifica 2, consideremos un objeto B cualquiera en \mathcal{C} . Entonces $\text{hom}_A(\text{id}_B) : \text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, B)$ está dado por

$$\text{hom}_A(\text{id}_B)(h) = \text{id}_B \circ h = h = \text{id}_{\text{Hom}_{\mathcal{C}}(A, B)}(h)$$

donde la última es la identidad en Set . Luego $\text{hom}_A(\text{id}_B) = \text{id}_{\text{hom}_A(B)}$.

Veamos ahora que se verifica la condición 3. Sean $f \in \text{Hom}_{\mathcal{C}}(B, C)$ y $g \in \text{Hom}_{\mathcal{C}}(C, D)$. Tendremos entonces:

$$\begin{array}{ccccc} \text{Hom}_{\mathcal{C}}(A, B) & \xrightarrow{\text{hom}_A(f)} & \text{Hom}_{\mathcal{C}}(A, C) & \xrightarrow{\text{hom}_A(g)} & \text{Hom}_{\mathcal{C}}(A, D) \\ h \mapsto & & f \circ h \mapsto & & g \circ (f \circ h) \end{array}$$

$$\begin{array}{ccccc} B & \xrightarrow{f} & C & \xrightarrow{g} & D \\ & \nwarrow h & \uparrow f \circ h & \nearrow g \circ (f \circ h) & \\ & & A & & \end{array}$$

que si $h \in \text{Hom}_{\mathcal{C}}(A, B)$,

$$\text{hom}_A(g) \circ \text{hom}_A(f)(h) = \text{hom}_A(g)(f \circ h) = g \circ (f \circ h) = (g \circ f) \circ h = \text{hom}_A(g \circ f)(h).$$

Muchas veces el funtor hom_A se denota como $\text{Hom}(A, -)$, donde la barra $-$ debe reemplazarse con los objetos de \mathcal{C} , esto es, esta notación sólo indica cómo actúa el funtor en $\text{ob } \mathcal{C}$. De esta manera $\text{Hom}(A, f)$ para un morfismo f simplemente denota la función $\text{hom}_A(f)$. ■

Ejemplo 6.3.6. Homomorfismos como funtores. Hemos visto en los ejemplos 6.2.8 y 6.2.9 que un poset o un monoide pueden pensarse como categorías. Veremos ahora que los funtores entre dos categorías de alguno de estos tipos no son más que los morfismos de las respectivas estructuras.

1. Sean P, Q posets, \mathcal{C}_P y \mathcal{C}_Q las categorías asociadas y sea $F : P \rightarrow Q$ un morfismo de orden, esto es

$$x \preceq_P y \implies F(x) \preceq_Q F(y)$$

Entonces F define una función de $\text{ob } \mathcal{C}_P$ en $\text{ob } \mathcal{C}_Q$. Pero observemos que si $(x, y) \in \text{mor } \mathcal{C}_P$, es decir si $x \preceq_P y$, entonces $(F(x), F(y)) \in \text{mor } \mathcal{C}_Q$. Por lo tanto $F(x, y) = (F(x), F(y))$ es una función entre $\text{mor } \mathcal{C}_P$ y $\text{mor } \mathcal{C}_Q$.

Es inmediato verificar que F cumple las tres condiciones de la definición 6.3.1 y por lo tanto es un funtor de \mathcal{C}_P en \mathcal{C}_Q . Veremos en el Ejercicio 11 de este capítulo que si $G : \mathcal{C}_P \rightarrow \mathcal{C}_Q$ es un funtor, si nos quedamos con la función $G : \text{ob } \mathcal{C}_P \rightarrow \text{ob } \mathcal{C}_Q$, G es un morfismo de orden de P en Q .

2. Sean $(M, *_M)$ y $(M', *_M')$ monoides con identidades e_M y $e_{M'}$ respectivamente y sea $f : M \rightarrow M'$ un homomorfismo de monoides. Sean \mathcal{C}_M y $\mathcal{C}_{M'}$ las categorías asociadas, con $\text{ob } \mathcal{C}_M = \{\star\}$, $\text{mor } \mathcal{C}_M = M$, $\text{ob } \mathcal{C}_{M'} = \{\clubsuit\}$ y $\text{mor } \mathcal{C}_{M'} = M'$. Definamos $F : \text{ob } \mathcal{C}_M \rightarrow \text{ob } \mathcal{C}_{M'}$ poniendo $F(\star) = \clubsuit$ y $F : \text{mor } \mathcal{C}_M \rightarrow \text{mor } \mathcal{C}_{M'}$ poniendo $F(m) = f(m)$. Entonces $F(\text{id}_{\star}) = f(e_M) = e_{M'} = \text{id}_{\clubsuit}$ y $F(m \circ n) = f(m *_M n) = f(m) *_M' f(n) = F(m) \circ F(n)$ con lo cual se satisfacen todas las condiciones de la Definición 6.3.1 y $F : \mathcal{C}_M \rightarrow \mathcal{C}_{M'}$ es un funtor. Veremos en el Ejercicio 11 que recíprocamente, todo funtor $F : \mathcal{C}_M \rightarrow \mathcal{C}_{M'}$ define un morfismo de monoides. ■

Teorema 6.3.7 (Composición de funtores.). *Sean $F : \mathcal{C}_1 \rightarrow \mathcal{C}_2$ y $G : \mathcal{C}_2 \rightarrow \mathcal{C}_3$ dos funtores covariantes. Definamos $G \circ F : \text{ob } \mathcal{C}_1 \rightarrow \text{ob } \mathcal{C}_3$ como $G \circ F(A) = G(F(A))$ y $G \circ F : \text{mor } \mathcal{C}_1 \rightarrow \text{mor } \mathcal{C}_3$ por $G \circ F(f) = G(F(f))$. Entonces:*

1. $G \circ F$ es un funtor.
2. Si $H : \mathcal{C}_3 \rightarrow \mathcal{C}_4$ es un funtor, entonces $H \circ (G \circ F) = (H \circ G) \circ F$.
3. Si $\text{Id}_{\mathcal{C}_1}$ e $\text{Id}_{\mathcal{C}_2}$ son los funtores identidad en \mathcal{C}_1 y \mathcal{C}_2 , entonces $F \circ \text{Id}_{\mathcal{C}_1} = \text{Id}_{\mathcal{C}_2} \circ F = F$.

Demostración. Sea $f \in \text{Hom}_{\mathcal{C}_1}(A, B)$. Si $F(A) = A'$, $F(B) = B'$, $G(A') = A''$ y $G(B') = B''$, entonces si $f' = F(f)$, $f' \in \text{Hom}_{\mathcal{C}_2}(A', B')$ y $G(f') \in \text{Hom}_{\mathcal{C}_3}(A'', B'')$:

$$\begin{array}{ccccc}
 & A & \xrightarrow{f} & B & \\
 F : & \downarrow & & \downarrow & \downarrow \\
 & F(A) & \xrightarrow{F(f)} & F(B) & \\
 G : & \downarrow & & \downarrow & \downarrow \\
 & G(F(A)) & \xrightarrow{G(F(f))} & G(F(B)) &
 \end{array}$$

Por lo tanto

$$G \circ F(f) \in \text{Hom}_{\mathcal{C}_3}(G \circ F(A), G \circ F(B))$$

con lo cual se verifica la primera condición de la Definición 6.3.1.

Por otra parte, como F y G son funtores, tendremos $F(\text{id}_A) = \text{id}_{F(A)}$, $G(\text{id}_{F(A)}) = \text{id}_{G(F(A))}$ de donde $G \circ F(\text{id}_A) = \text{id}_{G \circ F(A)}$.

Finalmente, si $f \in \text{Hom}(A, B)$, $g \in \text{Hom}(C, D)$, tendremos que

$$G \circ F(g \circ f) = G(F(g) \circ F(f)) = G(F(g)) \circ G(F(f)) = (G \circ F)(g) \circ (G \circ F)(f).$$

Por lo tanto $G \circ F : \mathcal{C}_1 \rightarrow \mathcal{C}_3$ es un funtor, como queríamos probar.

Las últimas dos afirmaciones son inmediatas y las dejamos como **ejercicio**. □

Ejemplo 6.3.8. Categoría de categorías. Como la composición de funtores entre categorías es un funtor, la composición es asociativa y cada categoría tiene un funtor identidad, estamos tentados a considerar una nueva categoría Cat cuyos objetos sean todas las categorías y cuyos morfismos sean los funtores entre categorías.

Esta definición lleva, incluso en la teoría de clases, a contradicciones como la paradoja de Russell. Además recordemos que los objetos de una clase deben ser conjuntos.

Sin embargo, sí podemos considerar una categoría Cat cuyos objetos sean todas las categorías pequeñas y los morfismos son funtores entre categorías pequeñas. A partir del Teorema 6.3.7 es fácil verificar que Cat cumple con todas las condiciones que definen una categoría, y se trata de una categoría grande, con lo cual Cat no es un objeto de sí misma. ■

Ejemplo 6.3.9. Funtores y diagramas. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor entre dos categorías \mathcal{C} y \mathcal{D} . Consideremos los siguientes diagramas en \mathcal{C} :

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 & \searrow h & \swarrow g \\
 & C &
 \end{array}
 \qquad
 \begin{array}{ccc}
 A & \xrightarrow{j} & B \\
 l \downarrow & & \downarrow k \\
 C & \xrightarrow{m} & D
 \end{array}$$

Si ambos diagramas son conmutativos, es decir, si

$$g \circ f = h, \quad k \circ j = m \circ l$$

entonces, como F es un funtor,

$$F(g) \circ F(f) = F(g \circ f) = F(h), \quad F(k) \circ F(j) = F(k \circ j) = F(m \circ l) = F(m) \circ F(l)$$

es decir, en \mathcal{D} los siguientes diagramas también son conmutativos:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ & \searrow F(h) & \swarrow F(g) \\ & F(C) & \end{array} \qquad \begin{array}{ccc} F(A) & \xrightarrow{F(j)} & F(B) \\ F(l) \downarrow & & \downarrow F(k) \\ F(C) & \xrightarrow{F(m)} & F(D) \end{array}$$

■

Las mismas ideas del Ejemplo 6.3.9 pueden aplicarse a cualquier diagrama. Más específicamente, se tiene que:

Lema 6.3.10. *Si $F : \mathcal{C} \rightarrow \mathcal{D}$ es un funtor covariante, entonces F mapea diagramas conmutativos en \mathcal{C} en diagramas conmutativos en \mathcal{D} .*

La prueba del Lema 6.3.10 es intuitiva, pero engorrosa dado que deberíamos considerar cualquier diagrama conmutativo en una categoría. Lo aceptaremos sin demostrarlo, aunque es un buen **ejercicio** ensayar una prueba formal.

Veremos a continuación que el término *covariante* en la definición de un funtor, se opone al concepto de *contravariante*. Estos conceptos hacen referencia a la dirección de las flechas en la categoría de origen y de las imágenes de las flechas en la categoría de llegada.

Comenzaremos analizando un ejemplo:

Ejemplo 6.3.11. Funtores y dualidad. Supongamos ahora que $F : \mathcal{C} \rightarrow \mathcal{D}^{op}$ es un funtor de una categoría \mathcal{C} en la categoría opuesta (o dual) \mathcal{D}^{op} de una categoría \mathcal{D} . Observemos que $F : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{D}^{op}$ puede considerarse directamente como una función de clases $F : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{D}$, dado que $\text{ob } \mathcal{D}^{op} = \text{ob } \mathcal{D}$. Por otra parte, recordemos que $\text{Hom}_{\mathcal{D}^{op}}(A, B) = \text{Hom}_{\mathcal{D}}(B, A)$. Por lo tanto, $F : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{D}^{op}$ es una función de clase $F : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{D}$ tal que si $f \in \text{Hom}_{\mathcal{C}}(A, B)$, entonces

$$F(f) \in \text{Hom}_{\mathcal{D}^{op}}(F(A), F(B)) = \text{Hom}_{\mathcal{D}}(F(B), F(A)).$$

Finalmente, si $f \in \text{Hom}_{\mathcal{C}}(A, B)$ y $g \in \text{Hom}_{\mathcal{C}}(B, C)$, entonces

$$F(g \circ f) = F(g) \circ^{op} F(f) = F(f) \circ F(g).$$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \xrightarrow{g} C \\ & \searrow g \circ f & \swarrow \\ & & \end{array} \qquad \begin{array}{ccc} F(C) & \xrightarrow{F(g)} & F(B) \xrightarrow{F(f)} F(A) \\ & \searrow F(f \circ g) = F(f) \circ F(g) & \swarrow \\ & & \end{array}$$

Es decir que cualquier funtor de \mathcal{C} en \mathcal{D}^{op} puede describirse completamente en términos de \mathcal{C} y \mathcal{D} , con la salvedad que se invierten los ordenes de composición en la definición de un funtor covariante. Esto da lugar al concepto de *funtor contravariante*. ■

Definición 6.3.12. Sean \mathcal{C} y \mathcal{D} dos categorías. Un **funtor contrariante** de \mathcal{C} en \mathcal{D} , denotado $F : \mathcal{C} \rightarrow \mathcal{D}$ es un par de funciones de clase, ambas denotadas por F ,

$$F : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{D}, \quad F : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{D}$$

tales que:

1. para cada $f \in \text{Hom}_{\mathcal{C}}(A, B)$, $F(f) \in \text{Hom}_{\mathcal{D}}(F(B), F(A))$:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & & \text{en } \mathcal{C} \\ F : & \downarrow & \downarrow & & \downarrow \\ & F(A) & \xleftarrow{F(f)} & F(B) & \text{en } \mathcal{D} \end{array}$$

2. Para cada objeto A de \mathcal{C} , $F(\text{id}_A) = \text{id}_{F(A)}$
3. Para cualesquiera objetos A, B, C de \mathcal{C} y morfismo $f \in \text{Hom}(A, B)$, $g \in \text{Hom}(B, C)$,

$$F(g \circ f) = F(f) \circ F(g).$$

$$\begin{array}{ccc} A & \xrightarrow{f} B & \xrightarrow{g} C \\ & \searrow g \circ f & \nearrow \\ & & \end{array} \quad \begin{array}{ccccc} F(A) & \xleftarrow{F(f)} & F(B) & \xleftarrow{F(g)} & F(C) \\ & \searrow F(g \circ f) = F(f) \circ F(g) & \nearrow & & \end{array}$$

Ejemplo 6.3.13. El funtor contravariante Id^* . Sea \mathcal{C} una categoría y consideremos la categoría \mathcal{C}^{op} . Pongamos $\text{Id}^* : \mathcal{C} \rightarrow \mathcal{C}^{op}$ por $\text{Id}^*(A) = A$ para cada objeto A de \mathcal{C} y $\text{Id}^*(f) = f$ para cada morfismo f de \mathcal{C} . Si $f \in \text{Hom}_{\mathcal{C}}(A, B)$ entonces $f \in \text{Hom}_{\mathcal{C}^{op}}(B, A)$ con lo cual $\text{Id}^*(f) \in \text{Hom}_{\mathcal{C}^{op}}(\text{Id}^*(B), \text{Id}^*(A))$. Por otra parte,

$$\text{Id}^*(g \circ f) = g \circ f = f \circ^{op} g = \text{Id}^*(f) \circ^{op} \text{Id}^*(g)$$

y por lo tanto Id^* es un funtor contravariante.

Observemos que de manera completamente análoga podemos definir un funtor contravariante $\text{Id}^{**} : \mathcal{C}^{op} \rightarrow \mathcal{C}$, poniendo $\text{Id}^{**}(A) = A$ y $\text{Id}^{**}(f) = f$, y resulta $\text{Id}^* \circ \text{Id}^{**} = \text{Id}_{\mathcal{C}^{op}}$, $\text{Id}^{**} \circ \text{Id}^* = \text{Id}_{\mathcal{C}}$. ■

Ejemplo 6.3.14. El funtor contravariante hom^B . Si \mathcal{C} es una categoría localmente pequeña, podemos considerar

$$\text{hom}^B : \mathcal{C} \rightarrow \text{Set}$$

poniendo $\text{hom}^B(A) = \text{Hom}_{\mathcal{C}}(A, B)$ para cada objeto A de \mathcal{C} y si $f \in \text{Hom}_{\mathcal{C}}(A, C)$,

$$\text{hom}^B(f) : \text{Hom}_{\mathcal{C}}(C, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, B)$$

es tal que

$$\text{hom}^B(f)(h) = f \circ h$$

para cada $h \in \text{Hom}_{\mathcal{C}}(C, B)$:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(C, B) & \xrightarrow{\text{hom}^B(f)} & \text{Hom}_{\mathcal{C}}(A, B) \\ h & \longmapsto & h \circ f \end{array} \quad \begin{array}{ccc} A & \xrightarrow{f} & C \\ & \searrow h \circ f & \swarrow h \\ & B & \end{array}$$

Si ahora $f \in \text{Hom}(A, C)$, $g \in \text{Hom}(C, D)$, entonces para cada $h \in \text{Hom}_{\mathcal{C}}(D, B)$,

$$\text{hom}^B(f) \circ \text{hom}^B(g)(h) = \text{hom}^B(f)(h \circ g) = (h \circ g) \circ f = h \circ (g \circ f) = \text{hom}^B(g \circ f)(h)$$

de donde $\text{hom}^B(g \circ f) = \text{hom}^B(f) \circ \text{hom}^B(g)$:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(D, B) & \xrightarrow{\text{hom}^B(g)} & \text{Hom}_{\mathcal{C}}(C, B) & \xrightarrow{\text{hom}^B(f)} & \text{Hom}_{\mathcal{C}}(A, B) \\ h & \longmapsto & h \circ g & \longmapsto & (h \circ g) \circ f \end{array} \quad \begin{array}{ccccc} A & \xrightarrow{f} & C & \xrightarrow{g} & D \\ & \searrow (h \circ g) \circ f & \downarrow h \circ g & \swarrow h & \\ & & B & & \end{array}$$

Dejamos los demás detalles de la prueba de que hom^B es un funtor contravariante como ejercicio. El funtor contravariante hom^B suele denotarse también como $\text{Hom}(-, B)$. ■

Al igual que con los funtores covariantes, los funtores contravariantes preservan diagramas conmutativos, pero invierten las flechas:

Lema 6.3.15. *Un funtor contravariante mapea diagramas conmutativos en diagramas conmutativos, con las flechas en el sentido inverso del diagrama original.*

El concepto de funtor permite definir una noción de morfismos entre categorías que en cierta forma preservan las relaciones entre objetos y morfismos. El paso que nos queda dar es definir una noción de equivalencia entre categorías. Imitando las definiciones que hemos dado de isomorfismo en las distintas estructuras algebraicas que estudiamos, introducimos la siguiente definición:

Definición 6.3.16. *Sean \mathcal{C} y \mathcal{D} dos categorías. Decimos que \mathcal{C} es una **categoría isomorfa** a \mathcal{D} si existen funtores $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ tales que $G \circ F = \text{Id}_{\mathcal{C}}$ y $F \circ G = \text{Id}_{\mathcal{D}}$.*

*Decimos que \mathcal{C} es **anti-isomorfa** a \mathcal{D} si existen funtores contravariantes $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ tales que $G \circ F = \text{Id}_{\mathcal{C}}$, $F \circ G = \text{Id}_{\mathcal{D}}$.*

Ejemplo 6.3.17. Sea P un poset y P^* su poset dual. Consideremos las categorías \mathcal{C}_P y \mathcal{C}_P^{op} asociadas a P y la categoría \mathcal{C}_{P^*} asociada a P^* . Definamos $F : \mathcal{C}_{P^*} \rightarrow \mathcal{C}_P^{op}$ dada por $F(x) = x$ para cada $x \in P = \text{ob } \mathcal{C}_{P^*} = \text{ob } \mathcal{C}_P^{op}$ y si $f = (x, y) \in \text{mor } \mathcal{C}_{P^*}$, sea $F(f) = (y, x) \in \text{mor } \mathcal{C}_P^{op}$.

Observemos que si $f = (x, y) \in \text{Hom}_{\mathcal{C}_{P^*}}(x, y)$, entonces $y \preceq x$. Luego $(y, x) \in \text{Hom}_{\mathcal{C}_P}(y, x)$ y por lo tanto $(y, x) \in \text{Hom}_{\mathcal{C}_P^{op}}(x, y)$. Esto es,

$$f \in \text{Hom}_{\mathcal{C}_{P^*}}(x, y) \implies F(f) \in \text{Hom}_{\mathcal{C}_P^{op}}(F(x), F(y)).$$

Además $F(\text{id}_x^{\mathcal{C}_{P^*}}) = F((x, x)) = (x, x) = \text{id}_x^{\mathcal{C}_P^{op}}$. Finalmente, dados $x, y, z \in P^*$ tales que $z \preceq y \preceq x$, tenemos que $f = (x, y)$ es el único morfismo en $\text{Hom}_{\mathcal{C}_{P^*}}(x, y)$, $g = (y, z)$ es el único morfismo en $\text{Hom}_{\mathcal{C}_{P^*}}(y, z)$ y

$g \circ f = (x, z)$. Por otra parte,

$$F(g \circ f) = (z, x) = (y, x) \circ_{\mathcal{C}_P} (z, y) = (z, y) \circ_{\mathcal{C}_P^{op}} (y, x) = F(g) \circ_{\mathcal{C}_P^{op}} F(f)$$

con lo cual F es un funtor covariante.

De manera análoga podemos definir el funtor $G : \mathcal{C}_P^{op} \rightarrow \mathcal{C}_{P^*}$ poniendo $G(x) = x$ para cada $x \in \text{ob } \mathcal{C}_P^{op}$ y si $f = (y, x) \in \text{Hom}_{\mathcal{C}_P^{op}}(x, y)$, $G(f) = (x, y) \in \text{Hom}_{\mathcal{C}_{P^*}}(x, y)$. Dejamos como **ejercicio** verificar que efectivamente G es un funtor covariante.

Finalmente, $F \circ G(x) = x = G \circ F(x)$ para cada $x \in P = \text{ob } \mathcal{C}_{P^*} = \text{ob } \mathcal{C}_P^{op}$. Si ahora $f = (x, y) \in \text{Hom}_{\mathcal{C}_{P^*}}(x, y)$, entonces

$$G \circ F(f) = G((y, x)) = (x, y) = f$$

y de manera análoga, si $g = (y, x) \in \text{Hom}_{\mathcal{C}_P^{op}}(x, y)$, entonces

$$F \circ G(g) = F((x, y)) = (y, x) = g.$$

Concluimos que $G \circ F = \text{Id}_{\mathcal{C}_{P^*}}$ y $F \circ G = \text{Id}_{\mathcal{C}_P^{op}}$, con lo cual \mathcal{C}_{P^*} y \mathcal{C}_P^{op} son categorías isomorfas. ■

Las categorías isomorfas aparecen muy raramente. Se trata esencialmente de la misma categoría con los objetos y flechas renombrados. Mucho más interesante es la noción de *categorías equivalentes*. Lamentablemente necesitamos desarrollar un poco más la teoría para introducir este concepto. Lo haremos en el próximo capítulo.

6.4. Monomorfismos, epimorfismos e isomorfismos

En la categoría Set los morfismos son funciones entre conjuntos, y por lo tanto tiene sentido hablar de funciones inyectivas, sobreyectivas o biyectivas. Sin embargo, si $f : A \rightarrow B$ es un morfismo en mor Set , estas nociones están definidas en base a los elementos de A y B : por ejemplo f es inyectiva si $f(x) \neq f(y)$ cada vez que $x \neq y$ en A . En una categoría abstracta, los morfismos pueden no ser funciones, y los objetos podrían no ser conjuntos. Por lo tanto debemos dar una definición más general de estos conceptos pero que no haga referencia a otros elementos que no sean los objetos y los morfismos de la categoría.

Definición 6.4.1. Sea \mathcal{C} una categoría y $f : A \rightarrow B$ un morfismo de \mathcal{C} . Decimos que f es un **morfismo mónico** (o un **monomorfismo**) si para cualquier par de morfismos $g : C \rightarrow A$, $h : C \rightarrow A$ en $\text{mor } \mathcal{C}$ se verifica que

$$f \circ g = f \circ h \implies g = h.$$

Es decir, f es mónico si para cada $g, h \in \text{Hom}(C, A)$ se tiene

$$C \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} A \xrightarrow{f} B \quad \text{conmutativo} \implies g = h$$

Si un morfismo es mónico en una categoría \mathcal{C} lo será en cualquier subcategoría \mathcal{C}' de \mathcal{C} que lo contenga como morfismo, dado que la composición en \mathcal{C}' es la misma que en \mathcal{C} . Es decir:

Lema 6.4.2. Sea \mathcal{C} una categoría y \mathcal{C}' una subcategoría de \mathcal{C} . Si $f \in \text{mor } \mathcal{C}$ es mónico y $f \in \text{mor } \mathcal{C}'$, entonces f es un monomorfismo mónico en \mathcal{C}' .

Demostración. Sea \mathcal{C}' una subcategoría de una categoría \mathcal{C} y sea $f \in \text{mor } \mathcal{C}'$ tal que f es un morfismo mónico en \mathcal{C} . Si $g, h \in \text{mor } \mathcal{C}'$ son tales que $f \circ g = f \circ h$, en particular esta igualdad vale en \mathcal{C} . Como f es mónico en \mathcal{C} , resulta que $g = h$, y por lo tanto f es mónico en \mathcal{C}' . \square

El concepto de morfismo mónico generaliza la noción de función inyectiva en el siguiente sentido:

Teorema 6.4.3. En Set un morfismo es mónico si y sólo si es una función inyectiva.

Demostración. Supongamos primero que $f : A \rightarrow B$ es un morfismo mónico en Set . Sean $a, a' \in A$ tales que $f(a) = f(a') = b$. Sea $C = \{b\}$ y sean $g : C \rightarrow A$, $h : C \rightarrow A$ dadas por $g(b) = a$, $h(b) = a'$ respectivamente. Entonces

$$f \circ g(b) = f(a) = b, \quad f \circ h(b) = f(a') = b$$

con lo cual $f \circ g = f \circ h$. Siendo f mónico, deberá ser $g = h$, de donde $g(b) = h(b)$, o sea $a = a'$. Concluimos que f es una función inyectiva.

Supongamos ahora que $f : A \rightarrow B$ es una función inyectiva. Sea C un conjunto cualquiera y $g, h : C \rightarrow A$ funciones cualesquiera tales que $f \circ g = f \circ h$. Entonces para cada $c \in C$,

$$f(g(c)) = f(h(c)) \xrightarrow{f \text{ inyectiva}} g(c) = h(c).$$

Concluimos entonces que $g = h$ y f es un monomorfismo en Set . \square

Un resultado similar al Lema 6.4.3 es válido para aquellas categorías en las cuales los objetos son conjuntos y los morfismos son funciones entre conjuntos. Estas categorías pueden generalizarse de la siguiente manera:

Definición 6.4.4. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor. Decimos que F es **fiel** si para cada par de objetos A, B de \mathcal{C} , la función $\text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{D}}(F(A), F(B))$, $f \mapsto F(f)$ es inyectiva, es decir, si $f, g \in \text{Hom}_{\mathcal{C}}(A, B)$, entonces

$$F(f) = F(g) \implies f = g.$$

Si existe un funtor fiel $F : \mathcal{C} \rightarrow \text{Set}$, \mathcal{C} se dice una **categoría concreta**.

Ejemplo 6.4.5. El funtor identidad $\text{Id}_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$ (Ejemplo 6.3.2) es un funtor fiel. El funtor inclusión $\text{inc} : \mathcal{C}' \rightarrow \mathcal{C}$ (Ejemplo 6.3.3) para una subcategoría $\mathcal{C}' \subseteq \mathcal{C}$ es fiel. El funtor olvido $\text{fgt} : \mathcal{C} \rightarrow \text{Set}$ (Ejemplo 6.3.4) es fiel. En particular Poset , Ret , Grp , Mon y Sgrp son categorías concretas. \blacksquare

Lema 6.4.6. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor fiel y sea $f \in \text{mor } \mathcal{C}$. Si $F(f)$ es un morfismo mónico en \mathcal{D} , entonces f es un morfismo mónico en \mathcal{C} .

Demostración. Sea $f \in \text{Hom}_{\mathcal{C}}(A, B)$ y sean $g, h \in \text{hom}_{\mathcal{C}}(C, A)$ tales que $g \circ f = h \circ f$, es decir, el siguiente diagrama es conmutativo

$$C \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} A \xrightarrow{f} B$$

Como F es un funtor, el siguiente diagrama en \mathcal{D} también conmuta:

$$F(C) \begin{array}{c} \xrightarrow{F(g)} \\ \xrightarrow{F(h)} \end{array} F(A) \xrightarrow{F(f)} F(B)$$

Luego, como $F(f)$ es un morfismo mónico, $F(g) = F(h)$. Pero como F es fiel, debe ser $g = h$, con lo cual f es un morfismo mónico. \square

Corolario 6.4.7. En toda categoría donde los objetos son conjuntos, los morfismos son funciones entre conjuntos y la composición es la composición usual de funciones (por ejemplo, en Poset, Ret, Boole, Vect, Grp, Ab, Mon, Sgrp, etc.), toda función inyectiva es un morfismo mónico.

Demostración. Si \mathcal{C} es una categoría que verifica las hipótesis del Corolario, entonces existe un funtor olvido $\text{fgt} : \mathcal{C} \rightarrow \text{Set}$ tal que $\text{fgt}(f) = f$ para cada $f \in \text{mor } \mathcal{C}$ que es un funtor fiel. Luego si f es inyectiva, del Teorema 6.4.3 $\text{fgt}(f)$ es un morfismo mónico en Set y del Lema 6.4.6, f un morfismo mónico en \mathcal{C} . \square

Ejemplo 6.4.8. En una categoría concreta, donde existe un funtor fiel $F : \mathcal{C} \rightarrow \text{Set}$, los morfismos que se mapean por F en funciones inyectivas automáticamente son morfismos mónicos en \mathcal{C} por el Lema 6.4.6 y el Teorema 6.4.3. La recíproca en general es falsa, esto es, en general **no es cierto que** en una categoría concreta **los morfismos mónicos son mapeados en funciones inyectivas**.

Consideremos la categoría $\mathbf{2}$, tal que $\text{ob } \mathbf{2} = \{A, B\}$, $\text{mor } \mathbf{2} = \{\text{id}_A, \text{id}_B, f\}$ con $f : A \rightarrow B$ (ver Ejemplo 6.2.6):

$$\mathbf{2} : \quad \begin{array}{c} \text{id}_A \quad \text{id}_B \\ \curvearrowright \quad \curvearrowright \\ A \xrightarrow{f} B \end{array}$$

Consideremos ahora los conjuntos $X = \{1, 2\}$, $Y = \{1\}$ y la función $r : X \rightarrow Y$ tal que $r(1) = r(2) = 1$.

Pongamos $F : \mathbf{2} \rightarrow \text{Set}$ tal que $F(A) = X$, $F(B) = Y$, $F(\text{id}_A) = \text{id}_X$, $F(\text{id}_B) = \text{id}_Y$ y $F(f) = r$. Entonces es inmediato que F es un funtor fiel, y por lo tanto $\mathbf{2}$ es una categoría concreta. En $\mathbf{2}$, f es un morfismo mónico, dado que f puede componerse a derecha sólo por id_A . Sin embargo, $F(f) = r$ no es una función inyectiva.

Observemos que entonces r no es un morfismo mónico en Set. Por lo tanto, este ejemplo prueba además que, en general, un funtor no mapea morfismos mónicos en morfismos mónicos. \blacksquare

Ejemplo 6.4.9. Morfismos mónicos en Poset y en Ret. En Poset (resp. en Ret) un homomorfismo de posets $f : X \rightarrow Y$ (resp. un homomorfismo de retículos) es un morfismo mónico si y sólo si es un homomorfismo inyectivo.

En efecto, sea $f : X \rightarrow Y$ un homomorfismo de posets que es un morfismo mónico en Poset. Sean $a, a' \in X$ tales que $f(a) = f(a') = b$. Entonces $\{b\}$ es un poset trivialmente y $g, h : \{b\} \rightarrow X$ tales que $g(b) = a$ y $h(b) = a'$ son homomorfismos de posets. Por lo tanto la prueba sigue de modo completamente análogo a la prueba del Teorema 6.4.3. Recíprocamente, por el Corolario 6.4.7, todo homomorfismo de posets inyectivo es un morfismo mónico en Poset.

Como $\{b\}$ es además un retículo, la prueba en Ret es análoga. Dejamos los detalles como **ejercicio**. ■

Ejemplo 6.4.10. Morfismos mónicos en Grp, Mon y Sgrp. En Grp (resp. en Mon y Sgrp) un morfismo $f \in \text{Hom}(G, H)$ es mónico si y sólo si $f : G \rightarrow H$ es un monomorfismo de grupos (resp. de monoides, semigrupos).

Comencemos probando el resultado en la categoría de grupos. Del Corolario 6.4.7, si f es un monomorfismo de grupos entonces f es un morfismo mónico en Grp. Veamos que también vale la recíproca.

Supongamos que $f : G \rightarrow H$ es un morfismo mónico en Grp. Sean $x, y \in G$ tales que $f(x) = f(y) = a$ y consideremos los homomorfismos de grupo

$$g : (\mathbb{Z}, +) \rightarrow G, \quad g(k) = x^k; \quad h : (\mathbb{Z}, +) \rightarrow G, \quad h(k) = y^k.$$

Entonces

$$f \circ g(k) = f(x^k) = f(x)^k = a^k = f(y)^k = f(y^k) = f \circ h(k).$$

Como f es un morfismo mónico, resultan $g = h$. En particular, $x = g(1) = h(1) = y$. Luego f es inyectivo.

Pasemos ahora a Mon. Que todo morfismo mónico en Mon es un monomorfismo de monoides es consecuencia del Corolario 6.4.7. Para probar la recíproca, supongamos que $f : X \rightarrow Y$ es un morfismo mónico en Mon y sean $x, y \in X$ tales que $f(x) = f(y) = a \in Y$. Consideremos los homomorfismos de monoides

$$g : (\mathbb{N}_0, +) \rightarrow X, \quad g(n) = x^n; \quad h : (\mathbb{N}_0, +) \rightarrow Y, \quad h(n) = y^n.$$

Con exactamente el mismo argumento que antes tenemos que $f \circ g = f \circ h$ y por lo tanto $g = h$. En particular $x = g(1) = h(1) = y$, con lo cual f es inyectivo.

A esta altura debería quedar claro que la prueba para Sgrp es análoga, considerando los morfismos g y h con dominio en el semigrupo $(\mathbb{N}, +)$. Dejamos los detalles como **ejercicio**. ■

Los ejemplos anteriores pueden hacernos pensar que si \mathcal{C} es una categoría cuyos objetos son conjuntos (con cierta estructura) y los morfismos son funciones, entonces los morfismos mónicos son los morfismos inyectivos. Esto es en general **falso** como mostraremos en el siguiente ejemplo:

Ejemplo 6.4.11. La categoría de grupos divisibles. Un grupo abeliano $(G, +)$ se dice *divisible* si para cada $n \in \mathbb{N}$ y cada $x \in G$, existe $y \in G$ tal que $ny = x$. Por ejemplo $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ son trivialmente grupos divisibles, pero $(\mathbb{Z}, +)$ no lo es, pues en este caso si $x \in \mathbb{Z}$ es un número impar y tomamos $n = 2$ vemos que no existe $y \in \mathbb{Z}$ tal que $2y = x$. El grupo multiplicativo (\mathbb{C}^*, \cdot) también es un grupo divisible: dado $x \in \mathbb{C}^*$ y $n \in \mathbb{N}$, cualquier $y \in \mathbb{C}^*$ que sea una raíz n -ésima de x verifica $y^n = x$. En contraposición, (\mathbb{R}^*, \cdot) no es divisible, pues si tomamos $n \in \mathbb{N}$ par y $x < 0$, no existe $y \in \mathbb{R}$ tal que $y^n = x$.

Si G es un grupo divisible y $N \triangleleft G$, entonces G/N también es divisible. En efecto, dado $[x] \in G/N$ y $n \in \mathbb{N}$, sea $y \in G$ tal que $ny = x$. Entonces $n[y] = [x]$. Los grupos divisibles forman una categoría DivGrp (donde los morfismos son homomorfismos de grupos usuales) que es una subcategoría full de Ab y de Grp .

Consideremos $(\mathbb{Q}, +) \in \text{ob DivGrp}$. Como $\mathbb{Z} \triangleleft \mathbb{Q}$, $(\mathbb{Q}/\mathbb{Z}, +)$ también es un grupo divisible y la proyección al cociente $\pi : \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ es un morfismo en DivGrp . π es claramente una función no inyectiva, dado que $\ker \pi = \mathbb{Z}$ no es trivial. Veremos que sin embargo π es un morfismo mónico en DivGrp .

Para esto consideremos un grupo divisible $(G, +)$ cualquiera y sea $g : G \rightarrow \mathbb{Q}$ un homomorfismo de grupos. Denotemos por $t : G \rightarrow \mathbb{Q}$ y $\tilde{t} : G \rightarrow \mathbb{Q}/\mathbb{Z}$ a los homomorfismos triviales, es decir, $t(x) = 0$ y $\tilde{t}(x) = [0]$ para cada $x \in G$. Probaremos primero que

$$(6.4) \quad \pi \circ g = \tilde{t} \implies g = t.$$

En efecto, supongamos que $\pi \circ g = \tilde{t}$. Entonces para cada $x \in G$, $\pi(g(x)) = [0]$, o sea, $g(x) \in \mathbb{Z}$.

Fijemos $x \in G$. Supongamos que $g(x) \geq 0$. Entonces $g(x) \in \mathbb{N}_0$ y por lo tanto $n = g(x) + 1 \in \mathbb{N}$. Como G es un grupo divisible, existirá $y \in G$ tal que $ny = x$. Aplicando el homomorfismo g a ambos lados de la igualdad tendremos que $ng(y) = g(x)$, o sea

$$g(y) = \frac{g(x)}{1 + g(x)} \implies 0 \leq g(y) < 1.$$

Como $g(y) \in \mathbb{Z}$ deberá ser $g(y) = 0$. Luego $g(x) = ng(y) = 0$.

Si fuese $g(x) \leq 0$, entonces $g(-x) = -g(x) \geq 0$. Luego, por el desarrollo anterior, $g(-x) = 0$, de donde

$$g(x) = g(-(-x)) = -g(-x) = 0.$$

Concluimos que $g = t$ como queríamos probar.

Sean ahora $g : G \rightarrow \mathbb{Q}$ y $h : G \rightarrow \mathbb{Q}$ dos morfismos tales que $\pi \circ g = \pi \circ h$ y sea $f = g - h : G \rightarrow \mathbb{Q}$ dado por $f(x) = g(x) - h(x)$. Observemos que f es un homomorfismo de grupos. En efecto,

$$f(x + y) = g(x + y) - h(x + y) = g(x) + g(y) - (h(x) + h(y)) = (g(x) - h(x)) + (g(y) - h(y)) = f(x) + f(y).$$

Además,

$$\pi \circ f(x) = \pi(g(x) - h(x)) = [g(x) - h(x)] = [g(x)] - [h(x)] = \pi(g(x)) - \pi(h(x)) = [0]$$

para cada $x \in X$. Concluimos que $\pi \circ f = \tilde{t}$, y por lo tanto $f = t$, es decir, $f(x) = 0$ para cada $x \in G$, y entonces $g(x) = h(x)$ para todo $x \in G$. Luego $g = h$ y por lo tanto π es mónico. ■

Observación 6.4.12. El Ejemplo 6.4.11 muestra que la recíproca del Lema 6.4.2 es falsa: un morfismo f en una subcategoría \mathcal{C}' de una categoría \mathcal{C} puede ser mónico en \mathcal{C}' sin ser mónico en \mathcal{C} . La razón es que en \mathcal{C}' hay “menos” morfismos que en \mathcal{C} con los cuales componer a f para verificar la condición de monomorfismo. Podemos observar que los morfismos $g : (\mathbb{Z}, +) \rightarrow G$ y $h : (\mathbb{Z}, +) \rightarrow G$ que utilizamos en la prueba del Teorema 6.4.10 no aplican en el caso de la categoría DivGrp , dado que $(\mathbb{Z}, +)$ no es un grupo divisible.

Ejemplo 6.4.13. Si P es un poset, en la categoría \mathcal{C}_P (ver Ejemplo 6.2.8) todo morfismo es un monomorfismo. En efecto, dado un morfismo $(p, p') \in \text{mor } \mathcal{C}_P$ y $p'' \in \text{ob } \mathcal{C}$ cualquiera, si existe un morfismo en $f \in \text{Hom}(p'', p)$ es porque $p'' \preceq p$. En este caso $f = (p'', p)$ es el único morfismo tal que $\text{dom } f = p''$ y $\text{codom } f = p$ con lo cual la definición de monomorfismo se cumple trivialmente. ■

Ejemplo 6.4.14. Sea $(M, *)$ un monoide y consideremos la categoría \mathcal{C}_M con $\text{ob } \mathcal{C}_M = \{\star\}$ del Ejemplo 6.2.9. Un morfismo en la categoría \mathcal{C}_M es un elemento de M y la composición de morfismos está dada por la operación en M . Luego f es un morfismo mónico si y sólo si para cada $g, h \in M$ se verifica:

$$f * g = f * h \implies g = h$$

es decir, f es un morfismo mónico en \mathcal{C}_M si y sólo si f es un elemento cancelativo a izquierda en M . En particular si (G, \cdot) es un grupo, todo morfismo en \mathcal{C}_G es un monomorfismo. ■

Así como los morfismos mónicos generalizan el concepto de funciones inyectivas entre conjuntos, daremos ahora una generalización de las funciones sobreyectivas introduciendo los morfismos denominados *épico*:

Definición 6.4.15. Sea \mathcal{C} una categoría y $f : A \rightarrow B$ un morfismo de \mathcal{C} . Decimos que f es un **morfismo épico** (o un **epimorfismo**) si para cualquier $C \in \text{ob } \mathcal{C}$ y cualquier par de morfismos $g, h \in \text{Hom}(B, C)$, se verifica

$$g \circ f = h \circ f \implies g = h.$$

Es decir, f es épico si para cada $g, h \in \text{Hom}(B, C)$ se tiene

$$A \xrightarrow{f} B \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} C \quad \text{conmutativo} \implies g = h$$

Nuevamente, tenemos que los epimorfismos de \mathcal{C} son epimorfismos en cualquier subcategoría que los contenga como morfismos. Dejamos los detalles de la prueba como **ejercicio**:

Lema 6.4.16. Sea \mathcal{C} una categoría y \mathcal{C}' una subcategoría de \mathcal{C} . Si $f \in \text{mor } \mathcal{C}$ es épico y $f \in \text{mor } \mathcal{C}'$, entonces f es un epimorfismo en \mathcal{C}' .

Como hemos mencionado anteriormente, los morfismos épicos generalizan el concepto de función sobreyectiva. Más precisamente:

Teorema 6.4.17. *En Set un morfismo es épico si y sólo si es una función sobreyectiva.*

Demostración. Supongamos primero que $f : A \rightarrow B$ es un morfismo épico en Set. Sea $b \in B$ cualquiera. Debemos probar que existe $a \in A$ tal que $f(a) = b$. Supongamos que esto no ocurre. Entonces B tiene al menos dos elementos distintos, digamos $b_1 \neq b_2$ (uno de ellos podría ser igual a b). Consideremos las funciones $g : B \rightarrow B$ y $h : B \rightarrow B$ tal que

$$g(x) = \begin{cases} b_1 & \text{si } x = b \\ x & \text{si } x \neq b \end{cases}, \quad h(x) = \begin{cases} b_2 & \text{si } x = b \\ x & \text{si } x \neq b \end{cases}.$$

Claramente $g \neq h$. Como $f(x) \neq b$ para cada $x \in A$, resulta $g \circ f(x) = x$ y $h \circ f(x) = x$ para cada $x \in A$. Luego $g \circ f = h \circ f$, pero $h \neq g$ lo que contradice la hipótesis. Luego f es sobreyectiva.

Supongamos ahora que f es una función sobreyectiva. Sea C un conjunto cualquiera y sean $g, h : B \rightarrow C$ funciones tales que $g \circ f = h \circ f$. Sea $b \in B$. Como f es sobre, existe $a \in A$ tal que $f(a) = b$. Luego

$$g(b) = g(f(a)) = h(f(a)) = h(b).$$

Como $b \in B$ es un elemento genérico, concluimos que $g = h$ y entonces f es un epimorfismo. \square

Lema 6.4.18. *Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor fiel y sea $f \in \text{mor } \mathcal{C}$. Si $F(f)$ es un morfismo épico en \mathcal{D} , entonces f es un morfismo épico en \mathcal{C} .*

Demostración. Sea $f \in \text{Hom}_{\mathcal{C}}(A, B)$ y sean $g, h \in \text{hom}_{\mathcal{C}}(C, A)$ tales que $f \circ g = f \circ h$, es decir, el siguiente diagrama es conmutativo

$$A \xrightarrow{f} B \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} C$$

Como F es un funtor, el siguiente diagrama en \mathcal{D} también conmuta:

$$F(A) \xrightarrow{F(f)} F(B) \begin{array}{c} \xrightarrow{F(g)} \\ \xrightarrow{F(h)} \end{array} F(C)$$

Luego, como $F(f)$ es un morfismo épico, $F(g) = F(h)$. Pero como F es fiel, debe ser $g = h$, con lo cual f es un morfismo épico. \square

La prueba del siguiente resultado es completamente análoga a la del Corolario 6.4.7. Dejamos los detalles como **ejercicio**:

Corolario 6.4.19. *En toda categoría donde los objetos sean conjuntos, los morfismos sean funciones entre conjuntos y la composición sea la composición usual de funciones (por ejemplo, en Poset, Ret, Boole, Vect, Grp, Ab, Mon, Sgrp, etc.), toda función sobreyectiva es un morfismo épico.*

Observación 6.4.20. *El morfismo f del Ejemplo 6.4.8 en la categoría $\mathbf{2}$ es trivialmente un epimorfismo. Siguiendo las mismas ideas que en ese ejemplo es posible construir un funtor fiel $F : \mathbf{2} \rightarrow \text{Set}$ tal que $F(f)$ no sea una función sobreyectiva (dejamos los detalles como **ejercicio**). Por lo tanto la recíproca del Lema 6.4.18 también es falsa.*

Ejemplo 6.4.21. Morfismos épicos en Poset Un homomorfismo de posets $f : X \rightarrow Y$ es un morfismo épico en Poset si y sólo si es un homomorfismo sobreyectivo.

En efecto, por el Corolario 6.4.19, todo homomorfismo sobreyectivo en Poset o en Ret es un morfismo épico.

Supongamos ahora que X, Y son posets y $f : X \rightarrow Y$ es un morfismo épico en Poset, y supongamos por el absurdo que f no es sobreyectivo. Sea $b \in Y$ tal que $b \notin \text{Im}(f)$. Consideremos el poset $\mathbf{2} = \{0, 1\}$ con el orden usual (o sea, tal que $0 < 1$) y sean $g : Y \rightarrow \mathbf{2}$, $h : Y \rightarrow \mathbf{2}$ dadas por

$$(6.5) \quad g(y) = \begin{cases} 0 & \text{si } b \not\leq y \\ 1 & \text{si } b \leq y \end{cases}, \quad h(y) = \begin{cases} 0 & \text{si } b \not\leq y \text{ o } y = b \\ 1 & \text{si } b < y \end{cases}$$

(observemos que $y \not\leq b$ significa que $b < y$ o y y b no son comparables). Observemos que g es un homomorfismo de posets. En efecto, si $y, z \in Y$ verifican $y \leq z$, entonces:

- si $b \leq y$, entonces $b \leq z$ y por lo tanto $g(y) = g(z) = 1$. En particular, $g(y) \leq g(z)$;
- si $b \not\leq y$, entonces $g(y) = 0$, y entonces automáticamente $g(y) \leq g(z)$.

De manera similar, h es un homomorfismo de posets. Si $b < y$ o $b \not\leq y$ la prueba es análoga a la de g . Supongamos que $y = b$. Luego, si $y = z$, entonces $b = y = z$ y por lo tanto $h(y) = h(z) = 0$. En particular, $h(y) \leq h(z)$. Si $y \neq z$, entonces $b = y < z$, y por lo tanto $h(y) = 0$, $h(z) = 1$. O sea, $h(y) \leq h(z)$.

Como para cada $x \in X$, $f(x) \neq b$, resulta que $b < f(x)$ o $b \not\leq f(x)$ para cada $x \in X$. Luego $g(f(x)) = h(f(x))$ para cada $x \in X$, y como f es épico, deberían ser $g = h$, lo cual es absurdo dado que $g(b) = 1$ y $h(b) = 0$.

Concluimos que $\text{Im}(f) = Y$, y por lo tanto f es sobreyectiva. ■

Ejemplo 6.4.22. Morfismos épicos en Grp. En Grp un morfismo $f : G \rightarrow H$ es épico si y sólo si es un epimorfismo de grupos.

La prueba que presentaremos aquí se debe a C. E. Linderholm (cf. [15]). Si $f : G \rightarrow H$ es un epimorfismo de grupos, en particular es una función sobreyectiva, y por el Corolario 6.4.19 resulta un morfismo épico en Grp.

Supongamos ahora que $f : G \rightarrow H$ es un homomorfismo de grupos que es un morfismo épico en Grp. Sea $A = f(G)$. Debemos probar que $A = H$.

Observemos que $f(A)$ es un subgrupo de H , no necesariamente normal. Por lo tanto podemos considerar el conjunto cociente

$$X = H / \equiv_r (A)$$

de H por la congruencia a derecha módulo A (ver la sección 5.1). Un elemento genérico de X es de la forma $[y]_r = Ay$ para $y \in H$, y en particular $A = [e]_r$.

Si $h \in H$, entonces la función $R_h : X \rightarrow X$ tal que $R_h([y]_r) = A([yh]_r)$ está bien definida. En efecto, si $[y]_r = [y']_r$, entonces $y(y')^{-1} \in A$, y por lo tanto $(yh)(y'h)^{-1} = y(y')^{-1} \in A$, es decir, $[yh]_r = [y'h]_r$. Más aún, es inmediato verificar que $R_h \circ R_{h^{-1}} = R_{h^{-1}} \circ R_h = \text{Id}_X$, con lo cual R_h es biyectiva y $R_h^{-1} = R_{h^{-1}}$.

Sea ahora A' un subconjunto cualquiera de H que no sea una coclase a derecha y pongamos

$$Y = X \cup \{A'\}$$

Finalmente, pongamos $K = \mathcal{B}(Y)$, el grupo de biyecciones de Y (ver Ejemplo 4.3.6).

Para cada $h \in H$, definamos la función $\varphi_h : Y \rightarrow Y$ dada por $\varphi_h|_X = R_h$ y $\varphi_h(A') = A'$. Como $R_h : X \rightarrow X$ es biyectiva, resulta inmediato que $\varphi_h : Y \rightarrow Y$ es biyectiva y por lo tanto $\varphi_h \in \mathcal{B}(Y)$ para cada $h \in H$. Más aún, la función $\varphi : H \rightarrow \mathcal{B}(Y)$ dada por $\varphi(h) = \varphi_h$ es un homomorfismo de grupos. En efecto, si $[y]_r \in X$, entonces

$$\begin{aligned} \varphi(hh')([y]_r) &= \varphi_{hh'}([y]_r) = [y(hh')]_r = [(yh)h']_r = R_{h'}([yh]_r) = R_{h'}(R_h([y]_r)) \\ &= \varphi_{h'}(\varphi_h([y]_r)) = \varphi(h) \circ \varphi(h')([y]_r). \end{aligned}$$

y además

$$\varphi(hh')(A') = \varphi_{hh'}(A') = A' = \varphi_{h'}(\varphi_h(A')) = \varphi(h') \circ \varphi(h)(A').$$

Concluimos entonces que $\varphi(hh') = \varphi(h) \circ \varphi(h')$ como queríamos ver.

Consideremos ahora la biyección $\sigma : Y \rightarrow Y$ tal que $\sigma(A') = A$, $\sigma(A) = A'$ y $\sigma([y]_r) = [y]_r$ si $[y]_r \neq A$ (recordemos que $A = [e]_r$). Si $I_\sigma : \mathcal{B}(Y) \rightarrow \mathcal{B}(Y)$ es la conjugación en $\mathcal{B}(Y)$ por σ (ver la Definición 4.7.21) entonces

$$\psi : H \rightarrow \mathcal{B}(Y), \quad \psi = I_\sigma \circ \varphi$$

es un homomorfismo de grupos. Explícitamente,

$$\Psi(h) = \sigma \circ \varphi(h) \circ \sigma^{-1}$$

para cada $h \in H$.

Tenemos entonces el siguiente diagrama en Grp:

$$(6.6) \quad G \xrightarrow{f} H \xrightleftharpoons[\varphi]{\psi} \mathcal{B}(Y).$$

Veamos que se trata de un diagrama conmutativo. Sea $g \in G$. Entonces $f(g) \in f(G) = A = [e]_r$, y por lo tanto $[f(g)]_r = A$. Luego

$$\varphi(f(g))(A) = [ef(g)]_r = [f(g)]_r = A.$$

Además, por definición, $\varphi(f(g))(A') = A'$.

Ahora bien, como $\sigma(A) = A'$ y $\sigma(A') = A$,

$$\Psi(f(g))(A) = \sigma \circ \varphi(f(g))\sigma^{-1}(A) = \sigma(\varphi(f(g))(A')) = \sigma(A') = A$$

y de manera análoga, $\Psi(f(g))(A') = A$.

Finalmente, si $[y]_r = Ay \neq A$, es decir, $y \notin [e]_r$, entonces $\varphi(f(g))([y]_r) = [yf(g)]_r \neq A$ y como $\sigma([y]_r) = [y]_r$ resulta $\Psi(f(g))([y]_r) = [yf(g)]_r$.

Concluimos que para cada $g \in G$, $\varphi(f(g)) = \Psi(f(g))$. Como g es arbitrario, resulta $\varphi \circ f = \Psi \circ f$ y como f es un morfismo épico, $\varphi = \Psi$.

Sea ahora $h \in H$ cualquiera. Entonces

$$\varphi(h)(A) = \Psi(h)(A) = \sigma(\varphi(h)(\sigma^{-1}(A))) = \sigma(\varphi_h(A')) = \sigma(A') = A$$

Luego $[h]_r = \varphi_h([e]_r) = \varphi_h(A) = A = [e]_r$ y por lo tanto $h \in [e]_r = A$. Concluimos que $H \subseteq A$ y por lo tanto $H = A = f(G)$, con lo cual f es sobreyectiva. ■

Comparando los ejemplos 6.4.10 y 6.4.22 podemos observar que el segundo sólo ha sido enunciado para Grp, y no para Mon y Sgrp. Ocurre que en estos últimos casos puede existir un morfismo épico que no sea un epimorfismo de monoides o semigrupos:

Ejemplo 6.4.23. Los morfismos épicos en Sgrp y en Mon no necesariamente son sobreyectivos.

Consideremos el semigrupo (\mathbb{R}^+, \cdot) . Observemos que el intervalo semiabierto $(0, 1]$ es un subconjunto cerrado para el producto, y por lo tanto es un subsemigrupo de (\mathbb{R}^+, \cdot) . Por lo tanto, la inclusión $i : (0, 1] \rightarrow \mathbb{R}^*$ es un morfismo de subsemigrupos. Veamos que i es un morfismo épico en Sgrp, aunque claramente no es sobreyectivo.

Sea S un semigrupo cualquiera y $g, h : (\mathbb{R}^*, \cdot) \rightarrow S$ morfismos de semigrupos tales que $g \circ i = h \circ i$. En particular, para cada $x \in (0, 1]$, $h(x) = h(i(x)) = g(i(x)) = g(x)$, es decir, h y g coinciden en $(0, 1]$. En particular, $g(1) = h(1)$.

Sea $x > 1$. Entonces $1/x \in (0, 1]$ y por lo tanto $g(1/x) = h(1/x)$. Luego tenemos

$$\begin{aligned} g(x) &= g(x \cdot 1) = g(x) * g(1) = g(x) * h(1) = g(x) * h(1/x \cdot x) = g(x) * (h(1/x) * h(x)) \\ &= (g(x) * h(1/x)) * h(x) = (g(x) * g(1/x)) * h(x) = g(x \cdot 1/x) * h(x) = g(1) * h(x) \\ &= h(1) * h(x) = h(1 \cdot x) = h(x). \end{aligned}$$

Concluimos que $h(x) = g(x)$ para cada $x \in \mathbb{R}^+$ y por lo tanto $h = g$. Luego i es un morfismo épico que no es sobreyectivo.

Como $i(1) = 1$, claramente $i : (0, 1] \rightarrow \mathbb{R}^+$ es un morfismo de monoides. Luego del Lema 6.4.16, i es un morfismo mónico en Mon que no es sobreyectivo. ■

Así como los morfismos mónicos generalizan el concepto de funciones inyectivas y los morfismos épicos el de funciones sobreyectivas, introduciremos a continuación el concepto de *isomorfismo* que generaliza el concepto de función biyectiva. En este caso, la generalización es más directa, dado que una función biyectiva está completamente caracterizada por la existencia de su inverso:

Definición 6.4.24. Sea \mathcal{C} una categoría y $f \in \text{mor } \mathcal{C}$ un morfismo. Si $f \in \text{Hom}(A, B)$, decimos que f es un **isomorfismo** si existe un morfismo $f' \in \text{Hom}(B, A)$ tal que $f' \circ f = \text{id}_A$ y $f \circ f' = \text{id}_B$. Si existe un isomorfismo $f \in \text{Hom}(A, B)$ decimos que A y B son objetos **isomorfos**.

Lema 6.4.25. Sea \mathcal{C} una categoría y $f \in \text{Hom}_{\mathcal{C}}(A, B)$ un isomorfismo. Entonces existe un único $g \in \text{Hom}_{\mathcal{C}}(B, A)$ tal que $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$

Demostración. El morfismo $g : B \rightarrow A$ tal que $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$ existe por la definición de isomorfismo. Debemos probar que es único. Supongamos que existe un morfismo $h : B \rightarrow A$ tal que $h \circ f = \text{id}_A$ y $f \circ h = \text{id}_B$. Entonces

$$h = h \circ \text{id}_B = h \circ (f \circ g) = (h \circ f) \circ g = \text{id}_A \circ g = g$$

como queríamos ver. □

Definición 6.4.26. Sea \mathcal{C} una categoría y $f \in \text{Hom}_{\mathcal{C}}(A, B)$ un isomorfismo. El único morfismo $g \in \text{Hom}_{\mathcal{C}}(B, A)$ tal que $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$ se denomina **inverso** de f y se denota $g = f^{-1}$.

La prueba del siguiente resultado es standard. Dejamos los detalles como **ejercicio**.

Lema 6.4.27. Sea \mathcal{C} una categoría. Entonces:

1. Para cada $A \in \text{ob } \mathcal{C}$, id_A es un isomorfismo.
2. Si $f \in \text{Hom}(A, B)$ es un isomorfismo, entonces $f^{-1} \in \text{Hom}(B, A)$ es un isomorfismo.
3. Si $f \in \text{Hom}(A, B)$ y $g \in \text{Hom}(B, C)$ son isomorfismos, entonces $g \circ f \in \text{Hom}(A, C)$ es un isomorfismo.
4. La relación \sim en $\text{ob } \mathcal{C}$ dada por $A \sim B$ si existe un isomorfismo $f \in \text{Hom}(A, B)$ es una relación de equivalencia.

En el caso de Set , la caracterización de los isomorfismos es inmediata, dada que una función admite un inverso si y sólo si es biyectiva. Esto es:

Teorema 6.4.28. En Set , una función $f : A \rightarrow B$ es un isomorfismo si y sólo si es biyectiva.

A partir de los resultados obtenidos en los capítulos 2, 3 y 4 tenemos que:

Teorema 6.4.29. Los isomorfismos en Poset , Ret , Sgrp , Mon y Grp son los isomorfismos de las respectivas estructuras.

Observemos que lsi \mathcal{C} es una categoría donde los objetos son conjuntos, los morfismos son funciones entre conjuntos, la composición y las identidades son las usuales, entonces **todo isomorfismo es una función biyectiva**. En este sentido, tenemos la implicación inversa de las que teníamos para las definiciones de monomorfismo y epimorfismo. Esto es, si en \mathcal{C} los morfismos son funciones, entonces:

1. f inyectiva $\implies f$ morfismo mónico.
2. f sobreyectiva $\implies f$ morfismo épico.
3. f isomorfismo $\implies f$ biyectiva

Ya vimos que en Set valen todas las recíprocas, pero hay categorías donde las recíprocas de los puntos (1) y (2) son falsas. Veremos en el Ejemplo 6.4.31 que la recíproca del punto (3) también es falsa. Como hay morfismos mónicos o épicos que no son inyectivos o sobre, **en una categoría un morfismo puede**

ser simultáneamente un monomorfismo y un epimorfismo (como en los ejemplos 6.4.11 y 6.4.23) **sin ser un isomorfismo**. Sin embargo, la recíproca de esta afirmación es válida:

Lema 6.4.30. *Sea \mathcal{C} una categoría y $f \in \text{Hom}_{\mathcal{C}}(A, B)$ un isomorfismo. Entonces f es un monomorfismo y un epimorfismo.*

Demostración. Probaremos que si f es un isomorfismo, entonces es un monomorfismo.

Sean $g, h \in \text{Hom}_{\mathcal{C}}(C, A)$ tales que $f \circ g = f \circ h$. Entonces:

$$g = \text{id}_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ (f \circ h) = (f^{-1} \circ f) \circ h = \text{id}_A \circ h = h.$$

La prueba de que f es un epimorfismo es similar y la dejamos como **ejercicio**. □

Ejemplo 6.4.31. En Poset, un morfismo biyectivo no necesariamente es un isomorfismo En efecto, hemos visto en el Ejemplo 2.5.4 que $f = \text{Id} : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$ es un morfismo de orden, y por lo tanto un morfismo en Poset, que es biyectivo. Sin embargo f no es un isomorfismo de orden, y por lo tanto no es un isomorfismo en Poset. ■

6.5. Objetos iniciales, terminales y nulos

A partir de esta sección comenzaremos con lo que en teoría de categorías se denominan *propiedades y construcciones universales*. Como ya hemos visto, es posible construir analogías y generalizar propiedades conocidas de los conjuntos y funciones entre conjuntos a otras colecciones de objetos y morfismos abstractos. Una construcción universal, en términos generales que especificaremos más adelante, se basa en relaciones entre objetos y morfismos, normalmente a través de diagramas, que establecen la existencia de nuevos objetos en cualquier categoría que las verifique.

Para comenzar, introducimos las nociones de objetos *iniciales* y *terminales*.

Definición 6.5.1. *Sea \mathcal{C} una categoría. Un objeto $0 \in \text{ob } \mathcal{C}$ se dice un **objeto inicial** si para cada objeto A de \mathcal{C} existe un único morfismo $f : 0 \rightarrow A$. Un objeto $1 \in \text{ob } \mathcal{C}$ se dice un **objeto terminal** si para cada objeto A de \mathcal{C} existe un único morfismo $g : A \rightarrow 1$. Un objeto en \mathcal{C} se dice un **objeto nulo** u **objeto cero** si es inicial y terminal.*

Ejemplo 6.5.2. Objetos iniciales y terminales en Set. En Set existe un único objeto inicial, el conjunto vacío, y cada conjunto de un único elemento es un objeto terminal (ver Ejemplo 6.2.4). ■

Ejemplo 6.5.3. Objetos iniciales y terminales en Grp. Consideremos un grupo trivial $0 = \{e\}$ es decir, un grupo que consta de un único elemento, que necesariamente es la identidad. Para cualquier grupo, existe un único homomorfismo de grupos $f : 0 \rightarrow G$, dado que debe verificarse necesariamente $f(0) = e_G$. Por lo tanto 0 es un objeto inicial (observemos que cualquier grupo de orden 1 es un objeto inicial, y estos grupos son todos isomorfos entre sí). Por otra parte, 0 también es un objeto terminal, dado que $g : G \rightarrow 0$ tal que $g(x) = e$ para cada $x \in G$ es un homomorfismo de grupos (y el único posible de G a 0). Luego Grp tiene objetos nulos que son los grupos triviales. ■

Ejemplo 6.5.4. Objetos iniciales y terminales en Boole. Consideremos la categoría Boole de álgebras de Boole: los objetos son álgebras de Boole y los morfismos son morfismos de álgebras de Boole (recordemos que un álgebra de Boole es un retículo acotado, complementado y distributivo). Consideremos el álgebra de Boole de dos elementos $B = \{0, 1\}$ con el orden usual. Entonces B es un elemento inicial en Boole. En efecto, dado cualquier álgebra de Boole $(B', \vee, \wedge, 0', 1')$, $f : B \rightarrow B'$ tal que $f(0) = 0'$, $f(1) = 1'$ es el único morfismo de álgebras de Boole posible entre B y B' . ■

Ejemplo 6.5.5. Consideremos un poset P y la categoría \mathcal{C}_P asociada. \mathcal{C}_P tendrá un objeto inicial si existe un elemento $x \in P$ tal que $x \preceq y$ para cada $y \in P$, esto es, si P tiene un mínimo. Análogamente, \mathcal{C}_P tendrá un objeto terminal si P tiene un máximo. ■

Ejemplo 6.5.6. Consideremos la categoría Vect de espacios vectoriales reales. Entonces $\{0\}$ es un objeto nulo. En efecto, existe un único morfismo de $\{0\}$ en cualquier espacio vectorial V : la transformación lineal que envía 0 en el 0 de V . Por otra parte, la transformación lineal nula que manda todo V en 0 es el único morfismo de V a $\{0\}$. Por lo tanto $\{0\}$ es un objeto inicial y terminal de Vect. ■

En toda categoría, los objetos iniciales y finales son únicos salvo isomorfismo. Esto es:

Teorema 6.5.7. Sea \mathcal{C} una categoría y sean $0, 0' \in \text{ob } \mathcal{C}$ objetos iniciales de \mathcal{C} . Entonces 0 es un objeto isomorfo a $0'$.

Demostración. Como 0 es un objeto inicial y $0' \in \text{ob } \mathcal{C}$, existe un único morfismo $f : 0 \rightarrow 0'$. Como también $0'$ es inicial y $0 \in \text{ob } \mathcal{C}$, existe un único morfismo $g : 0' \rightarrow 0$.

Luego $g \circ f : 0 \rightarrow 0$ y $f \circ g : 0' \rightarrow 0'$ son morfismos en \mathcal{C} . Pero como 0 es inicial, en particular existe un único morfismo de 0 en 0 , que necesariamente es la identidad id_0 . Luego $g \circ f = \text{id}_0$. De manera análoga, $f \circ g = \text{id}_{0'}$. Por lo tanto f (y g) son isomorfismos en \mathcal{C} , y 0 y $0'$ son objetos isomorfos. □

De manera completamente análoga se prueba que:

Teorema 6.5.8. Sea \mathcal{C} una categoría y sean $1, 1' \in \text{ob } \mathcal{C}$ objetos terminales de \mathcal{C} . Entonces 1 es un objeto isomorfo a $1'$.

6.6. Productos y coproductos

A continuación intentaremos definir el producto $A \times B$ de dos objetos en una categoría. Comencemos observando que en Set el producto $A \times B$ de dos conjuntos (objetos de Set) tiene un sentido propio: es un nuevo conjunto, formado por los pares ordenados (a, b) donde a es un elemento de A y b es un elemento de B . Esta misma construcción puede hacerse en cualquier categoría donde los objetos son conjuntos, y obtener un nuevo objeto de la misma categoría: el producto de dos posets es un poset, de dos retículos es un retículo, de dos grupos es un grupo, etc. Ahora bien, en una categoría arbitraria \mathcal{C} , esta definición carece de sentido, dado que sus objetos pueden no ser conjuntos, y por lo tanto no tener elementos. Necesitamos entonces caracterizar de alguna manera el producto cartesiano recurriendo solo a objetos y morfismos. Ya hemos encontrado una propiedad que caracteriza (salvo isomorfismos) el producto de dos grupos a

partir de la existencia de un homomorfismo que hace conmutativo un cierto diagrama. Más precisamente, recordemos que si G y H son dos grupos, el grupo producto $G \times H$ está completamente caracterizado por las siguientes propiedades:

- existen dos homomorfismos de grupo $\pi_G : G \times H \rightarrow G$, $\pi_H : G \times H \rightarrow H$.
- Para cada grupo K y cada par de homomorfismos de grupo $\varphi : K \rightarrow G$ y $\rho : K \rightarrow H$, existe un único homomorfismo $\Psi = \varphi \times \rho : K \rightarrow G \times H$ que hace conmutativo el diagrama

$$\begin{array}{ccccc} & & K & & \\ & \swarrow \varphi & \downarrow \Psi & \searrow \rho & \\ G & \xleftarrow{\pi_G} & G \times H & \xrightarrow{\pi_H} & H \end{array}$$

Más aún, el Teorema 5.5.6 establece que el producto es el único grupo con esta propiedad salvo isomorfismos.

Esta caracterización puede generalizarse a cualquier categoría:

Definición 6.6.1. Sea \mathcal{C} una categoría y A, B objetos de \mathcal{C} . Un **producto** de A y B en \mathcal{C} es una terna $(A \times B, \pi_A, \pi_B)$ tales que:

- $A \times B \in \text{ob } \mathcal{C}$, $\pi_A \in \text{Hom}(A \times B, A)$ y $\pi_B \in \text{Hom}(A \times B, B)$.

y se satisface la siguiente propiedad universal:

- para todo objeto C y para todo par de morfismos $f : C \rightarrow A$, $g : C \rightarrow B$, existe un único morfismo $\langle f, g \rangle : C \rightarrow A \times B$ tal que el siguiente diagrama conmuta

$$(6.7) \quad \begin{array}{ccccc} & & C & & \\ & \swarrow f & \downarrow \exists! \langle f, g \rangle & \searrow g & \\ A & \xleftarrow{\pi_A} & A \times B & \xrightarrow{\pi_B} & B \end{array}$$

Si en \mathcal{C} existe el producto $(A \times B, \pi_A, \pi_B)$ para cualquier par de objetos A y B , decimos que \mathcal{C} es **una categoría con productos**.

Ejemplo 6.6.2. Productos en Set. Sean A y B dos conjuntos. Observemos que existen dos funciones naturales que vinculan $A \times B$ con A y B , las proyecciones $\pi_A : A \times B \rightarrow A$ y $\pi_B : A \times B \rightarrow B$, definidas respectivamente como

$$\pi_A(a, b) = a, \quad \pi_B(a, b) = b.$$

Por otra parte, si C es un conjunto cualquiera y $f : C \rightarrow A$, $g : C \rightarrow B$ son funciones cualesquiera, está bien definida una función

$$\langle f, g \rangle : C \rightarrow A \times B, \quad \langle f, g \rangle(c) = (f(c), g(c))$$

que hace que el siguiente diagrama sea conmutativo:

$$(6.8) \quad \begin{array}{ccccc} & & C & & \\ & f \swarrow & \downarrow \langle f, g \rangle & \searrow g & \\ A & \xleftarrow{\pi_A} & A \times B & \xrightarrow{\pi_B} & B \end{array}$$

esto es,

$$\pi_A \circ \langle f, g \rangle = f, \quad \pi_B \circ \langle f, g \rangle = g.$$

La función $\langle f, g \rangle$ es la única con esta propiedad. En efecto, sea $F : C \rightarrow A \times B$ y pongamos $F(c) = (F_1(c), F_2(c))$. Si F verifica que $\pi_A \circ F = f$ y $\pi_B \circ F = g$ (es decir, hace conmutativo el diagrama (6.8)), entonces $F_1(c) = \pi_A(F(c)) = f(c)$ y $F_2(c) = \pi_B(F(c)) = g(c)$. Luego $F(c) = (f(c), g(c)) = \langle f, g \rangle(c)$ para cada $c \in C$, y por lo tanto $F = \langle f, g \rangle$. ■

En la Definición 6.6.1 hablamos de *un* producto de A y B . En efecto, en una categoría pueden existir distintos objetos que la verifiquen. Ya hemos visto en el Teorema 5.5.6, que cualquier grupo que sea un producto de A y B en Grp debe ser isomorfo al grupo producto $A \times B$. Esto ocurre en cualquier categoría:

Teorema 6.6.3. *Sea \mathcal{C} una categoría y sean A y B dos objetos de \mathcal{C} . Si existe el producto $(A \times B, \pi_A, \pi_B)$, éste es único salvo isomorfismos.*

Demostración. Sea (P, π_A, π_B) y $(P', \tilde{\pi}_A, \tilde{\pi}_B)$ que satisfacen la Definición 6.6.1 del producto de A y B . Si $C \in \text{ob } \mathcal{C}$ y $f \in \text{Hom}(C, A)$, $g \in \text{Hom}(C, B)$, denotemos por $\langle f, g \rangle$ y $\widetilde{\langle f, g \rangle}$ a los únicos morfismos que hacen conmutativos, respectivamente, los siguientes diagramas:

$$(6.9) \quad \begin{array}{ccccc} & & C & & \\ & f \swarrow & \downarrow \langle f, g \rangle & \searrow g & \\ A & \xleftarrow{\pi_A} & P & \xrightarrow{\pi_B} & B \end{array} \quad \begin{array}{ccccc} & & C & & \\ & f \swarrow & \downarrow \widetilde{\langle f, g \rangle} & \searrow g & \\ A & \xleftarrow{\tilde{\pi}_A} & P' & \xrightarrow{\tilde{\pi}_B} & B \end{array}$$

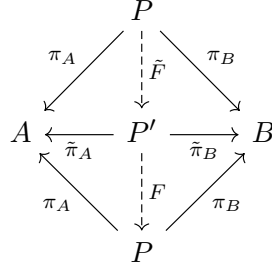
Pongamos P' en el lugar de C en el diagrama de la izquierda de (6.9) con las funciones $f = \tilde{\pi}_A$ y $g = \tilde{\pi}_B$ y consideremos la función $F = \langle \pi_A, \pi_B \rangle : P' \rightarrow P$. Entonces

$$(6.10) \quad \pi_A \circ F = \tilde{\pi}_A, \quad \pi_B \circ F = \tilde{\pi}_B.$$

Pongamos ahora P en el lugar de C en el diagrama de la derecha de (6.9) con las funciones $f = \pi_A$ y $g = \pi_B$ y consideremos la función $\tilde{F} : P \rightarrow P'$, $\tilde{F} = \widetilde{\langle \pi_A, \pi_B \rangle}$ correspondiente. Entonces

$$(6.11) \quad \tilde{\pi}_A \circ \tilde{F} = \pi_A, \quad \tilde{\pi}_B \circ \tilde{F} = \pi_B.$$

Consideremos ahora el siguiente diagrama:



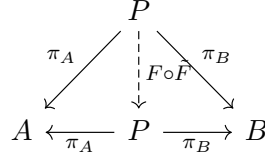
Observemos que de (6.10) y (6.11) resulta que

$$(6.12) \quad \pi_B \circ (F \circ \tilde{F}) = (\pi_B \circ F) \circ \tilde{F} = \tilde{\pi}_B \circ \tilde{F} = \pi_B$$

y de manera análoga,

$$(6.13) \quad \pi_A \circ (F \circ \tilde{F}) = \pi_A$$

De (6.12) y (6.13), si ponemos $C = P$ en 6.7, con $f = \pi_A$, $g = \pi_B$, $F \circ \tilde{F}$ hace conmutativo el diagrama



Pero trivialmente, id_P también hace conmutativo el diagrama. Luego por unicidad deberá ser

$$F \circ \tilde{F} = \langle \pi_A, \pi_B \rangle = \text{id}_P.$$

De manera completamente análoga se prueba que $\tilde{F} \circ F = \text{id}'_P$, y por lo tanto F es un isomorfismo en \mathcal{C} . Luego P y P' son objetos isomorfos. \square

Ejemplo 6.6.4. Como hemos visto antes de dar la definición 6.6.1, el producto en Set entre dos objetos A y B es $(A \times B, \pi_A, \pi_B)$, donde $A \times B$ es el producto cartesiano usual y π_A, π_B son las proyecciones canónicas a cada factor. Veamos ahora otra forma (isomorfa) de presentar al producto de dos conjuntos en Set . Sea

$$\mathcal{F} = \{h : \{1, 2\} \rightarrow A \cup B : h(1) \in A, h(2) \in B\}.$$

Definamos las proyecciones $\tilde{\pi}_A : \mathcal{F} \rightarrow A$, $\tilde{\pi}_B : \mathcal{F} \rightarrow B$ por

$$\tilde{\pi}_A(h) = h(1), \quad \tilde{\pi}_B(h) = h(2).$$

Si C es un conjunto y $f : C \rightarrow A$, $g : C \rightarrow B$ son dos funciones cualesquiera, pongamos

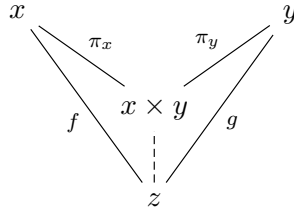
$$\langle f, g \rangle : C \rightarrow \mathcal{F}, \quad \langle f, g \rangle(c) = h : \{1, 2\} \rightarrow A \cup B / h(1) = f(c), h(2) = g(c)$$

de donde resulta claro que $\langle f, g \rangle$ es la única función de C en \mathcal{F} tal que $\tilde{\pi}_A \circ \langle f, g \rangle = f$, $\tilde{\pi}_B \circ \langle f, g \rangle = g$. Luego \mathcal{F} es isomorfo a $A \times B$, y es un producto de A y B . \blacksquare

Ejemplo 6.6.5. En Sgrp , Mon y Grp , los productos entre dos objetos siempre existen y son el semigrupo, monoide o grupo producto respectivamente. En efecto, es fácil ver que las proyecciones de $A \times B$ en A y B son morfismos de semigrupos, monoides o grupos respectivamente, y que $(A \times B, \pi_A, \pi_B)$ satisface la propiedad universal del producto. En realidad todas las categorías del Ejemplo 6.2.5 son categorías con productos. ■

Ejemplo 6.6.6. Consideremos un poset P y sea \mathcal{C}_P la categoría asociada. Sean $x, y \in P$ dos objetos de \mathcal{C}_P . Supongamos que existe el producto $(x \times y, \pi_x, \pi_y)$. Recordemos que un morfismo en \mathcal{C}_P no es más que un par de elementos (a, b) tal que $a \preceq b$. Por lo tanto, para que exista un morfismo $\pi_x : x \times y \rightarrow x$, deberá ser $x \times y \preceq x$, en cuyo caso $\pi_x = (x \times y, x)$. De manera análoga, debemos tener $x \times y \preceq y$ y $\pi_y = (x \times y, y)$. Por lo tanto $x \times y$ debe ser una cota inferior en P del conjunto $\{x, y\}$.

En este caso, la propiedad universal del producto puede interpretarse a través de un diagrama de Hasse en P . En efecto, supongamos que $z \in P$ es un objeto de \mathcal{C}_P cualquiera para el cual existen dos morfismos $f : z \rightarrow x$ y $g : z \rightarrow y$. Esto simplemente quiere decir que $z \preceq x$, $z \preceq y$ y $f = (z, x)$, $g = (z, y)$. Como estamos suponiendo que el producto existe, deberá existir un único morfismo $\langle f, g \rangle : z \rightarrow x \times y$, pero este morfismo no puede ser otro que $(z, x \times y)$, o sea, $z \preceq x \times y$:



Observemos que para los morfismos que tenemos,

$$\pi_x \circ \langle f, g \rangle = (x \times y, x) \circ (z, x \times y) = (z, x) = f,$$

$$\pi_y \circ \langle f, g \rangle = (x \times y, y) \circ (z, x \times y) = (z, y) = g.$$

Es decir, que de existir, el producto $x \times y$ debe ser una cota inferior de $\{x, y\}$ (para que existan los morfismos π_x y π_y), y tal que para cualquier otra cota inferior z de $\{x, y\}$ (que son los objetos para los cuales existen morfismos a x y a y), $z \preceq x \times y$. O sea, existe el producto de x e y en \mathcal{C}_P si y sólo si $\{x, y\}$ tiene ínfimo. En este caso, $x \times y = \inf\{x, y\}$.

Si ahora consideramos el poset dual P^* , es decir (P, \succeq) , con un razonamiento análogo al anterior veremos que \mathcal{C}_{P^*} (ver el Ejemplo 6.2.12) admite el producto $x \times y$ si y sólo si existe $\sup\{x, y\}$.

Por lo tanto tendremos que un poset P es un retículo si y sólo si \mathcal{C}_P y \mathcal{C}_{P^*} son categorías con productos. En ese caso, las operaciones join y meet están dadas por $x \wedge y = x \times y$ y $x \vee y = x \times^* y$, donde \times^* indica el producto en \mathcal{C}_{P^*} . ■

Sea \mathcal{C} una categoría y A, B, C, D objetos de \mathcal{C} para los cuales existen los productos $(A \times B, \pi_A, \pi_B)$ y $(C \times D, \pi_C, \pi_D)$. Sean $f : A \rightarrow C$ y $g : B \rightarrow D$ son dos morfismos de \mathcal{C} . Podemos considerar entonces el siguiente diagrama:

$$\begin{array}{ccccc}
 A & \xleftarrow{\pi_A} & A \times B & \xrightarrow{\pi_B} & B \\
 f \downarrow & f \circ \pi_A \swarrow & & \searrow g \circ \pi_B & \downarrow g \\
 C & \xleftarrow{\pi_C} & C \times D & \xrightarrow{\pi_D} & D
 \end{array}$$

Aplicando la definición del producto $C \times D$, existe un único morfismo $f \times g = \langle f \circ \pi_A, g \circ \pi_B \rangle$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccccc}
 & & A \times B & & \\
 & f \circ \pi_A \swarrow & \downarrow f \times g & \searrow g \circ \pi_B & \\
 C & \xleftarrow{\pi_C} & C \times D & \xrightarrow{\pi_D} & D
 \end{array}$$

Definición 6.6.7. Sea \mathcal{C} una categoría y A, B, C, D objetos de \mathcal{C} para los cuales existen los productos $(A \times B, \pi_A, \pi_B)$ y $(C \times D, \pi_C, \pi_D)$. Sean $f : A \rightarrow C$ y $g : B \rightarrow D$ son dos morfismos de \mathcal{C} . El morfismo $f \times g = \langle f \circ \pi_A, g \circ \pi_B \rangle : A \times B \rightarrow C \times D$, se denomina el **morfismo producto** de f y g .

Ejemplo 6.6.8. En Set , si $f : A \rightarrow C$ y $g : B \rightarrow D$ son dos funciones, entonces $f \times g(a, b) = (f(a), g(b))$ como se comprueba fácilmente de la definición. Lo mismo ocurre para aquellas categorías donde los productos son los productos cartesianos usuales. ■

Ejemplo 6.6.9. Consideremos un retículo L y sea \mathcal{C}_L la categoría asociada. Sean $x, y, z, w \in L = \text{ob } \mathcal{C}_L$. Entonces existen los productos $x \times y = x \wedge y$ y $z \times w = z \wedge w$. Si existen morfismos $f : x \rightarrow z$ y $g : y \rightarrow w$ es porque $x \preceq z$ y $y \preceq w$. Luego $x \wedge y \preceq z \wedge w$ y por lo tanto existe el morfismo (único) $f \times g : x \times y \rightarrow z \times w$. Esto es, $f \times g = (x \wedge y, z \wedge w)$. ■

La existencia de un morfismo producto permite definir un funtor particular en las categorías con productos:

Ejemplo 6.6.10. Los funtores producto \times_A y \times^A . Sea \mathcal{C} una categoría con productos binarios. Fijemos un objeto $A \in \mathcal{C}$ y definamos $\times_A : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{C}$ tal que $\times_A(B) = A \times B$. Si $f \in \text{Hom}(B, C)$, podemos considerar el morfismo producto $\text{id}_A \times f : A \times B \rightarrow A \times C$ y por lo tanto queda definida una función de clases $\times_A : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{C}$ tal que $\times_A(f) = \text{id}_A \times f$. Claramente \times_A verifica la condición 1 de la Definición 6.3.1. Veamos que se verifican las otras dos.

Recordemos que dado $f \in \text{Hom}(B, C)$, $f \circ \pi_B : A \times B \rightarrow C$ y $\text{id}_A \times f$ es el único morfismo que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccccc}
 A & \xleftarrow{\pi_A} & A \times B & \xrightarrow{\pi_B} & B \\
 \text{id}_A \downarrow & \pi_A \swarrow & \downarrow \text{id}_A \times f & \searrow f \circ \pi_B & \downarrow f \\
 A & \xleftarrow{\pi_A} & A \times C & \xrightarrow{\pi_C} & C
 \end{array}
 \qquad
 \begin{array}{ccccc}
 & & A \times B & & \\
 & \pi_A \swarrow & \downarrow \text{id}_A \times f & \searrow f \circ \pi_B & \\
 A & \xleftarrow{\pi_A} & A \times C & \xrightarrow{\pi_C} & C
 \end{array}$$

esto es, $\text{id}_A \times f = \langle \pi_A, f \circ \pi_B \rangle$.

Como $\text{id}_B \circ \pi_B = \pi_B$, $\text{id}_A \times \text{id}_B$ es el único morfismo que hace conmutativo el diagrama

$$\begin{array}{ccccc} & & A \times B & & \\ & \swarrow \pi_A & \downarrow \text{id}_A \times \text{id}_B & \searrow \pi_B & \\ A & \xleftarrow{\pi_A} & A \times B & \xrightarrow{\pi_B} & B \end{array}$$

Pero es evidente que $\text{id}_{A \times B}$ también hace conmutativo el diagrama, de donde

$$\text{id}_A \times \text{id}_B = \text{id}_{A \times B} \implies \times_A(\text{id}_B) = \text{id}_{\times_A(B)}$$

y entonces vale la condición 2. Si ahora $f \in \text{Hom}(B, C)$ y $g \in \text{Hom}(C, D)$, tenemos que $(\text{id}_A \times g) \circ (\text{id}_A \times f)$ hace conmutativo el diagrama:

$$\begin{array}{ccccc} & & A \times B & & \\ & \swarrow \pi_A & \downarrow \text{id}_A \times f & \searrow f \circ \pi_B & \\ A & \xleftarrow{\pi_A} & A \times C & \xrightarrow{\pi_C} & C \\ \downarrow \text{id}_A & \swarrow \pi_A & \downarrow \text{id}_A \times g & \searrow g \circ \pi_C & \downarrow g \\ A & \xleftarrow{\pi_A} & A \times D & \xrightarrow{\pi_D} & D \end{array}$$

En particular,

$$(6.14) \quad \pi_D \circ [(\text{id}_A \times g) \circ (\text{id}_A \times f)] = g \circ (f \circ \pi_B) = (g \circ f) \circ \pi_B.$$

Ahora bien, $\Phi = \text{id}_A \times (g \circ f)$ es el único morfismo que hace conmutativo el diagrama

$$\begin{array}{ccccc} & & A \times B & & \\ & \swarrow \pi_A & \downarrow \Phi & \searrow (g \circ f) \circ \pi_B & \\ A & \xleftarrow{\pi_A} & A \times D & \xrightarrow{\pi_D} & D \end{array}$$

pero por (6.14) también hace conmutativo el diagrama, de donde

$$(\text{id}_A \times g) \circ (\text{id}_A \times f) = \text{id}_A \times (g \circ f) \implies (\times_A(g)) \circ \times_A(f) = \times_A(g \circ f)$$

y por lo tanto se verifica la condición 3 de la Definición 6.3.1. Luego \times_A es un funtor de \mathcal{C} en \mathcal{C} . Nuevamente, el funtor \times_A muchas veces se denota por $A \times -$.

De manera completamente análoga, puede probarse que $s \times^A = - \times A$ dado por $\times^A(B) = B \times A$ para cada objeto B de \mathcal{C} y si $f \in \text{Hom}(B, C)$, $\times^A(f) = f \times \text{id}_A \in \text{Hom}(B \times A, C \times A)$ es un funtor covariante. Dejamos los detalles como ejercicio. ■

El Ejemplo 6.6.6 resulta ilustrativo para la introducción del siguiente concepto universal, el de *coproductos*. Como hemos mencionado en el Ejemplo 6.3.17, la categoría \mathcal{C}_{P^*} es una categoría isomorfa a \mathcal{C}_P^{op} , y el producto en \mathcal{C}_{P^*} es útil para caracterizar ciertas propiedades de P que no se obtienen con el producto

en \mathcal{C}_P . Como los objetos de \mathcal{C}_P y $\mathcal{C}_P^{op} \simeq \mathcal{C}_{P^*}$ son los mismos y los morfismos son las flechas revertidas, podemos formular cualquier propiedad en una de ellas en términos de propiedades en la otra.

Lo mismo ocurre para cualquier categoría \mathcal{C} y su opuesta \mathcal{C}^{op} . Podemos por lo tanto considerar el producto en \mathcal{C}^{op} y expresarlo en términos de objetos y flechas en \mathcal{C} . Esto da lugar al concepto de **coproducto**:

Definición 6.6.11. Sea \mathcal{C} una categoría y A, B objetos de \mathcal{C} . El **coproducto** de A y B en \mathcal{C} es una terna

$(A + B, i_A, i_B)$ tales que:

- $i_A \in \text{Hom}(A, A + B)$ y $i_B \in \text{Hom}(B, A + B)$.

y se satisface la siguiente propiedad universal:

- para todo objeto C y para todo par de morfismos $f : A \rightarrow C$, $g : B \rightarrow C$, existe un único morfismo $[f, g] : A + B \rightarrow C$ tal que el siguiente diagrama conmuta

$$(6.15) \quad \begin{array}{ccccc} A & \xrightarrow{i_A} & A + B & \xleftarrow{i_B} & B \\ & \searrow f & \downarrow \exists! [f, g] & \swarrow g & \\ & & C & & \end{array}$$

Si en \mathcal{C} existe el coproducto $(A + B, i_A, i_B)$ para cualquier par de objetos A y B , decimos que \mathcal{C} es **una categoría con coproductos**.

Teorema 6.6.12. Sea \mathcal{C} una categoría y sean $A, B \in \text{ob } \mathcal{C}$. Existe el coproducto de A y B en \mathcal{C} si y sólo si existe el producto de $A \times B$ en \mathcal{C}^{op} . Más precisamente, $(A + B, i_A, i_B)$ es el coproducto dos objetos A y B en \mathcal{C} si y sólo si $(A \times B, \pi_A, \pi_B)$ es el producto de A y B en \mathcal{C}^{op} .

Demostración. Supongamos que en \mathcal{C} existe el coproducto $(A + B, i_A, i_B)$ de dos objetos A y B . Denotemos $A \times^{op} B = A + B$, $\pi_A^{op} = i_A$ y $\pi_B^{op} = i_B$. Observemos que $A \times^{op} B$ es un objeto en \mathcal{C}^{op} , y

$$\pi_A \in \text{Hom}^{op}(A \times^{op} B, A), \quad \pi_B \in \text{Hom}^{op}(A \times^{op} B, B).$$

Veremos que $(A \times^{op} B, \pi_A^{op}, \pi_B^{op})$ es efectivamente un producto de A y B en \mathcal{C}^{op} . Para ello, consideremos un objeto C cualquiera de \mathcal{C}^{op} y sean $f \in \text{Hom}^{op}(A, C)$, $g \in \text{Hom}^{op}(B, C)$. Entonces C es también un objeto de \mathcal{C} y $f \in \text{Hom}(C, A)$, $g \in \text{Hom}(C, B)$.

Ahora bien, en \mathcal{C} existe un único morfismo $[f, g] : A + B \rightarrow C$ tal que $[f, g] \circ i_A = f$, $[f, g] \circ i_B = g$. Luego $[f, g] \in \text{Hom}^{op}(C, A \times^{op} B)$ verifica

$$\pi_A^{op} \circ^{op} [f, g] = [f, g] \circ \pi_A^{op} = [f, g] \circ i_A = f, \quad \pi_B^{op} \circ^{op} [f, g] = g.$$

Por otra parte, si existiese otro morfismo $F \in \text{Hom}^{op}(C, A \times^{op} B)$ tal que $\pi_A^{op} \circ^{op} F = f$ y $\pi_B^{op} \circ^{op} F = g$, entonces tendríamos que $F \in \text{Hom}(A + B, C)$ verifica $F \circ i_A = f$ y $F \circ i_B = g$, con lo cual $F = [f, g]$.

Concluimos entonces que $[f, g]$ es el único morfismo en $\text{Hom}^{op}(C, A \times^{op} B)$ que hace conmutativo el diagrama (6.7), y por lo tanto $\langle f, g \rangle^{op} = [f, g]$.

La prueba de la recíproca es similar. Dejamos los detalles como **ejercicio**. \square

A partir del Teorema 6.6.12, del Lema 6.6.3 y del Ejercicio 18 de este capítulo, obtenemos inmediatamente:

Lema 6.6.13. *Sea \mathcal{C} una categoría y A, B objetos en \mathcal{C} . Si existe el coproducto $(A + B, i_A, i_B)$, éste es único salvo isomorfismos.*

Ejemplo 6.6.14. Como vimos en el Ejemplo 6.6.6, si P es un poset, un coproducto en \mathcal{C}_P es un producto en \mathcal{C}_P^{op} . Como \mathcal{C}_P^{op} es isomorfa a \mathcal{C}_{P^*} , del Ejercicio 22 de este capítulo, tenemos que existe el coproducto en \mathcal{C}_P si y sólo si existe el producto en \mathcal{C}_P^{op} . Luego dados $x, y \in P = \text{ob } \mathcal{C}_P$, existe el coproducto $x + y$ si y sólo si $\{x, y\}$ tiene supremo. Por lo tanto \mathcal{C}_P es una categoría con productos y coproductos si y sólo si P es un retículo. \blacksquare

Ejemplo 6.6.15. Coproducto en Set. Veamos ahora que Set es una categoría con coproductos. Sean A y B dos conjuntos y sea

$$A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$$

su unión disjunta (es decir, 0 y 1 son parámetros que distinguen los elementos de A de los de B , y en caso que tuviésemos $A \cap B \neq \emptyset$ permite considerar estos elementos comunes como elementos distintos en la unión). Podemos entonces considerar las inclusiones

$$i_A : A \rightarrow A \sqcup B, \quad i_A(a) = (a, 0), \quad i_B : B \rightarrow A \sqcup B, \quad i_B(b) = (b, 1).$$

Para ver que $(A \sqcup B, i_A, i_B)$ es un coproducto en Set, consideremos un conjunto C cualquiera y sean $f : A \rightarrow C, g : B \rightarrow C$ dos funciones cualesquiera. Definamos $[f, g] : A \sqcup B \rightarrow C$ por

$$[f, g](x, j) = \begin{cases} f(x) & \text{si } j = 0 \\ g(x) & \text{si } j = 1. \end{cases}$$

Es evidente entonces que $[f, g] \circ i_A = f$ y $[f, g] \circ i_B = g$.

Por otra parte, si $F : A \sqcup B \rightarrow C$ es una función tal que $F \circ i_A = f$ y $F \circ i_B = g$, entonces

$$F(x, 0) = F \circ i_A(x) = f(x) = [f, g](x, 0)$$

y análogamente $F(x, 1) = [f, g](x, 1)$. Por lo tanto $[f, g]$ es la única función que hace conmutativo el diagrama (6.15) como queríamos ver. \blacksquare

Ejemplo 6.6.16. Coproducto en Ab. Sean $(A, +), (B, +)$ dos grupos abelianos (en estos grupos, es usual utilizar la notación aditiva, aunque la operación podría ser un producto). En este caso, el grupo producto $A \times B$ suele denotarse como $A + B$ y se denomina **suma directa** de A y B . Podemos considerar los morfismos $i_A : A \rightarrow A + B$ e $i_B : B \rightarrow A + B$ dados por

$$i_A(a) = (a, 0_B), \quad i_B(b) = (0_A, b)$$

donde 0_A y 0_B son los neutros de A y B respectivamente (que en el caso de notación aditiva suelen denotarse por 0). Veamos que $(A + B, i_A, i_B)$ es un coproducto de A y B .

Consideremos entonces un grupo abeliano C cualquiera y sean $f : A \rightarrow C$, $g : B \rightarrow C$ dos homomorfismos. Pongamos $[f, g] : A + B \rightarrow C$ por

$$[f, g](a, b) = f(a) + g(b).$$

Entonces

$$[f, g] \circ i_A(a) = [f, g](a, 0_B) = f(a) + g(0_B) = f(a) + 0_C = f(a)$$

y análogamente $[f, g] \circ i_B = g$.

Si ahora $F : A + B \rightarrow C$ es un homomorfismo tal que $F \circ i_A = f$, $F \circ i_B = g$, entonces

$$F(a, b) = F((a, 0_B) + (0_A, b)) = F(a, 0_B) + F(0_A, b) = F(i_A(a)) + F(i_B(b)) = f(a) + g(b) = [f, g](a, b)$$

lo que concluye la prueba. ■

Ejemplo 6.6.17. Coproducto en Grp. Sean ahora (A, \cdot) y (B, \cdot) dos grupos cualesquiera. Intentemos repetir la construcción que hicimos para Ab. En este caso, deberíamos considerar el grupo producto $A \times B$ con las inclusiones $i_A : A \rightarrow A \times B$, $i_A(a) = (a, e_B)$ y $i_B : B \rightarrow A \times B$, $i_B(b) = (e_A, b)$. Sin importar que A y B no sean abelianos, i_A y i_B son homomorfismos bien definidos. Sin embargo, si ahora consideramos un grupo C cualquiera y dos homomorfismos $f : A \rightarrow C$, $g : B \rightarrow B$, la función $[f, g](a, b) = f(a)g(b)$ ya no es un homomorfismo si los grupos no son abelianos, como es fácil comprobar.

Por lo tanto $(A \times B, i_A, i_B)$ no será, en general, un coproducto en Grp. En efecto, a partir del Teorema 5.5.23, tenemos que si A y B son grupos, el coproducto de A y B en Grp es el producto libre $A * B$. ■

Las nociones de producto y coproducto pueden generalizarse a una familia arbitraria de objetos:

Definición 6.6.18. Si $\{A_k\}_{k \in K}$ es una familia de objetos en una categoría \mathcal{C} , indexada por un conjunto K , un **producto** de $\{A_k\}_{k \in K}$ es un objeto $\prod_{k \in K} A_k$ junto con una familia de morfismos

$$\left\{ \pi_j : \prod_{k \in K} A_k \rightarrow A_j \right\}_{j \in K} \quad \text{que verifican la siguiente propiedad universal:}$$

- para todo objeto C y para toda familia de morfismos $\{f_k : C \rightarrow A_k\}_{k \in K}$, existe un único morfismo

$$\langle f_k \rangle_{k \in K} : C \rightarrow \prod_{k \in K} A_k$$

tal que para cada $j \in K$, el siguiente diagrama conmuta:

$$(6.16) \quad \begin{array}{ccc} C & & \\ \downarrow \exists! \langle f_k \rangle_{k \in K} & \searrow f_j & \\ \prod_{k \in K} A_k & \xrightarrow{\pi_j} & A_j \end{array}$$

Ejemplo 6.6.19. Producto arbitrario en Set. Encontremos un producto arbitrario en Set. Si tenemos dos conjuntos A_1 y A_2 , ya vimos en el Ejemplo 6.6.4 que el producto de A_1 y A_2 coincide con el producto cartesiano usual junto con las proyecciones canónicas. Es fácil verificar que esta construcción puede generalizarse a una familia finita de conjuntos A_1, A_2, \dots, A_n cuyo producto es el conjunto

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_i \in A_i, \forall i = 1, \dots, n\}$$

junto con las proyecciones $\pi_i : A_1 \times \cdots \times A_n \rightarrow A_i$, $\pi_i(a_1, \dots, a_n) = a_i$. Con una prueba análoga a las anteriores puede verse también que si $\{A_k\}_{k \in \mathbb{N}}$ es una familia numerable de conjuntos, su producto es

$$\prod_{k \in \mathbb{N}} A_k = \{(a_k)_{k \in \mathbb{N}} : a_k \in A_k\}$$

y las proyecciones son las naturales.

¿Pero qué ocurre si ahora tomamos un conjunto K arbitrario de índices? ¿Cómo podemos definir el producto de una familia de conjuntos indexada por ejemplo por $K = \mathbb{R}$ o $K = \mathbb{C}$? Para poder dar este paso será útil recordar la construcción alternativa del producto que vimos en el Ejemplo 6.6.4. En efecto, si $\{A_k\}_{k \in K}$ es una familia de conjuntos indexada por un conjunto K arbitrario, consideremos el conjunto

$$\mathcal{F} = \left\{ h : K \rightarrow \bigcup_{k \in K} A_k : h(k) \in A_k \right\}$$

y sea $\pi_k : \mathcal{F} \rightarrow A_k$, $\pi_k(f) = f(k)$. Entonces dado un conjunto C y una familia de morfismos $\{f_k : C \rightarrow A_k\}_{k \in K}$, la función

$$\langle f_k \rangle_{k \in K}(c) = h : C \rightarrow \prod_{k \in K} A_k / h(k) = f_k(c)$$

es la única función que hace conmutativo el diagrama 6.16. ■

Ejemplo 6.6.20. Producto arbitrario en Grp. Sea ahora $\{G_k\}_{k \in K}$ una familia de grupos. Pongamos

$$G = \{f : K \rightarrow \cup_{k \in K} G_k / f(k) \in G_k\}$$

el producto de los conjuntos G_k . Daremos a este conjunto estructura de grupo. Si $f, g \in G$ ponemos

$$f * g(k) = f(k)g(k)$$

Luego si $f, g, h \in G$,

$$(f * g) * h(k) = (f * g)(k)h(k) = (f(k)g(k))h(k) = f(k)(g(k)h(k)) = f * (g * h)(k)$$

con lo cual $*$ es asociativa.

Pongamos $e : K \rightarrow \cup_{k \in K} G_k$, $e(k) = e_k$ y si $f \in G$, ponemos $f^* : K \rightarrow \cup_{k \in K} G_k$, $f^*(k) = f(k)^{-1}$. Entonces para cada $g \in G$,

$$e * g(k) = e(k)g(k) = e_k g(k) = g(k), \quad g * e(k) = g(k)e(k) = g(k)e_k = g(k)$$

con lo cual e es el elemento neutro de G . Además

$$f * f^*(k) = f(k)f(k)^{-1} = e_k = e(k), \quad f^* * f(k) = f(k)^{-1}f(k) = e_k = e(k)$$

con lo cual todo elemento f de G admite un inverso f^* . Concluimos que $(G, *)$ es un grupo.

Cosideremos ahora las funciones $\pi_k : G \rightarrow G_k$, $\pi_k(f) = f(k)$. Entonces

$$\pi_k(f * g) = f * g(k) = f(k)g(k) = \pi_k(f)\pi_k(g)$$

con lo cual π_k es un morfismo de grupos. A partir de aquí no es difícil verificar que $(G, \{\pi_k\}_{k \in K})$ verifica la propiedad universal del producto en Grp. ■

Definición 6.6.21. Si $\{A_k\}_{k \in K}$ es una familia de objetos en una categoría \mathcal{C} , indexada por un conjunto K , un **coproducto** de $\{A_k\}_{k \in K}$ es un objeto $\bigoplus_{k \in K} A_k$ junto con una familia de morfismos

$\left\{ i_j : A_j \rightarrow \bigoplus_{k \in K} A_k \right\}_{j \in K}$ que verifican la siguiente propiedad universal:

- Para todo objeto C y para toda familia de morfismos $\{f_k : A_k \rightarrow C\}_{k \in K}$, existe un único morfismo

$$[f_k]_{k \in K} : \bigoplus_{k \in K} A_k \rightarrow C$$

tal que para cada $j \in K$, el siguiente diagrama conmuta:

$$\begin{array}{ccc} A_j & \xrightarrow{i_j} & \bigoplus_{k \in K} A_k \\ & \searrow f_j & \downarrow \exists! [f_k]_{k \in K} \\ & & C \end{array}$$

Ejemplo 6.6.22. Coproducto arbitrario en Set. Si $\{X_k\}_{k \in K}$ es una familia indexada de conjuntos, entonces el coproducto de esta familia en Set es la unión disjunta $\bigsqcup_{k \in K} X_k = \bigcup_{k \in K} X_k \times \{k\}$, donde las inclusiones son las funciones $i_j : X_j \rightarrow \bigsqcup_{k \in K} X_k$, $i_j(x)(x, j)$. Dejamos los detalles de la prueba como **ejercicio**. ■

Ejemplo 6.6.23. Coproducto arbitrario en Grp. A partir del Teorema 5.5.23 resulta inmediato que si $\{G_k\}_{k \in K}$ es una familia arbitraria de grupos, entonces el producto libre $\ast_{k \in K} G_k$ es un coproducto de esta familia en Grp. ■

Ejemplo 6.6.24. Retículos completos Sea L un retículo. L se dice **completo** si para cada subconjunto X de L existen $\inf X$ y $\sup X$ (más detalles y propiedades de los retículos completos pueden verse en [6]). No es difícil ver, siguiendo la idea de los ejemplos 6.6.6 y 6.6.14 que L es un retículo completo si y sólo si \mathcal{C}_L es una categoría con productos y coproductos arbitrarios. ■

6.7. Ecualizadores y coecualizadores

Muchos problemas matemáticos pueden modelarse a través del conjunto de soluciones de una ecuación. El caso más simple es aquel en el que intervienen dos funciones $f, g : X \rightarrow Y$, y se desea hallar el conjunto

$$S = \{x \in X : f(x) = g(x)\}$$

Por ejemplo, si $f : G \rightarrow H$ es un homomorfismo de grupos, entonces $\ker(f)$ es un conjunto de este tipo: basta considerar el homomorfismo trivial $g : G \rightarrow H$ tal que $g(x) = e_H$ para cada $x \in G$.

El conjunto S se denomina *ecualizador* de las funciones f y g . Nos interesa definir un concepto análogo para dos morfismos entre objetos de una categoría cualquiera. Pero como los objetos de una categoría no tienen por qué ser conjuntos (ya lo hemos repetido un centenar de veces) la definición del conjunto S no tiene sentido en muchos casos. Por lo tanto, una vez más, debemos caracterizarlo a partir de alguna propiedad universal que involucre estos objetos y estos morfismos.

Observemos que como $S \subseteq X$, podemos considerar la inclusión $i : S \rightarrow X$. Entonces i verifica que $f \circ i = g \circ i$. Supongamos ahora que tenemos un conjunto Z y una función $h : Z \rightarrow X$ tal que $f \circ h = g \circ h$. Esto implica que $h(z) \in S$ para cada $z \in Z$, y por lo tanto podemos definir una nueva función $\tilde{h} : Z \rightarrow S$ (simplemente restringiendo el codominio de h) que verifica que $i \circ \tilde{h} = h$, es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} S & \xrightarrow{i} & X \\ \uparrow \tilde{h} & \nearrow h & \downarrow \\ Z & & \end{array} \quad \begin{array}{c} f \\ \rightrightarrows \\ g \end{array} \quad Y$$

Claramente \tilde{h} es la única función que hace conmutativo el diagrama anterior, pues si $\tilde{h}' : Z \rightarrow S$ es tal que $i \circ \tilde{h}' = h$, entonces $\tilde{h}'(z) = h(z) = \tilde{h}(z)$ para cada $z \in Z$.

Con esta idea en mente, definiremos a continuación el ecualizador de dos morfismos en una categoría arbitraria:

Definición 6.7.1. El *ecualizador* de dos morfismos $f, g : A \rightarrow B$ en una categoría \mathcal{C} es un par (X, e) donde X es un objeto de \mathcal{C} y $e : X \rightarrow A$ es un morfismo de \mathcal{C} tal que:

- $f \circ e = g \circ e$
- para todo objeto X' de \mathcal{C} y todo morfismo $e' : X' \rightarrow A$ tal que $f \circ e' = g \circ e'$, existe un único morfismo $k : X' \rightarrow X$ tal que $e \circ k = e'$

$$\begin{array}{ccc} X & \xrightarrow{e} & A \\ \uparrow \exists! k & \nearrow e' & \downarrow \\ X' & & \end{array} \quad \begin{array}{c} f \\ \rightrightarrows \\ g \end{array} \quad B$$

Ejemplo 6.7.2. Ecualizadores en Set y Poset. Como vimos en la motivación inicial, en Set el ecualizador de $f, g : X \rightarrow Y$ es el par (S, i) donde $S = \{x \in X : f(x) = g(x)\}$ e $i : S \rightarrow X$ es la inclusión.

En Poset, el ecualizador es similar: si P y P' son posets y $f, g : P \rightarrow P'$ son morfismos de posets, entonces $S = \{x \in P : f(x) = g(x)\}$ es un poset con el orden restringido de P y la inclusión $i : S \rightarrow P$ es un morfismo de posets. La propiedad universal se demuestra de manera completamente análoga a la propiedad en Set. ■

Ejemplo 6.7.3. Ecualizadores en Sgrp, Mon y Grp. Sean $f, g : M \rightarrow N$ morfismos de monoides. Entonces

$$S = \{x \in M : f(x) = g(x)\}$$

es un monoide: en efecto si $x, y \in S$, $f(x * y) = f(x) * f(y) = g(x) * g(y) = g(x * y)$, entonces $x * y \in S$. Además, dado que $f(e_M) = e_N = g(e_N)$, $e_M \in S$. Luego S es un submonoide de M y la inclusión $i : S \rightarrow M$ es un morfismo de monoides.

Veamos que (S, i) es un ecualizador de f y g en Mon. Sea M' un monoide y $h : M' \rightarrow M$ un homomorfismo de monoides tal que $f \circ h = g \circ h$. Entonces con el mismo argumento que en Set, tenemos que $h(M') \subseteq S$ y $\tilde{h} : M' \rightarrow S$ dado por $\tilde{h}(x) = h(x)$ es el único homomorfismo de monoides tal que $\tilde{h} \circ i = h$.

De manera completamente análoga pueden encontrarse los ecualizadores en Sgrp y en Grp. ■

Ejemplo 6.7.4. Los ecualizadores no siempre existen Sea G un grupo y sea \mathcal{C}_G la categoría que determina (considerando G como un monoide), es decir, tal que $\text{ob } \mathcal{C}_G = \{\star\}$, $\text{mor } \mathcal{C}_G = \text{Hom}(\star, \star) = G$. Si $f, g : \star \rightarrow \star$ es un morfismo, para que exista un ecualizador de f y g debe existir en primer lugar un morfismo $h : \star \rightarrow \star$ tal que $f \circ h = g \circ h$. Ahora bien, $f, g, h \in G$ y $f \circ h = f \cdot h$, $g \circ h = g \cdot h$. Luego existe tal h si y sólo si $f = h$.

En ese caso, es inmediato verificar que (\star, h) es un ecualizador de f y g cualquiera sea $h \in G$. ■

Lema 6.7.5. Sea \mathcal{C} una categoría y sea $f, g \in \text{Hom}(A, B)$. Si existe un ecualizador (X, e) de los morfismos f y g , este es único salvo isomorfismos. Más precisamente, si (X', e') es un ecualizador, el único morfismo $k : X' \rightarrow X$ tal que $e' = e \circ k$ es un isomorfismo.

Demostración. Supongamos que (X, e) y (X', e') son ecualizadores de f y g . Entonces, como (X, e) es un ecualizador y $e' : X' \rightarrow A$ verifica que $f \circ e' = g \circ e'$, existe un único morfismo $k : X' \rightarrow X$ tal que $e \circ k = e'$.

Con el mismo razonamiento, existe un morfismo $k' : X \rightarrow X'$ tal que $e' \circ k' = e$. Es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccccc}
 & X' & & & \\
 & \uparrow & \searrow e' & & \\
 k' \uparrow & X & \xrightarrow{e} & A & \xrightleftharpoons[f]{g} B \\
 & \uparrow k & \nearrow e' & & \\
 & X' & & &
 \end{array}$$

En particular, tenemos que $e' \circ (k' \circ k) = (e' \circ k') \circ k = e \circ k = e'$ y por lo tanto el siguiente diagrama es conmutativo:

$$\begin{array}{ccccc} X' & \xrightarrow{e'} & A & \xrightleftharpoons[g]{f} & B \\ \uparrow k' \circ k & \nearrow e' & & & \\ X' & & & & \end{array}$$

Como (X', e') es un ecualizador, hay un único morfismo de X' en X' que hace conmutativo el diagrama anterior. Pero $\text{id}_{X'}$ trivialmente hace conmutativo el diagrama, de donde debe ser $k' \circ k = \text{id}_{X'}$. De manera completamente análoga se prueba que $k \circ k' = \text{id}_X$ y por lo tanto k (y k') es un isomorfismo. \square

La noción dual de un ecualizador es un *coecualizador*:

Definición 6.7.6. El **coecualizador** de dos morfismos $f, g : A \rightarrow B$ en una categoría \mathcal{C} es un par (Y, q) , donde Y es un objeto de \mathcal{C} y $q : B \rightarrow Y$ es un morfismo de \mathcal{C} tal que:

- $q \circ f = q \circ g$
- para todo objeto Y' de \mathcal{C} y todo morfismo $q' : B \rightarrow Y'$ tal que $q' \circ f = q' \circ g$, existe un único morfismo $u : Y \rightarrow Y'$ tal que $u \circ q = q'$.

$$\begin{array}{ccccc} A & \xrightleftharpoons[g]{f} & B & \xrightarrow{q} & Y \\ & & \searrow q' & & \downarrow \exists! u \\ & & & & Y' \end{array}$$

Lema 6.7.7. Sea \mathcal{C} una categoría y \mathcal{C}^{op} su categoría opuesta. Si $f, g \in \text{Hom}_{\mathcal{C}}(A, B)$ entonces (Y, q) es un coecualizador de f y g si y sólo si (Y, q) es un ecualizador de f y g en \mathcal{C}^{op} .

Demostración. Supongamos que (Y, q) es un coecualizador de f y g . Entonces, en primer lugar, $q \in \text{Hom}_{\mathcal{C}}(B, Y)$ hace conmutativo el siguiente diagrama en \mathcal{C} :

$$A \xrightleftharpoons[g]{f} B \xrightarrow{q} Y$$

Luego $q \in \text{Hom}_{\mathcal{C}^{op}}(Y, B)$ verifica

$$f \circ^{op} q = q \circ f = q \circ g = g \circ^{op} q$$

es decir, el siguiente diagrama en \mathcal{C}^{op} es conmutativo:

$$Y \xrightarrow{q} B \xrightleftharpoons[g]{f} A$$

Sea ahora $Y' \in \text{ob } \mathcal{C}^{op} = \text{ob } \mathcal{C}$ y $q' \in \text{Hom}_{\mathcal{C}^{op}}(Y', B) = \text{Hom}_{\mathcal{C}}(Y', B)$ que hace conmutativo el diagrama en \mathcal{C}^{op}

$$Y' \xrightarrow{q'} B \xrightleftharpoons[g]{f} A$$

Entonces el siguiente diagrama en \mathcal{C} también es conmutativo

$$A \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} B \xrightarrow{q'} Y'$$

y como (Y, q) es un coequalizador, existe un único morfismo $u \in \text{Hom}_{\mathcal{C}}(Y, Y')$ que hace conmutativo en \mathcal{C} el siguiente diagrama.

$$\begin{array}{ccc} A & \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} & B \\ & & \searrow q' \\ & & Y' \end{array} \quad \begin{array}{c} \xrightarrow{q} \\ \downarrow u \end{array} \begin{array}{c} Y \\ \\ Y' \end{array}$$

Invirtiendo las flechas, tenemos que $u \in \text{Hom}_{\mathcal{C}^{op}}(Y', Y)$ es el único morfismo que hace conmutativo en \mathcal{C}^{op} el siguiente diagrama:

$$\begin{array}{ccc} Y & \xrightarrow{q} & B \\ \uparrow u & \nearrow q' & \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} \\ Y' & & A \end{array}$$

y por lo tanto (Y, q) es un equalizador de f y g en $\text{Hom}_{\mathcal{C}^{op}}$.

La prueba de la recíproca es análoga y la dejamos como **ejercicio**. □

Como consecuencia del Lema 6.7.5 tenemos

Corolario 6.7.8. *Sean \mathcal{C} una categoría y $f, g \in \text{Hom}(A, B)$. Si existe el coequalizador de f y g , éste es único salvo isomorfismos.*

Ejemplo 6.7.9. Coequalizador en Set. Sean A, B dos conjuntos y $f, g : A \rightarrow B$ dos funciones. Para determinar su coequalizador, necesitamos encontrar en primer lugar un conjunto Y y una función $q : B \rightarrow Y$ tal que $q(f(a)) = q(g(a))$ para cada $a \in A$.

Sea $C = \{(f(a), g(a)) : a \in A\} \subset B \times B$ y sea \sim la menor relación de equivalencia en B que contiene a C (observemos que \sim se obtiene de intersecar, como subconjuntos de $B \times B$, todas las relaciones de equivalencia que contienen a C). Pongamos $Y = B / \sim$ y sea $q : B \rightarrow Y$ la proyección al cociente, esto es, $q(b) = [b]$. Como $C \subset \sim$, resulta $f(a) \sim g(a)$ para cada $a \in A$, y por lo tanto $[f(a)] = [g(a)]$, es decir, $q(f(a)) = q(g(a))$ para cada $a \in A$. Luego q satisface la condición que queríamos.

Si ahora $q' : B \rightarrow Y'$ satisface $q' \circ f = q' \circ g$, entonces $q'(f(a)) = q'(g(a))$ para cada $a \in A$. Pongamos entonces

$$(6.17) \quad u : Y \rightarrow Y', \quad u([b]) = q'(b).$$

Debemos probar que u está bien definida, esto es, si $b_1 \sim b_2$, entonces $q'(b_1) = q'(b_2)$. Una vez que hayamos probado esto, es claro que $u \circ q = q'$ y es la única función de Y en Y' que verifica esta propiedad. Por lo tanto (Y, q) será un coequalizador de f, g .

Para ello necesitamos describir explícitamente a \sim en función de C . Observemos primero que como \sim es una relación de equivalencia que contiene a C , debe contener a $\Delta = \{(b, b) : b \in B\}$ (para que sea

reflexiva) y a $C^{-1} = \{(g(a), f(a)) : a \in A\}$ (para que sea simétrica). Esto es, si ponemos $C^1 = C \cup \Delta \cup C^{-1}$, entonces $C^1 \subset \sim$. Definamos inductivamente

$$C^{i+1} = C^1 \circ C^i = \{(b_1, b_2) \in B \times B : \exists b \in B / (b_1, b) \in C_1 \wedge (b, b_2) \in C_i\}$$

Como la composición de relaciones es asociativa, inductivamente se prueba que

$$(6.18) \quad C^{i+1} = C^i \circ C^1 = C^k \circ C^j \quad \text{tal que} \quad k + j = i + 1.$$

Definamos

$$\mathcal{R} = \bigcup_{i \in \mathbb{N}} C^i$$

Como \sim es transitiva, debemos tener que $C^i \subset \sim$ para cada $i \in \mathbb{N}$ y por lo tanto $\mathcal{R} \subset \sim$. Veamos que en realidad estos subconjuntos de $B \times B$ son iguales. Como \sim es la menor relación de equivalencia que contiene a C , bastará probar que \mathcal{R} es una relación de equivalencia (que claramente contiene a C).

Observemos primero que \mathcal{R} es reflexiva pues contiene a Δ .

Veamos que \mathcal{R} es simétrica. Probaremos inductivamente que $(C^i)^{-1} = C_i$ para cada $i \in \mathbb{N}$. Esto es evidente para $i = 1$. Supongamos que es válido para un cierto i . Sea $(b_1, b_2) \in C^{i+1}$. Entonces existe $b \in B$ tal que $(b_1, b) \in C^1$ y $(b, b_2) \in C^i$. Pero entonces $(b, b_1) \in C^1$, y por hipótesis inductiva $(b_2, b) \in C^i$. Luego $(b_2, b_1) \in C^i \circ C = C^{i+1}$ (por (6.18)).

Finalmente, \mathcal{R} es transitiva pues es la clausura transitiva de C^1 (ver Ejercicio 24 del Capítulo 1).

Probemos entonces que la función u definida en (6.17) está efectivamente bien definida. Para ello probaremos inductivamente que si $(b_1, b_2) \in C^i$, entonces $q'(b_1) = q'(b_2)$. Para $i = 1$ tenemos tres posibilidades: $b_1 = b_2$ (o sea $b_1, b_2 \in \Delta$), o bien $b_1 = f(a)$ y $b_2 = g(a)$ para algún $a \in A$ ($(b_1, b_2) \in C$) o $b_1 = g(a)$, $b_2 = f(a)$ ($(b_1, b_2) \in C^{-1}$). Si se verifica la primera posibilidad es trivial que $q'(b_1) = q'(b_2)$. Las dos últimas posibilidades son análogas, por lo que probaremos que si $b_1 = f(a)$ y $b_2 = g(a)$, entonces $q'(b_1) = q'(b_2)$. Pero esto es inmediato del hecho que $q' \circ f = q' \circ g$.

Probado el caso base, supongamos que es cierto que para un cierto i , si $(b_1, b_2) \in C^i$ entonces $q'(b_1) = q'(b_2)$. Sea $(b_1, b_2) \in C^{i+1}$. Entonces existe $b \in B$ tal que $(b_1, b) \in C$ y $(b, b_2) \in C^i$. Luego por el caso base $q'(b_1) = q'(b)$ y por hipótesis inductiva $q'(b) = q'(b_2)$. Concluimos que $q'(b_1) = q'(b_2)$ como queríamos probar. ■

Ejemplo 6.7.10. Coecualizador en Grp. Sean G y H grupos y $f, g : G \rightarrow H$ dos homomorfismos de grupos. Consideremos el conjunto $S = \{f(x)g(x)^{-1} : x \in G\} \subseteq H$. Sea N el menor subgrupo normal de H que contiene a S , que se obtiene de intersecar todos los subgrupos normales que contienen a S (N se denomina la *clausura normal* de S). Sea $Y = H/N$ y consideremos la proyección al cociente $q : H \rightarrow Y$. Entonces $\ker(q) = N$ y como $S \subseteq N$, resulta $q(S) = [e]$. Como además para cada $x \in G$, $f(x)g(x)^{-1} \in S$, se tiene que

$$q(f(x)g(x)^{-1}) = [e] \implies q(f(x))q(g(x))^{-1} = [e] \implies q(f(x)) = q(g(x)).$$

Si ahora $q' : H \rightarrow Y'$ verifica que $q'(f(x)) = q'(g(x))$ para cada $x \in G$, entonces $q'(f(x)g(x)^{-1}) = [e]$, y por lo tanto $S \subseteq \ker(q')$. Como N es el menor subgrupo normal de H que contiene a S , y $\ker(q')$ es un subgrupo normal de H que contiene a S , debe ser $N \subseteq \ker(q')$. Luego, por el Lema de Factorización (Lema 5.3.7) existe un único morfismo $u : Y' \rightarrow Y$ que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc} H & \xrightarrow{q} & Y = H/N \\ & \searrow q' & \downarrow u=q' \\ & & Y' \end{array}$$

Concluimos que (Y, q) es un coecualizador de f y g . ■

Observemos que en Set un ecualizador tiene asociado una función inyectiva, o sea un monomorfismo, y un coecualizador una función sobreyectiva, o sea un epimorfismo. Esto es válido en cualquier categoría:

Lema 6.7.11. *Sea \mathcal{C} una categoría, A, B objetos en \mathcal{C} y $f, g : A \rightarrow B$ dos morfismos en \mathcal{C} .*

1. *Si (X, e) es un ecualizador de f y g , entonces $e : X \rightarrow A$ es un morfismo mónico. Si además e es épico, entonces es un isomorfismo.*
2. *Si (Y, q) es un coecualizador de f y g , entonces $q : B \rightarrow Y$ es un morfismo épico. Si además q es mónico, entonces es un isomorfismo.*

Demostración. Probaremos el punto 1. El punto 2 es consecuencia del Ejercicio 18 de este capítulo y del Lema 6.7.7. Dejamos los detalles como **ejercicio**.

Sea (X, e) un ecualizador de los morfismos $f, g : A \rightarrow B$. En particular, $f \circ e = g \circ e$.

Sean $j, k : X' \rightarrow X$ dos morfismos tales que $e \circ k = e \circ j$. Pongamos $e' = e \circ k = e \circ j : X' \rightarrow A$. Entonces

$$f \circ e' = f \circ (e \circ k) = (f \circ e) \circ k = (g \circ e) \circ k = g \circ (e \circ k) = g \circ e'$$

Entonces los siguientes diagramas conmutan:

$$\begin{array}{ccc} X & \xrightarrow{e} & A \xrightarrow[f]{g} B \\ \uparrow j & \nearrow e' & \\ X' & & \end{array}, \quad \begin{array}{ccc} X & \xrightarrow{e} & A \xrightarrow[f]{g} B \\ \uparrow k & \nearrow e' & \\ X' & & \end{array}$$

Como (X, e) es un ecualizador de f y g , hay un único morfismo de X' en X que hace conmutativo el diagrama

$$\begin{array}{ccc} X & \xrightarrow{e} & A \xrightarrow[f]{g} B \\ \uparrow \text{---} j & \nearrow e' & \\ X' & & \end{array}$$

Concluimos que debe ser $j = k$ y por lo tanto e es un morfismo mónico.

Supongamos ahora que (X, e) es un ecualizador y $e : X \rightarrow A$ es un morfismo épico. Como $e \circ f = e \circ g$, debe ser $f = g$. Pero entonces (A, id_A) también es un ecualizador del par $f, g = f$. En efecto,

$f \circ \text{id}_A = f = g = g \circ \text{id}_A$, y dado $X' \in \text{ob } \mathcal{C}$ tal que existe un morfismo $e' : X' \rightarrow A$, se verifica trivialmente que $f \circ e' = g \circ e'$ y e' es el único morfismo tal que $e' \circ \text{id}_A = e'$:

$$\begin{array}{ccccc} A & \xrightarrow{\text{id}_A} & A & \xrightarrow[f]{g} & B \\ \uparrow e' & & \nearrow e' & & \\ X' & & & & \end{array}$$

Luego del Lema 6.7.5 resulta que $e : X \rightarrow A$ es un isomorfismo. \square

6.8. Conos, coconos, límites y colímites

En esta sección presentaremos algunas construcciones universales asociadas a diagramas en una categoría, que incluyen como casos particulares a algunas de las construcciones que hemos desarrollado en las secciones anteriores.

Definición 6.8.1. Sea \mathcal{C} una categoría y \mathcal{D} un diagrama en \mathcal{C} . Denotemos por $\text{ob } \mathcal{D}$ los objetos de \mathcal{C} que representan algún nodo de \mathcal{D} y $\text{mor } \mathcal{D}$ los morfismos de \mathcal{C} que representan aristas de \mathcal{D} .

Un **cono** para \mathcal{D} es un par $(X, \mathcal{F}_{\mathcal{D}})$ donde:

- X es un objeto en \mathcal{C} .
- $\mathcal{F}_{\mathcal{D}}$ es una familia de morfismos de \mathcal{C} tal que:
 - Para cada $D \in \text{ob } \mathcal{D}$ existe un único morfismo $f_D : X \rightarrow D \in \mathcal{F}_{\mathcal{D}}$
 - si $f : A \rightarrow B$ es un morfismo en $\text{mor } \mathcal{D}$, el siguiente diagrama conmuta:

$$\begin{array}{ccc} & X & \\ f_A \swarrow & & \searrow f_B \\ A & \xrightarrow{f} & B \end{array}$$

Un **límite** para \mathcal{D} es un cono $(X, \mathcal{F}_{\mathcal{D}})$ que verifica la siguiente propiedad universal:

- para todo cono $(X', \mathcal{F}'_{\mathcal{D}})$ de \mathcal{D} , existe un único morfismo $k : X' \rightarrow X$ tal que el siguiente diagrama conmuta para cada objeto D en $\text{ob } \mathcal{D}$:

$$\begin{array}{ccc} X' & \xrightarrow{\quad k \quad} & X \\ f'_D \searrow & & \swarrow f_D \\ & D & \end{array}$$

Ejemplo 6.8.2. Un ecualizador es un límite. Para el diagrama \mathcal{D}

$$A \xrightarrow[f]{g} B$$

un cono está unívocamente determinado por cualquier morfismo $f_A : X \rightarrow A$ tal que

$$g \circ f_A = f \circ f_A$$

Este ejemplo muestra que no siempre existen límites para cualquier diagrama.

Más generalmente, para un diagrama sin flechas \mathcal{D} (formado por una colección arbitraria de objetos) un límite para \mathcal{D} es un producto entre sus objetos. ■

Veremos más adelante que los límites (y sus duales, los colímites) son único salvo isomorfismos. Sin embargo esto no es cierto para los conos:

Ejemplo 6.8.4. Un cono no necesariamente es único salvo isomorfismos. Consideremos el diagrama \mathcal{D} :

$$\begin{array}{ccc} & & B \\ & & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

Un cono para \mathcal{D} es $(X, \mathcal{F}_\mathcal{D})$ con $\mathcal{F}_\mathcal{D} = \{f_A : X \rightarrow A, f_B : X \rightarrow B, f_C : X \rightarrow C\}$ que completan \mathcal{D} a un cuadrado **conmutativo**

$$\begin{array}{ccc} X & \xrightarrow{f_B} & B \\ f_A \downarrow & \searrow f_C & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

es decir, $f \circ f_A = f_C$, $g \circ f_B = f_C$. Observemos que conociendo \mathcal{D} , f_A y f_B podemos deducir f_C .

Consideremos un caso particular de \mathcal{D} en la categoría Set:

$$\begin{array}{ccc} A = \mathbb{R} & & \\ & \downarrow g & \\ B = \mathbb{R} & \xrightarrow{f} & C = \mathbb{R} \end{array}$$

donde $f(x) = x^2$, $g(x) = x^3$. Un cuadrado conmutativo se obtiene poniendo $f_B(x) = x^2$, $f_A(x) = x^3$, luego un cono para \mathcal{D} es $(\mathbb{R}, \{f_A, f_B, f_C\})$, donde $f_C(x) = x^6$. Pero también podemos considerar el cono $(\mathbb{R}, \{f'_A, f'_B, f'_C\})$ poniendo $f'_B(x) = x^4$, $f'_A(x) = x^6$, $f'_C(x) = x^{12}$. En este caso, el objeto X del cono es el mismo, aunque varían los morfismos. Un tercer cono es $(\mathbb{N}, \{f''_A, f''_B, f''_C\})$, donde las leyes de f''_A , f''_B , f''_C pueden tomarse iguales a cualquiera de las dos opciones anteriores.

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f_B(x)=x^2} & \mathbb{R} \\ f_A(x)=x^3 \downarrow & \searrow f_C & \downarrow g(x)=x^3 \\ \mathbb{R} & \xrightarrow{f(x)=x^2} & \mathbb{R} \end{array} \quad \begin{array}{ccc} \mathbb{R} & \xrightarrow{f'_B(x)=x^4} & \mathbb{R} \\ f'_A(x)=x^6 \downarrow & \searrow f'_C & \downarrow g(x)=x^3 \\ \mathbb{R} & \xrightarrow{f(x)=x^2} & \mathbb{R} \end{array} \quad \begin{array}{ccc} \mathbb{N} & \xrightarrow{f''_B(x)=x^2} & \mathbb{R} \\ f''_A(x)=x^3 \downarrow & \searrow f''_C & \downarrow g(x)=x^3 \\ \mathbb{R} & \xrightarrow{f(x)=x^2} & \mathbb{R} \end{array}$$

En este caso vemos que los conjuntos $X = \mathbb{R}$ y $X' = \mathbb{N}$ que definen ambos conos no sólo son distintos, sino que ni siquiera son isomorfos (dado que no hay ninguna biyección entre \mathbb{R} y \mathbb{N}). Luego el concepto de cono no es único salvo isomorfismos. ■

Ejemplo 6.8.5. El pullback de dos morfismos. Sean $f : A \rightarrow C$ y $g : B \rightarrow C$ dos morfismos en una categoría \mathcal{C} con igual codominio. Ya hemos visto que para el diagrama \mathcal{D}

$$\begin{array}{ccc} & B & \\ & \downarrow g & \\ A & \xrightarrow{f} & C \end{array}$$

un cono es $(X, \mathcal{F}_{\mathcal{D}})$ con $\mathcal{F}_{\mathcal{D}} = \{f_A : X \rightarrow A, f_B : X \rightarrow B, f_C : X \rightarrow C\}$ que completan \mathcal{D} a un cuadrado conmutativo

$$\begin{array}{ccc} X & \xrightarrow{f_B} & B \\ f_A \downarrow & & \downarrow g \\ A & \xrightarrow{f} & C \end{array}$$

donde $f_C = g \circ f_B = f \circ f_A$. En este caso, $(X, \mathcal{F}_{\mathcal{D}})$ es un límite si para cada objeto X' y cada par de morfismos $f'_B : X' \rightarrow B$, $f'_A : X' \rightarrow A$ tal que $g \circ f'_B = f \circ f'_A$, existe un único morfismo $k : X' \rightarrow X$ tal que $f'_A = f_A \circ k$, $f'_B = f_B \circ k$:

$$(6.19) \quad \begin{array}{ccccc} X' & & \xrightarrow{f'_B} & & B \\ & \searrow k & & & \downarrow g \\ & & X & \xrightarrow{f_B} & B \\ & \swarrow f'_A & \downarrow f_A & & \downarrow g \\ & & A & \xrightarrow{f} & C \end{array}$$

En este caso, el límite $(X, \mathcal{F}_{\mathcal{D}})$ recibe el nombre de **pullback** de los morfismos $f : A \rightarrow C$, $g : B \rightarrow C$.

Por ejemplo, en Set , el pullback de dos funciones $f : A \rightarrow C$, $g : B \rightarrow C$ está dado por

$$X = \{(a, b) \in A \times B : f(a) = g(b)\} \subseteq A \times B$$

y las funciones $f_A : X \rightarrow A$ y $f_B : X \rightarrow B$ no son más que la restricción a X de las proyecciones $\pi_A : A \times B \rightarrow A$ y $\pi_B : A \times B \rightarrow B$ respectivamente. En efecto, para cada $(a, b) \in X$,

$$f \circ f_A(a, b) = f(a) = g(b) = g \circ f_B(a, b)$$

Luego poniendo $f_C = g \circ f_B = f \circ f_A$, resulta que $(X, \{f_A, f_B, f_C\})$ es un cono para \mathcal{D} .

Si ahora $(X', \{f'_A, f'_B, f'_C\})$ es otro cono para \mathcal{D} , entonces $g \circ f'_B = f \circ f'_A$ y por lo tanto $k : X' \rightarrow X$ dada por $k(x) = (f'_A(x), f'_B(x))$ está bien definida y hace de (6.19) un diagrama conmutativo.

Si $k' : X' \rightarrow X$ es una función que hace de (6.19) un diagrama conmutativo, y supongamos que $k'(x) = (k'_1(x), k'_2(x))$, entonces

$$k'_1(x) = f_A(k'(x)) = f'_A(x), \quad k'_2(x) = f_B(k'(x)) = f'_B(x)$$

de donde $k'(x) = k(x)$. Luego $(X, \{f_A, f_B, f_C\})$ es un límite para \mathcal{D} . ■

Ejemplo 6.8.6. La categoría de conos sobre un diagrama. Sea \mathcal{D} un diagrama cualquiera en una categoría \mathcal{C} . Sean $(X, \mathcal{F}_{\mathcal{D}})$ y $(X', \mathcal{F}'_{\mathcal{D}})$ conos sobre \mathcal{D} y supongamos que existe un morfismo $k : X' \rightarrow X$ tal que $f_A \circ k = f'_A$ para cada $A \in \text{ob } \mathcal{D}$:

$$\begin{array}{ccc} X' & \xrightarrow{k} & X \\ & \searrow f'_A & \swarrow f_A \\ & A & \end{array}$$

Decimos entonces que k es un morfismo del cono $(X', \mathcal{F}'_{\mathcal{D}})$ y el cono $(X, \mathcal{F}_{\mathcal{D}})$ y lo denotamos

$$k : (X', \mathcal{F}'_{\mathcal{D}}) \rightarrow (X, \mathcal{F}_{\mathcal{D}})$$

Supongamos que $(X'', \mathcal{F}''_{\mathcal{D}})$ es un cono sobre \mathcal{D} y $k' : (X'', \mathcal{F}''_{\mathcal{D}}) \rightarrow (X', \mathcal{F}'_{\mathcal{D}})$ es un morfismo de conos. Veamos que $k \circ k'$ es un morfismo de conos de $(X'', \mathcal{F}''_{\mathcal{D}})$ en $(X, \mathcal{F}_{\mathcal{D}})$. En efecto, si $A \in \text{ob } \mathcal{D}$, en el siguiente diagrama

$$\begin{array}{ccccc} X'' & \xrightarrow{k'} & X' & \xrightarrow{k} & X \\ & \searrow f''_A & \downarrow f'_A & \swarrow f_A & \\ & & A & & \end{array}$$

los triángulos interiores conmutan. Luego

$$f_A \circ (k \circ k') = (f_A \circ k) \circ k' = f'_A \circ k' = f''_A$$

es decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} X'' & \xrightarrow{k \circ k'} & X \\ & \searrow f''_A & \swarrow f_A \\ & A & \end{array}$$

y por lo tanto $k \circ k' : (X'', \mathcal{F}''_{\mathcal{D}}) \rightarrow (X, \mathcal{F}_{\mathcal{D}})$ es un morfismo de conos. Es inmediato verificar que la composición de morfismos de conos es asociativa y que $\text{id}_X : (X, \mathcal{F}_{\mathcal{D}}) \rightarrow (X, \mathcal{F}_{\mathcal{D}})$ es un morfismo de conos (dejamos los detalles como **ejercicio**)

Por lo tanto $\text{Cone}(\mathcal{D})$ tal que $\text{ob Cone}(\mathcal{D})$ son todos los conos sobre \mathcal{D} y $\text{mor Cone}(\mathcal{D})$ son los morfismos entre conos, con la composición y las identidades que vimos recién, y las funciones dominio y codominio obvias, es una categoría, denominada **categoría de conos** sobre \mathcal{D} . ■

Teorema 6.8.7. Sea \mathcal{D} un diagrama en una categoría \mathcal{C} . Si $(X, \mathcal{F}_{\mathcal{D}})$ es un límite para \mathcal{D} . Entonces $(X, \mathcal{F}_{\mathcal{D}})$ es único salvo isomorfismos. Más precisamente, si $(X', \mathcal{F}'_{\mathcal{D}})$ es un límite sobre \mathcal{D} , existe un isomorfismo $k : X' \rightarrow X$ tal que para cada $A \in \text{ob } \mathcal{D}$, $f'_A = f_A \circ k$.

Demostración. Sea \mathcal{D} un diagrama y $\text{Cone}(\mathcal{D})$ la categoría de conos sobre \mathcal{D} . Entonces del Ejercicio 27 de este capítulo, resulta que si $(X, \mathcal{F}_{\mathcal{D}})$ es un límite para \mathcal{D} , entonces es un objeto terminal de $\text{Cone}(\mathcal{D})$. Luego del Lema 6.5.7 resulta que si $(X', \mathcal{F}'_{\mathcal{D}})$ es un límite, entonces $(X, \mathcal{F}_{\mathcal{D}})$ y $(X', \mathcal{F}'_{\mathcal{D}})$ son isomorfos en $\text{Cone}(\mathcal{D})$. El resultado sigue entonces del Ejercicio 26. □

El concepto dual al de cono y límite es el de cocono y colímite:

Definición 6.8.8. Un **cocono** para \mathcal{D} es un par $(Y, \mathcal{G}_{\mathcal{D}})$ donde:

- Y es un objeto en \mathcal{C} .
- $\mathcal{G}_{\mathcal{D}}$ es una familia de morfismos de \mathcal{C} tal que
 - Para cada $D \in \text{ob } \mathcal{D}$ existe un único morfismo $g_D : D \rightarrow Y \in \mathcal{G}_{\mathcal{D}}$
 - si $f : A \rightarrow B$ es un morfismo en $\text{mor } \mathcal{D}$, el siguiente diagrama conmuta:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow g_A & \swarrow g_B \\ & Y & \end{array}$$

Un **colímite** para \mathcal{D} es un cocono $(Y, \mathcal{G}_{\mathcal{D}})$ que verifica la siguiente propiedad universal:

- para todo cocono $(Y', \mathcal{G}'_{\mathcal{D}})$ de \mathcal{D} , existe un único morfismo $k : Y \rightarrow Y'$ tal que el siguiente diagrama conmuta para cada objeto D en $\text{ob } \mathcal{D}$:

$$\begin{array}{ccc} Y & \xrightarrow{\quad k \quad} & Y' \\ & \nwarrow g_D \quad \nearrow g'_D & \\ & D & \end{array}$$

A esta altura deberíamos estar convencidos que los conceptos duales de un determinado concepto en una categoría \mathcal{C} , son esos mismos conceptos en la categoría \mathcal{C}^{op} . Enunciaremos a continuación las propiedades de coconos y colímites que se demuestran de manera completamente análoga a resultados similares de las secciones anteriores. Dejamos las pruebas como **ejercicio**.

Lema 6.8.9. Sea \mathcal{D} un diagrama en una categoría \mathcal{C} . Denotemos por \mathcal{D}^{op} el diagrama en \mathcal{C}^{op} con los mismos objetos y los mismos morfismos que en \mathcal{D} (es decir, es el diagrama que se obtiene de revertir las flechas en \mathcal{D}). Entonces $(Y, \mathcal{G}_{\mathcal{D}})$ es un cocono (resp. un colímite) para \mathcal{D} en \mathcal{C} si y sólo si $(Y, \mathcal{G}_{\mathcal{D}})$ es un cono (resp. un límite) para \mathcal{D}^{op} en \mathcal{C}^{op} .

Teorema 6.8.10. Sea \mathcal{D} un diagrama en una categoría \mathcal{C} . Si existe un colímite para \mathcal{D} , entonces éste es único salvo isomorfismos.

Ejemplo 6.8.11. Coecualizadores y coproductos son colímites De la misma manera que en el Ejemplo 6.8.2, tenemos que un colímite para el diagrama \mathcal{D}

$$A \rightrightarrows B$$

es un coecualizador de f y g .

Si ahora consideramos un diagrama \mathcal{D} con dos nodos A y B y sin flechas, del mismo modo que en el Ejemplo 6.8.3 podemos ver que un colímite para \mathcal{D} es un coproducto de $(A + B, i_A, i_B)$. ■

Ejemplo 6.8.12. El pushout de dos morfismos. Consideremos dos morfismos $f : C \rightarrow A$, $g : C \rightarrow B$ en una categoría \mathcal{C} , con el mismo dominio y consideremos el diagrama \mathcal{D}' :

$$\begin{array}{ccc} & & B \\ & & \uparrow g \\ A & \xleftarrow{f} & C \end{array}$$

un colímite para \mathcal{D}' está completamente determinado por dos morfismos $i_B : B \rightarrow Y$, $i_A : A \rightarrow Y$ que hacen conmutativo el diagrama

$$\begin{array}{ccc} Y & \xleftarrow{i_B} & B \\ \uparrow i_A & & \uparrow g \\ A & \xleftarrow{f} & C \end{array}$$

y por lo tanto determinan un cocono $(Y, \{i_A, i_B, i_C\})$, donde $i_C = i_B \circ g = i_A \circ f$. Además para cada Y' y cada par de morfismos i'_A, i'_B tales que $i'_B \circ g = i'_A \circ f$, existe un único morfismo $k : Y \rightarrow Y'$ tal que $k \circ i_A = i'_A$, $k \circ i_B = i'_B$:

$$\begin{array}{ccccc} & & Y' & & \\ & & \swarrow k & & \\ & & Y & \xleftarrow{i_B} & B \\ & \uparrow i_A & \uparrow g & & \\ A & \xleftarrow{f} & C & & \end{array}$$

En este caso, este colímite se denomina un **pushout** de f y g .

6.9. Exponenciales - Categorías cartesianas cerradas.

Para finalizar con los conceptos básicos asociados a los objetos y morfismos de una categoría introduciremos la noción de *exponenciales*. El objetivo es definir un objeto B^A a partir de dos objetos A y B en una categoría \mathcal{C} .

Comencemos analizando la categoría \mathbf{Set} . Si tenemos un conjunto B , podemos definir el conjunto B^A como el producto

$$B^A = \prod_{a \in A} B_a = \{f : A \rightarrow B\} = \mathbf{Hom}(A, B),$$

poniendo $B_a = B$ para cada $a \in A$ (ver Ejemplo 6.6.19).

Esta construcción sin embargo no puede generalizarse a cualquier otra categoría. En primer lugar, porque queremos definir B^A para objetos arbitrarios A, B de \mathcal{C} , por lo tanto el producto $\prod_{a \in A} B_a$, poniendo $B_a = B$, sólo tiene sentido en una categoría \mathcal{C} cuyos objetos son conjuntos (además que \mathcal{C} debe admitir productos arbitrarios). Podemos pensar entonces en definir B^A como $\mathbf{Hom}(A, B)$, copiando lo que ocurre

en Set . Pero aquí tenemos el problema que $\text{Hom}(A, B)$ no necesariamente es un objeto de \mathcal{C} , algo que sí ocurre en Set .

Por lo tanto intentaremos encontrar alguna propiedad universal que nos permita caracterizar B^A en Set y así extender esta definición a categorías arbitrarias. Recordemos que B^A , al ser un producto, está dado además por la familia de funciones $\{\pi_a : B^A \rightarrow B\}_{a \in A}$ tales que $\pi_a(f) = f(a)$ para cada $a \in A$. Ahora bien, podemos reunir toda la información que nos brinda la familia anterior de funciones en una única función, que llamaremos eval y que definimos como

$$\text{eval} : B^A \times A \rightarrow B, \quad \text{eval}(f, a) = f(a) = \pi_a(f).$$

Por otra parte, la propiedad universal del producto nos dice que para cada familia de morfismos $\{f_a : C \rightarrow B\}_{a \in A}$, existe una única función $\tilde{g} = \langle f_a \rangle_{a \in A} : C \rightarrow B^A$ tal que para cada $x \in A$, $\pi_x \circ \tilde{g} = f_x$. Por lo tanto si ponemos

$$\tilde{g} \times \text{id}_A : C \times A \rightarrow B^A \times A, \quad \tilde{g} \times \text{id}_A(c, a) = (\tilde{g}(c), a)$$

tenemos que

$$\text{eval} \circ (\tilde{g} \times \text{id}_A)(c, x) = \text{eval}(\tilde{g}(c), x) = \pi_x(\tilde{g}(c)) = f_x(c).$$

Finalmente observemos que considerar una familia de funciones $\{f_a : C \rightarrow B\}_{a \in A}$ es equivalente a considerar una única función $g : C \times A \rightarrow B$. En efecto, la familia $\{f_a\}_{a \in A}$ permite definir la función $g(c, a) = f_a(c)$, y recíprocamente, dada $g : C \times A \rightarrow B$, g define la familia $\{f_a : C \rightarrow B\}_{a \in A}$ poniendo $f_a(c) = g(c, a)$.

En conclusión, tenemos que B^A está caracterizado por la siguiente propiedad universal: existe una función $\text{eval} : B^A \times A \rightarrow B$ tal que para cada conjunto C y cada función $g : C \times A \rightarrow B$, existe una única función $\tilde{g} : C \rightarrow B^A$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} B^A & & B^A \times A \xrightarrow{\text{eval}} B \\ \uparrow \tilde{g} & \nearrow g & \\ C & & C \times A \end{array}$$

Definición 6.9.1. Sea \mathcal{C} una categoría con productos finitos y sean A, B dos objetos de \mathcal{C} . Un objeto B^A es un **exponencial** si existe un morfismo $\text{eval} : B^A \times A \rightarrow B$ tal que para cada conjunto C y cada morfismo $g : C \times A \rightarrow B$, existe un único morfismo $\tilde{g} : C \rightarrow B^A$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} B^A & & B^A \times A \xrightarrow{\text{eval}} B \\ \uparrow \tilde{g} & \nearrow g & \\ C & & C \times A \end{array}$$

El morfismo \tilde{g} se denota $\text{curry}(g)$. Si para cualquier par de objetos A, B de \mathcal{C} existe un exponencial, \mathcal{C} se dice una categoría con exponenciales.

Ejemplo 6.9.2. Ya vimos que \mathbf{Set} es una categoría con exponenciales. Consideremos ahora la categoría \mathbf{Poset} . Sea (A, \preceq_A) , (B, \preceq_B) dos objetos en \mathbf{Poset} y pongamos

$$B^A = \{f : A \rightarrow B : f \text{ es un morfismo de posets}\} = \mathbf{Hom}_{\mathbf{Poset}}(A, B).$$

Definimos un orden \preceq_m en B^A por

$$f \preceq_m g \iff f(a) \preceq_B g(a) \forall a \in A.$$

Es fácil ver que \preceq_m es un orden parcial en B^A y por lo tanto (B^A, \preceq_m) es un objeto en \mathbf{Poset} .

Consideremos la función $\text{eval} : B^A \times A \rightarrow B$, tal que $\text{eval}(f, a) = f(a)$. Debemos probar que eval es un morfismo de \mathbf{Poset} , es decir que es un morfismo de orden de $(B^A \times A, \preceq)$ en (B, \preceq_B) , donde \preceq es el orden producto de \preceq_m y \preceq_A , esto es,

$$(f, a) \preceq (f', a') \iff f \preceq_m f' \text{ y } a \preceq_A a'.$$

Tomemos entonces $(f, a), (f', a') \in B^A \times A$ tales que $(f, a) \preceq (f', a')$. Entonces en particular $a \preceq_A a'$, y como f es un morfismo de orden tendremos $f(a) \preceq_B f(a')$. Por otra parte, $f \preceq_m f'$, entonces $f(a') \preceq_B f'(a')$. Luego

$$f(a) \preceq_B f(a') \preceq_B f'(a') \implies \text{eval}(f, a) \preceq_B \text{eval}(f', a').$$

Para terminar de probar que B^A es efectivamente un exponencial en \mathbf{Poset} , nos falta encontrar el curry de un morfismo de orden arbitrario $g : (C \times A) \rightarrow B$. Sea (C, \preceq_C) un poset y consideremos $(C \times A)$ con el orden producto $\preceq' = \preceq_C \times \preceq_A$. Pongamos

$$\tilde{g} : C \rightarrow B^A, \quad \tilde{g}(c) = f_c : A \rightarrow B, \quad / \quad f_c(a) = g(c, a).$$

Observemos que \tilde{g} está bien definida, es decir, que para cada $c \in C$, $f_c : A \rightarrow B$ es efectivamente un morfismo de orden. En efecto, para cada $c \in C$ fijo, si $a \preceq_A a'$, entonces $(c, a) \preceq' (c, a')$ y como g es un morfismo de orden, $g(c, a) \preceq_B g(c, a')$, o sea, $f_c(a) \preceq_B f_c(a')$.

Por otra parte,

$$\text{eval} \circ (\tilde{g} \times \text{id}_A)(c, a) = \text{eval}(\tilde{g}(c), a) = \text{eval}(f_c, a) = f_c(a) = g(c, a).$$

Por lo tanto para ver que $\tilde{g} = \text{curry}(g)$ sólo nos queda probar que \tilde{g} es un morfismo de orden. Sean entonces $c, c' \in C$ tales que $c \preceq_C c'$. Entonces para $a \in A$ arbitrario tenemos que $(c, a) \preceq' (c', a)$ y por lo tanto

$$f_c(a) = g(c, a) \preceq_B g(c', a) = f_{c'}(a) \implies f_c \preceq_m f_{c'}.$$

Dejamos como ejercicio probar la unicidad de \tilde{g} (que es inmediata de la definición). Concluimos que \mathbf{Poset} es una categoría con exponenciales. ■

Ejemplo 6.9.3. El functor \exp_A . Sea \mathcal{C} una categoría con exponenciales y definamos $\exp_A : \mathcal{C} \rightarrow \mathcal{C}$ tal que $\exp_A(B) = B^A$ para cada objeto B de \mathcal{C} . Para definir $\exp_A(f)$ para un morfismo $f \in \mathbf{Hom}(B, C)$,

consideremos el morfismo $f \circ \text{eval}_B : B^A \times A \rightarrow C$. Por la propiedad universal de las exponenciales, existe un único morfismo $f^A := \text{curry}(f \circ \text{eval}_B) : B^A \rightarrow C^A$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc}
 C^A & & C^A \times A \xrightarrow{\text{eval}_C} C \\
 \uparrow f^A & \nearrow f \circ \text{eval}_B & \uparrow f \\
 B^A & & B^A \times A \xrightarrow{\text{eval}_B} B
 \end{array}$$

Por lo tanto podemos definir $\exp_A(f) = f^A \in \text{Hom}(B^A, C^A)$.

Veamos que $\exp_A : \mathcal{C} \rightarrow \mathcal{C}$ es un funtor. Sea B un objeto cualquiera de \mathcal{C} y veamos que $\exp_A(\text{id}_B) = \text{id}_{B^A}$. Observemos que $\text{id}_B^A = \text{curry}(\text{eval} \circ \text{id}_B)$ es el único morfismo que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc}
 B^A & & B^A \times A \xrightarrow{\text{eval}} B \\
 \uparrow \text{id}_B^A & \nearrow \text{id}_B \circ \text{eval} & \uparrow \text{id}_B \\
 B^A & & B^A \times A \xrightarrow{\text{eval}} B
 \end{array}$$

Pero trivialmente id_{B^A} también hace conmutativo el diagrama

$$\begin{array}{ccc}
 B^A & & B^A \times A \xrightarrow{\text{eval}} B \\
 \uparrow \text{id}_{B^A} & \nearrow \text{id}_{B^A} \circ \text{eval} & \uparrow \text{id}_B \\
 B^A & & B^A \times A \xrightarrow{\text{eval}} B
 \end{array}$$

con lo cual deberá ser $\text{id}_{B^A} = \text{id}_B^A = \exp(\text{id}_B)$.

Consideremos ahora objetos B, C, D y sean $f \in \text{Hom}(B, C)$, $g \in \text{Hom}(C, D)$ y observemos el siguiente diagrama:

$$\begin{array}{ccccc}
 D^A & & D^A \times A \xrightarrow{\text{eval}_D} D & & D^A \\
 \uparrow g^A & \nearrow g^A \times \text{id}_A & \uparrow g & & \uparrow g^A \circ f^A \\
 C^A & & C^A \times A \xrightarrow{\text{eval}_C} C & \rightsquigarrow & D^A \\
 \uparrow f^A & \nearrow f^A \times \text{id}_A & \uparrow f & & \uparrow \varphi \\
 B^A & & B^A \times A \xrightarrow{\text{eval}_B} B & & B^A
 \end{array}$$

donde $\varphi = (g^A \times \text{id}_A) \circ (f^A \times \text{id}_A)$. Como los cuadrados interiores del diagrama de la izquierda son conmutativos, el diagrama de la derecha resulta conmutativo, Pero por el Ejercicio 15 de la Práctica 6=, tenemos que

$$(g^A \times \text{id}_A) \circ (f^A \times \text{id}_A) = (g^A \circ f^A) \times \text{id}_A$$

Por otra parte, $(g \circ f)^A \times \text{id}_A$ hace conmutativo el diagrama

$$\begin{array}{ccc}
 D^A & & D^A \times A \xrightarrow{\text{eval}_D} D \\
 \uparrow (g \circ f)^A & & \uparrow (g \circ f)^A \times \text{id}_A \\
 B^A & & B^A \times A \xrightarrow{\text{eval}_B} B
 \end{array}
 \quad \begin{array}{c} \\ \\ \uparrow g \circ f \end{array}$$

y por lo tanto $(g \circ f)^A = g^A \circ f^A$, esto es, $\exp_A(g \circ f) = \exp_A(f) \circ \exp_A(g)$. ■

Ejemplo 6.9.4. El funtor contravariante B^- . Condieremos ahora una categoría con exponenciales \mathcal{C} y fijemos $B \in \mathcal{C}$. Pongamos $F_B : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{C}$ tal que

$$F_B(A) = B^A.$$

Denotemos por $\text{eval}^B : B^A \times A \rightarrow B$ y $\text{eval}^C : B^C \times C \rightarrow B$ las funciones eval para las exponenciales B^A y B^C respectivamente. Si $f \in \text{Hom}(A, C)$, definamos

$$\varphi = \text{eval}^C \circ (\text{id}_{B^C} \times f) : B^C \times A \rightarrow B$$

$$\begin{array}{ccccc}
 B^C \times A & \xrightarrow{\text{id}_{B^C} \times f} & B^C \times C & \xrightarrow{\text{eval}^C} & B \\
 & \searrow \varphi & & \nearrow & \\
 & & & &
 \end{array}$$

Entonces existe un único morfismo $\text{curry}(\varphi) : B^C \rightarrow B^A$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc}
 B^A & & B^A \times A \xrightarrow{\text{eval}^B} B \\
 \uparrow \text{curry}(\varphi) & & \uparrow \text{curry}(\varphi) \times \text{id}_A \\
 B^C & & B^C \times A
 \end{array}
 \quad \begin{array}{c} \\ \\ \nearrow \varphi \end{array}$$

Por lo tanto podemos definir $F_B : \text{Hom}(A, C) \rightarrow \text{Hom}(B^C, B^A)$ por

$$F_B(f) = \text{curry}(\text{eval}^C \circ (\text{id}_{B^C} \times f)).$$

Dejamos como ejercicio verificar que F_B es efectivamente un funtor contravariante. ■

Para finalizar esta unidad, introduciremos el concepto de *categoría cartesiana cerrada*.

Definición 6.9.5. Sea \mathcal{C} una categoría. Decimos que \mathcal{C} es una **categoría cartesiana cerrada (CCC)** si \mathcal{C} tiene objeto terminal y es una categoría con productos y con exponenciales.

Ejemplo 6.9.6. Set es una categoría cartesiana cerrada: todo singulete $\{x\}$ es un objeto terminal, y Set es una categoría con productos y exponenciales. Poset también es una categoría cartesiana cerrada: todo conjunto de cardinal 1 con el orden trivial es un poset que es un objeto terminal en Poset. Además como vimos en los ejemplos anteriores, Poset es una categoría con productos y exponenciales. ■

Ejemplo 6.9.7. Sea B un álgebra de Boole y sea \mathcal{C}_B la categoría asociada. Como B es un retículo, \mathcal{C}_B es una categoría con productos (Ejemplo 6.6.6). Además B es un retículo acotado y por lo tanto 1 es un objeto terminal de \mathcal{C}_B (Ejemplo 6.5.5). Veamos que \mathcal{C}_B es una categoría con exponenciales. Sean $x, y \in B = \text{ob } \mathcal{C}_B$. Recordemos que B es un retículo complementado, por lo tanto podemos considerar $y^c \in B$ tal que $y \wedge y^c = 0$, $y \vee y^c = 1$. Pongamos

$$x^y := y^c \vee x.$$

Veamos que efectivamente x^y es un exponencial en \mathcal{C}_B . Recordemos que para cualquier par de objetos a, b en \mathcal{C}_B existe un morfismo $f \in \text{Hom}(a, b)$ si y sólo si $a \preceq b$, en cuyo caso $f = (a, b)$. Por lo tanto hay un único morfismo posible $\text{eval} : x^y \times y \rightarrow x$, y éste existe sí y sólo si $x^y \times y \preceq x$. Pero como B es un retículo distributivo,

$$x^y \times y = x^y \wedge y = (y^c \vee x) \wedge y = (y^c \wedge y) \vee (x \wedge y) = 0 \vee (x \wedge y) = x \wedge y \preceq x.$$

Consideremos ahora $z \in B = \text{ob } \mathcal{C}_B$ tal que existe un morfismo $g : z \times y \rightarrow x$, es decir, tal que

$$(6.20) \quad z \wedge y \preceq x \iff (z \wedge y) \vee x = x$$

Nuevamente, el único candidato a $\text{curry}(g) : z \rightarrow x^y$ es el morfismo (z, x^y) que existe si y sólo si $z \preceq x^y$. En efecto:

$$\begin{aligned} z \vee x^y &= z \vee (y^c \vee x) = (z \wedge 0) \vee (y^c \vee x) = (z \wedge (y \vee y^c)) \vee (y^c \vee x) \\ &= [(z \wedge y) \vee (z \wedge y^c)] \vee (y^c \vee x) = (z \wedge y) \vee [(z \wedge y^c) \vee (y^c \vee x)] \\ &= (z \wedge y) \vee (y^c \vee x) = [(z \wedge y) \vee x] \vee y^c = x \vee y^c \\ &= x^y \end{aligned}$$

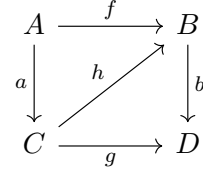
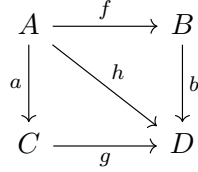
Finalmente, el morfismo producto $g \times \text{id}_y$ está dado por $(z \wedge y, x^y \wedge y)$ y verifica que

$$\text{eval} \circ (\text{curry}(g) \times \text{id}_y) = (x^y \wedge y, x) \circ (z \wedge y, x^y \wedge y) = (z \wedge y, x) = g.$$

Concluimos que \mathcal{C}_B es una categoría cartesiana cerrada. ■

6.10. Ejercicios

1. Considerar los siguientes diagramas en una categoría \mathcal{C} . En ambos casos, probar que si los dos triángulos interiores conmutan, también conmuta el cuadrado exterior.



2. Probar que si \mathcal{C} es una categoría con un único objeto, entonces $\mathcal{C} = \mathcal{C}_M$ para algún monoide $(M, *)$.
3. Sea \mathcal{C} tal que $\text{ob } \mathcal{C} = \mathbb{N}$, $\text{mor } \mathcal{C}$ es el conjunto de todas las matrices a coeficientes reales de modo que $M \in \text{Hom}(m, n)$ si M es una matriz $m \times n$ y la composición es el producto de matrices. Definir funciones dominio y codominio e identidades adecuadas y probar que \mathcal{C} es efectivamente una categoría.
4. Sea Rel tal que ob Rel es la clase de conjuntos, mor Rel son las relaciones binarias entre conjuntos y la composición de morfismos es la composición de relaciones. Definir funciones dominio y codominio e identidades adecuadas y probar que Rel es efectivamente una categoría, denominada *categoría de relaciones*.
5. Sea Pset tal que ob Pset son pares (X, x_0) donde X es un conjunto y $x_0 \in X$. El par (X, x_0) se denomina un *conjunto punteado*. Una función entre los conjuntos punteados (X, x_0) e (Y, y_0) es una función $f: X \rightarrow Y$ tal que $f(x_0) = y_0$. Probar que si mor Pset son funciones entre conjuntos punteados, con la composición usual de funciones y las identidades usuales, Pset es una categoría.
6. Sean \mathcal{C} una categoría y A un objeto de \mathcal{C} . Definimos $\mathcal{C}|A$ como la categoría cuyos objetos son las flechas f de \mathcal{C} tales que $\text{codom}(f) = A$. Una flecha g en $\mathcal{C}|A$ de $f: X \rightarrow A$ en $h: Y \rightarrow A$ es una flecha $g: X \rightarrow Y$ de \mathcal{C} tal que $f = h \circ g$.
 - a) Expresar las flechas de $\mathcal{C}|A$ en términos de diagramas conmutativos.
 - b) Verificar que $\mathcal{C}|A$ es una categoría.
 - c) Si \mathcal{C}_P es la categoría definida por un conjunto ordenado P y $x \in P$, determinar $\mathcal{C}_P|x$.
7. Probar en las siguientes inclusiones que cada categoría dada es una subcategoría de la siguiente. Determinar en cada caso si se trata de subcategorías full.

a) $\text{Grp} \subseteq \text{Mon}$.

b) $\text{Mon} \subseteq \text{Sgrp}$.

c) $\text{Set} \subseteq \text{Rel}$.

8. Sean \mathcal{C} y \mathcal{D} dos categorías y sean $P_1: \mathcal{C} \times \mathcal{D} \rightarrow \mathcal{C}$ tal que $P_1(C, D) = C$ y $P_2: \mathcal{C} \times \mathcal{D} \rightarrow \mathcal{D}$ tal que $P_2(C, D) = D$. Definir P_1 y P_2 sobre $\text{mor } \mathcal{C} \times \mathcal{D}$ de modo que P_1 y P_2 sean funtores.

9. Sea \mathcal{C} una categoría tal que $\text{ob } \mathcal{C} = \{X, Y, X', Y'\}$ y $\text{mor } \mathcal{C} = \{\text{id}_X, \text{id}_Y, \text{id}_{Y'}, \text{id}_Z, p, q\}$ con $\text{Hom}_{\mathcal{C}}(X, Y) = \{p\}$, $\text{Hom}_{\mathcal{C}}(Y', Z) = \{q\}$. \mathcal{C} puede representarse completamente mediante el siguiente diagrama:

$$\begin{array}{ccccc} \text{id}_X & & \text{id}_Y & & \text{id}_{Y'} & & \text{id}_Z \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ X & \xrightarrow{p} & Y & & Y' & \xrightarrow{q} & Z \end{array}$$

Consideremos la categoría **2** dada por el siguiente diagrama conmutativo:

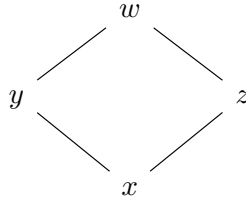
$$\begin{array}{ccccc} & & \text{id}_B & & \\ & & \downarrow & & \\ & & B & & \\ f \nearrow & & & & \searrow g \\ \text{id}_A \hookrightarrow A & \xrightarrow{h} & C & \hookrightarrow & \text{id}_C \end{array}$$

Sea $F : \mathcal{C} \rightarrow \mathbf{2}$ tal que $F(X) = A$, $F(Y) = F(Y') = B$, $F(Z) = C$, $F(p) = f$, $F(q) = g$ y F mapea las identidades en \mathcal{C} en las respectivas identidades en **2**.

- Probar que F es un funtor fiel pero no full.
 - Probar que poniendo $\text{Im}(F)$ tal que $\text{ob } \text{Im}(F) = \{F(O) : O \in \text{ob } \mathcal{C}\}$, $\text{mor } \text{Im}(F) = \{F(x) : x \in \text{mor } \mathcal{C}\}$, $\text{Im}(F)$ no es una categoría. Esto es, la imagen de una categoría por un funtor no necesariamente es una subcategoría del codominio.
10. Sea M un monoide y G_M el grupo de elementos invertibles de M .
- Si $f : M \rightarrow M'$ es un morfismo de monoides, probar que $f(G_M) \subseteq G_{M'}$ y $\tilde{f} : G_M \rightarrow G_{M'}$ tal que $\tilde{f}(x) = f(x)$ es un homomorfismo de grupos.
 - Probar que $F : \text{Mon} \rightarrow \text{Grp}$ tal que $F(M) = G_M$ para cada moniide M y $F(f) = \tilde{f}$ para cada morfismo de monoides es un funtor covariante.
11. Sean P, P' posets y M, M' monoides.
- Probar que si $F : \mathcal{C}_P \rightarrow \mathcal{C}_{P'}$ es un funtor, entonces $F : \text{ob } \mathcal{C}_P \rightarrow \text{ob } \mathcal{C}_{P'}$ es un homomorfismo de orden.
 - Probar que si $F : \mathcal{C}_M \rightarrow \mathcal{C}_{M'}$ es un funtor, entonces $F : \text{mor } \mathcal{C}_M \rightarrow \text{mor } \mathcal{C}_{M'}$ es un homomorfismo de monoides.
12. Sea Rel la categoría de relaciones del ejercicio 4. Probar que $F : \text{Rel} \rightarrow \text{Rel}^{\text{op}}$ dada por $F(A) = A$ para cada $A \in \text{ob } \text{Rel}$, $F(\mathcal{R}) = \mathcal{R}^{-1}$ para cada relación $\mathcal{R} \in \text{mor } \text{Rel}$ es un isomorfismo de categorías.
13. Sean \mathcal{C} una categoría y f, g flechas de \mathcal{C} . Probar que
- Si f y g son monomorfismos, entonces $g \circ f$ también lo es.
 - Si $g \circ f$ es un monomorfismo, f también lo es.
 - Si f y g son epimorfismos, entonces $g \circ f$ también lo es.
 - Si $g \circ f$ es un epimorfismo, g también lo es.
 - Si f^{-1} es la inversa de f y g^{-1} es la inversa de g , entonces $f^{-1} \circ g^{-1}$ es la inversa de $g \circ f$.
14. Sean P un poset y M un monoide. Determinar los epimorfismos y los isomorfismos en \mathcal{C}_P y \mathcal{C}_M .

15. Sea \mathcal{D} la subclase de $\mathbf{ob Ret}$ formada por los retículos distributivos.

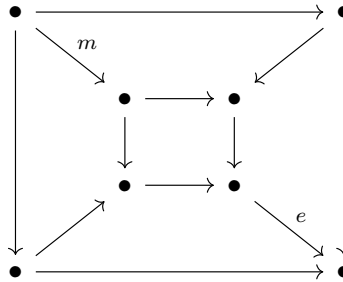
- Probar que \mathbf{DisRet} tal que $\mathbf{ob DisRet} = \mathcal{D}$, $\mathbf{Hom}_{\mathbf{DisRet}}(X, Y) = \mathbf{Hom}_{\mathbf{Ret}}(X, Y)$ es una subcategoría full de \mathbf{Ret} .
- Sean $L_1 = a, b, c$ el conjunto totalmente ordenado tal que $a \prec b \prec c$ y sea $L_2 = \{x, y, z, w\}$ el retículos cuyo diagrama de Hasse es el siguiente:



Probar que $f : L_1 \rightarrow L_2$ tal que $f(a) = x$, $f(b) = y$, $f(c) = z$ es un morfismo épico en \mathbf{DisRet} , pero no es épico en \mathbf{Ret} .

- Probar que en \mathbf{Ret} , un morfismo es épico si y sólo si es un homomorfismo de retículos sobre-
yectivo.

16. Considerar que en el siguiente diagrama los 4 trapecios conmutan



Probar que

- Si el cuadrado interno conmuta, también lo hace el cuadrado externo.
- Si e es un morfismo épico y m es un morfismo mónico, entonces si el cuadrado externo conmuta, también lo hace el cuadrado interno.

17. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor y sea $f \in \mathbf{mor} \mathcal{C}$.

- Probar que si f es un isomorfismo en \mathcal{C} , entonces $F(f)$ es un isomorfismo en \mathcal{D} .
- Probar que la recíproca del ítem anterior es falsa, incluso si F es un funtor fiel.

18. Sea \mathcal{C} una categoría y \mathcal{C}^{op} su categoría dual.

- Probar que $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$ es un monomorfismo si y solo si $f \in \mathbf{Hom}_{\mathcal{C}^{op}}(B, A)$ es un epimorfismo.
- Probar que $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$ es un epimorfismo si y solo si $f \in \mathbf{Hom}_{\mathcal{C}^{op}}(B, A)$ es un monomorfismo.
- Probar que $f \in \mathbf{Hom}_{\mathcal{C}}(A, B)$ es un isomorfismo si y sólo si $f \in \mathbf{Hom}_{\mathcal{C}^{op}}(B, A)$ es un isomorfismo.
- Probar que A es un objeto inicial (resp. terminal) en \mathcal{C} si y sólo si A es un objeto terminal (resp. inicial) en \mathcal{C}^{op} .

19. Determinar, si existen, los objetos iniciales, terminales y nulos en las siguientes categorías:

- a) Sgrp b) Mon c) Poset d) Ret e) Rel

20. Dar una categoría sin objetos iniciales. Dar una sin objetos terminales. Dar una donde los objetos terminales e iniciales coincidan.

21. Sean A y B objetos en una categoría \mathcal{C} . Un A, B -pairing se define como una terna (P, p_1, p_2) donde P es un objeto de \mathcal{C} y $p_1 : P \rightarrow A$ y $p_2 : P \rightarrow B$ son morfismos de \mathcal{C} . Un morfismo de A, B -pairings

$$f : (P, p_1, p_2) \rightarrow (Q, q_1, q_2)$$

es cualquier morfismo f de \mathcal{C} tal que $q_1 \circ f = p_1$ y $q_2 \circ f = p_2$, es decir, el siguiente diagrama conmuta.

$$\begin{array}{ccc} P & \xrightarrow{f} & Q \\ \downarrow p_1 & & \downarrow q_2 \\ & \searrow p_2 \quad \swarrow q_1 & \\ A & & B \end{array}$$

- a) Probar que los A, B -pairings y sus morfismos forman una categoría $\text{Pair}(A, B)$.
b) Siendo 0 un objeto inicial de \mathcal{C} , mostrar que

$$\begin{array}{ccc} & 0 & \\ \swarrow !_A & & \searrow !_B \\ A & & B \end{array}$$

es un objeto inicial de $\text{Pair}(A, B)$.

22. Probar que si $F : \mathcal{C} \rightarrow \mathcal{D}$ es un isomorfismo de categorías, entonces:

- a) A es un objeto inicial (resp. terminal) de \mathcal{C} si y sólo si $F(A)$ es un objeto inicial (resp. terminal) de \mathcal{D} .
b) Existe en \mathcal{C} el producto (resp. el coproducto) de A y B si y solo si existe en \mathcal{D} el producto (resp. el coproducto) de $F(A)$ y $F(B)$.

23. Sea \mathcal{C} una categoría y $A, B \in \text{ob } \mathcal{C}$ tales que existe el producto $(A \times B, \pi_A, \pi_B)$. Sea $S \in \text{ob } \mathcal{C}$ y $u, v : S \rightarrow A \times B$. Probar que si $\pi_A \circ u = \pi_A \circ v$ y $\pi_B \circ u = \pi_B \circ v$, entonces $u = v$.

24. Sea \mathcal{C} una categoría con productos. Mostrar las siguientes identidades (los morfismos y las composiciones están definidas donde tengan sentido):

- a) $\langle \pi_1, \pi_2 \rangle = \text{id}$
b) $\langle f \circ h, g \circ h \rangle = \langle f, g \rangle \circ h$
c) $(f \times h) \circ \langle g, k \rangle = \langle f \circ g, h \circ k \rangle$
d) $(f \times h) \circ (g \times k) = (f \circ g) \times (h \circ k)$
e) $\langle [f, g], [h, k] \rangle = [\langle f, h \rangle, \langle g, k \rangle]$

25. Sea \mathcal{C} una categoría con productos y supongamos que 1 es un objeto terminal de \mathcal{C} . Probar los siguientes isomorfismos:

$$a) A \times B \cong B \times A$$

$$b) A \times 1 \cong A$$

$$c) A \times (B \times C) \cong (A \times B) \times C$$

¿Cuáles son los enunciados duales?

26. Sea \mathcal{D} un diagrama en una categoría \mathcal{C} y sea $\text{Cone}(\mathcal{D})$ la categoría de conos sobre \mathcal{D} . Sean $(X, \mathcal{F}_{\text{diag}})$ y $(X', \mathcal{F}'_{\mathcal{D}})$ conos sobre \mathcal{D} y $k : (X', \mathcal{F}'_{\mathcal{D}}) \rightarrow (X, \mathcal{F}_{\mathcal{D}})$ un morfismo de conos. Probar que k es un morfismo mónico (resp. un morfismo épico, un isomorfismo) en $\text{Cone}(\mathcal{D})$ si y sólo si $k : X' \rightarrow X$ es un morfismo mónico (resp. un morfismo épico, un isomorfismo) en \mathcal{C} .
27. Sea \mathcal{D} un diagrama en una categoría \mathcal{C} y sea $\text{Cone}(\mathcal{D})$ la categoría de conos sobre \mathcal{D} . Probar que $(X, \mathcal{F}_{\mathcal{D}})$ es un límite para \mathcal{D} si y sólo si $(X, \mathcal{F}_{\mathcal{D}})$ es un objeto terminal de $\text{Cone}(\mathcal{D})$.
28. Sea \mathcal{C} una categoría y \mathcal{D} un diagrama en \mathcal{C} . Definir de manera adecuada una categoría de los coconos sobre \mathcal{D} y probar que un colímite para \mathcal{D} es un objeto inicial en esta categoría.
29. Encontrar el pullback de dos morfismos en Sgrp , Mon y Grp .
30. Sea \mathcal{C} una categoría con exponenciales,
- Probar que $\text{curry}(\text{eval}_{A,B}) = \text{id}_{B^A}$.
 - Dado un morfismo $f : B \rightarrow C$, construir un morfismo $B^A \rightarrow C^A$.
 - Dado un morfismo $f : A \rightarrow C^B$, construir un morfismo $\text{uncurry}(f) : A \times B \rightarrow C$.
 - Probar que $\text{uncurry}(\text{curry}(f)) = f$ y $\text{curry}(\text{uncurry}(f)) = f$.
31. Sea \mathcal{C} una CCC y sean A, B objetos de \mathcal{C} . Probar que:
- B^A es único salvo isomorfismo.
 - $1^A \cong 1$.
 - $B^1 \cong B$.
32. En una categoría con coproductos y objeto terminal 1 , podemos definir los booleanos como el objeto $\text{Bool} = 1 + 1$. En este caso, a i_1 le llamamos *true* y a i_2 le llamamos *false*. Escribir un morfismo $\text{not} : \text{Bool} \rightarrow \text{Bool}$ tal que

$$\text{not} \circ \text{true} = \text{false}$$

$$\text{not} \circ \text{false} = \text{true}$$

Suponiendo que la categoría tiene exponenciales, ¿puede escribir un morfismo $\text{and} : \text{Bool} \times \text{Bool} \rightarrow \text{Bool}$ que se comporte como la conjunción?

Equivalencias, adjunciones y mónadas

7.1. Transformaciones naturales

Como ya hemos mencionado en el Capítulo 6, la noción de categorías isomorfas (o anti-isomorfas) resulta demasiado restrictiva. Una noción más amplia y que tiene muchas más aplicaciones prevee que las composiciones $F \circ G$ y $G \circ F$ no necesariamente sean los funtores identidad, sino que sean *equivalentes* a ellos en un cierto sentido *natural*. Para poder definir estos conceptos necesitamos introducir la noción de *transformaciones naturales* entre funtores:

Definición 7.1.1. Sean \mathcal{C} y \mathcal{D} dos categorías y sean $F, G : \mathcal{C} \rightarrow \mathcal{D}$ dos funtores de \mathcal{C} en \mathcal{D} . Una **transformación natural** de F en G , denotada $\eta : F \rightarrow G$, es una función de clases $\eta : \text{ob } \mathcal{C} \rightarrow \text{mor } \mathcal{D}$ tal que:

1. para cada objeto A de \mathcal{C} , $\eta_A = \eta(A) \in \text{Hom}_{\mathcal{D}}(F(A), G(A))$
2. para cada morfismo $f \in \text{Hom}_{\mathcal{C}}(A, B)$, el siguiente diagrama en \mathcal{D} es conmutativo:

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ F(f) \downarrow & & \downarrow G(f) \\ F(B) & \xrightarrow{\eta_B} & G(B) \end{array}$$

es decir,

$$\eta_B \circ F(f) = G(f) \circ \eta_A.$$

Si cada morfismo η_A es un isomorfismo en \mathcal{D} , η se dice un **isomorfismo natural**. Si existe un isomorfismo natural $\eta : F \rightarrow G$ decimos que F y G son **naturalmente isomorfos** y lo denotamos $F \xrightarrow{\eta} G$.

Ejemplo 7.1.2. Isomorfismo natural identidad. Si $F : \mathcal{C} \rightarrow \mathcal{D}$ es un funtor, poniendo $\eta_A = \text{id}_{F(A)}$ para cada $A \in \mathcal{C}$, resulta trivial que η es un isomorfismo natural de F en F . Lo denominamos **isomorfismo natural identidad** de F y lo denotamos id_F . ■

Ejemplo 7.1.3. Sea \mathcal{C} una categoría con productos y sean \times_A y \times^A los funtores producto definidos en el Ejemplo 6.6.10, esto es,

$$\times_A = A \times -, \quad \times^A = - \times A.$$

Para cada $B \in \text{ob } \mathcal{C}$, tenemos los productos $(A \times B, \pi_A, \pi_B)$ y $(B \times A, \tilde{\pi}_B, \tilde{\pi}_A)$ para los cuales el siguiente diagrama conmuta:

$$\begin{array}{ccccc} & & A \times B & & \\ & \swarrow \pi_B & \downarrow \eta_B & \searrow \pi_A & \\ B & \xleftarrow{\tilde{\pi}_B} & B \times A & \xrightarrow{\tilde{\pi}_A} & A \end{array}$$

donde $\eta_B = \langle \pi_B, \pi_A \rangle \in \text{Hom}(A \times B, B \times A) = \text{Hom}(\times_A(B), \times^A(B))$. No es difícil ver que de hecho η_B es un isomorfismo para cada $B \in \text{ob } \mathcal{C}$ (ver el Ejercicio 25 del Capítulo 6).

Para ver que $\eta : \times_A \rightarrow \times^A$ define un isomorfismo natural debemos considerar $f \in \text{Hom}_{\mathcal{C}}(B, C)$ y probar que el diagrama siguiente conmuta:

$$\begin{array}{ccc} A \times B & \xrightarrow{\eta_B} & B \times A \\ \text{id}_A \times f = \times_A(f) \downarrow & & \downarrow \times^A(f) = f \times \text{id}_A \\ A \times C & \xrightarrow{\eta_C} & C \times A \end{array}$$

Analicemos la composición $\times^A(f) \circ \eta_B$. Usaremos la siguiente notación para las proyecciones en los distintos productos:

$$\begin{aligned} \pi_A : A \times B &\rightarrow A, \quad \pi_B : A \times B \rightarrow B, \quad \tilde{\pi}_A : B \times A \rightarrow A, \quad \tilde{\pi}_B : B \times A \rightarrow B \\ p_A : A \times C &\rightarrow A, \quad p_C : A \times C \rightarrow C, \quad \tilde{p}_A : C \times A \rightarrow A, \quad \tilde{p}_C : C \times A \rightarrow C. \end{aligned}$$

Entonces $\times^A(f) \circ \eta_B$ es un morfismo que hace conmutar el siguiente diagrama:

$$\begin{array}{ccccc} & & A \times B & & \\ & \swarrow \pi_B & \downarrow \eta_B & \searrow \pi_A & \\ B & \xleftarrow{\tilde{\pi}_B} & B \times A & \xrightarrow{\tilde{\pi}_A} & A \\ f \downarrow & & \downarrow \times^A(f) & & \downarrow \text{id}_A \\ C & \xleftarrow{\tilde{p}_C} & C \times A & \xrightarrow{\tilde{p}_A} & A \end{array}$$

Por lo tanto también conmuta el diagrama

$$(7.1) \quad \begin{array}{ccccc} & & A \times B & & \\ & \swarrow f \circ \pi_B & \downarrow \times^A(f) \circ \eta_B & \searrow \pi_A & \\ C & \xleftarrow{\tilde{p}_C} & C \times A & \xrightarrow{\tilde{p}_A} & A \end{array}$$

De manera similar, el morfismo $\eta_C \circ \times_A(f)$ hace conmutar los siguientes diagramas:

$$(7.2) \quad \begin{array}{ccccc} & A \times B & & & \\ & \swarrow \pi_A \quad \downarrow \times_A(f) \quad \searrow f \circ \pi_B & & & \\ A & \xleftarrow{p_A} & A \times C & \xrightarrow{p_C} & C \\ \downarrow \text{id}_A & & \downarrow \eta_C & & \downarrow \text{id}_C \\ A & \xleftarrow{\tilde{p}_A} & C \times A & \xrightarrow{\tilde{p}_C} & C \end{array} \quad \rightsquigarrow \quad \begin{array}{ccccc} & A \times B & & & \\ & \swarrow \pi_A \quad \downarrow \eta_C \circ \times_A(f) \quad \searrow f \circ \pi_B & & & \\ A & \xleftarrow{\tilde{p}_A} & C \times A & \xrightarrow{\tilde{p}_C} & C \end{array}$$

Si observamos el diagrama (7.1) y el diagrama de la derecha en (7.2), vemos que los triángulos exteriores son esencialmente los mismos. Como existe un único morfismo que hace conmutar el diagrama

$$\begin{array}{ccccc} & A \times B & & & \\ & \swarrow \pi_A \quad \downarrow \text{---} \quad \searrow f \circ \pi_B & & & \\ A & \xleftarrow{\tilde{p}_A} & C \times A & \xrightarrow{\tilde{p}_C} & C \end{array}$$

concluimos que

$$\times^A(f) \circ \eta_B = \eta_C \circ \times_A(f)$$

como queríamos probar. ■

Ejemplo 7.1.4. Consideremos una categoría \mathcal{C} con exponenciales y sea A un objeto fijo de \mathcal{C} . Pongamos $F_A : \mathcal{C} \rightarrow \mathcal{C}$ el funtor $F_A = \times^A \circ \exp_A$, esto es:

- $F_A(B) = B^A \times A$,
- Si $f \in \text{Hom}(B, C)$,

$$F_A(f) = \times^A \circ \exp_A(f) = f^A \times \text{id}_A.$$

Pongamos $\eta_B = \text{eval}_B : B^A \times A \rightarrow B$. Entonces $\eta : F_A \rightarrow \text{Id}$ es una transformación natural. En efecto, si $f \in \text{Hom}(B, C)$ vimos en el Ejemplo 6.9.3 que el siguiente diagrama conmuta:

$$\begin{array}{ccc} C^A \times A & \xrightarrow{\text{eval}_C} & C \\ \uparrow f^A \times \text{id}_A & & \uparrow f \\ B^A \times A & \xrightarrow{\text{eval}_B} & B \end{array}$$

En términos de los funtores F_A , Id y la transformación η lo podemos reescribir como

$$\begin{array}{ccc} F_A(B) & \xrightarrow{\eta_B} & \text{Id}(B) \\ \downarrow F(f) & & \downarrow \text{Id}(f) \\ F_A(C) & \xrightarrow{\eta_C} & \text{Id}(C) \end{array}$$

con $\text{Id}(f) \circ \eta_B = \eta_C \circ F(f)$ ■

Ejemplo 7.1.5. Composición de transformaciones naturales Sean \mathcal{C} y \mathcal{D} dos categorías y sean $F, G, H : \mathcal{C} \rightarrow \mathcal{D}$ funtores. Supongamos que existen transformaciones naturales $\eta : F \rightarrow G$ y $\tau : G \rightarrow H$. Pongamos $\tau \circ \eta : F \rightarrow H$ de modo que $\tau \circ \eta(A) = \tau_A \circ \eta_A$. Tenemos entonces el siguiente diagrama para cada par de objetos A, B de \mathcal{C} y cada $f \in \text{Hom}(A, B)$:

$$(7.3) \quad \begin{array}{ccccc} F(A) & \xrightarrow{\eta_A} & G(A) & \xrightarrow{\tau_A} & H(A) \\ F(f) \downarrow & & \downarrow G(f) & & \downarrow H(f) \\ F(B) & \xrightarrow{\eta_B} & G(B) & \xrightarrow{\tau_B} & H(B) \end{array}$$

Como los cuadrados interiores del diagrama (7.3) conmutan, conmuta el rectángulo exterior, esto es, el siguiente diagrama conmuta:

$$\begin{array}{ccc} F(A) & \xrightarrow{\tau_A \circ \eta_A} & H(A) \\ F(f) \downarrow & & \downarrow H(f) \\ F(B) & \xrightarrow{\tau_B \circ \eta_B} & H(B) \end{array}$$

y por lo tanto $\tau \circ \eta$ es una transformación natural de F en H . Como la composición de isomorfismos en una categoría es un isomorfismos, resulta que si η y τ son isomorfismos naturales, entonces $\tau \circ \eta$ es un isomorfismo natural. ■

Ejemplo 7.1.6. La categoría de funtores $\mathcal{D}^{\mathcal{C}}$. Sean \mathcal{C} y \mathcal{D} dos categorías y pongamos $\mathcal{D}^{\mathcal{C}}$ tal que los objetos de $\mathcal{D}^{\mathcal{C}}$ son los funtores de \mathcal{C} en \mathcal{D} y los morfismos son transformaciones naturales entre funtores.

Las funciones dom y codom son las obvias y la composición es la composición de transformaciones naturales, que como vimos en el Ejemplo 7.1.5 está bien definida.

Para cada funtor $F : \mathcal{C} \rightarrow \mathcal{D}$, el isomorfismo natural identidad $\text{id}_F : F \rightarrow F$ tal que $\text{id}_F(A) := \text{id}_{F(A)}$ es una transformación natural (ver Ejemplo 7.1.2) y es inmediato verificar que si $\eta : F \rightarrow G$ es una transformación natural entre F y G , entonces

$$\eta \circ \text{id}_F = \eta, \quad \text{id}_G \circ \eta = \eta$$

con lo cual id_F es una identidad en $\mathcal{D}^{\mathcal{C}}$.

Finalmente, si $\eta : F \rightarrow G$, $\tau : G \rightarrow H$ y $\rho : H \rightarrow N$ son transformaciones naturales, entonces

$$\rho \circ (\tau \circ \eta)(A) = \rho_A \circ (\tau_A \circ \eta_A) = (\rho_A \circ \tau_A) \circ \eta_A = (\rho \circ \tau) \circ \eta(A)$$

con lo cual la composición es asociativa. Concluimos que $\mathcal{D}^{\mathcal{C}}$ es una categoría.

La categoría $\mathcal{D}^{\mathcal{C}}$ es particularmente importante dado que muchas categorías son categorías de funtores “disfrazadas”. ■

Ejemplo 7.1.7. En Cat , $\mathcal{C}^1 \simeq \mathcal{C}$. Recordemos que $\mathbf{1}$ es la categoría con un único objeto, pongamos $\text{ob } \mathbf{1} = \{*\}$ y un único morfismo, id_* . Sea \mathcal{C} una categoría cualquiera en Cat (la categoría de categorías pequeñas, ver Ejemplo 6.3.8). Si $\text{ob } \mathcal{C} = \emptyset$, entonces $\text{mor } \mathcal{C} = \emptyset$ y $\mathcal{C}^1 = \mathcal{C}$. Supondremos entonces que $\text{ob } \mathcal{C}$ es un conjunto no vacío. Cada funtor de $\mathbf{1}$ en \mathcal{C} está completamente determinado por algún elemento

de $\text{ob } \mathcal{C}$, pues en efecto, una vez que fijamos $x \in \text{ob } \mathcal{C}$, existe un único funtor $F_x : \mathbf{1} \rightarrow \mathcal{C}$ que es aquel definido por $F_x(*) = x$, $F(\text{id}_*) = \text{id}_x$. Ahora bien, si $f \in \text{Hom}_{\mathcal{C}}(x, y)$ es un morfismo cualquiera de x en y , entonces $\eta(*) = f$ define una transformación natural $\eta : F_x \rightarrow F_y$: en efecto, el siguiente diagrama conmuta trivialmente:

$$\begin{array}{ccc} x = F_x(*) & \xrightarrow{f} & y = F_y(*) \\ \text{id}_x = F_x(\text{id}_*) \downarrow & & \downarrow \text{id}_y = F_y(\text{id}_*) \\ x = F_x(*) & \xrightarrow{f} & y = F_y(*) \end{array}$$

Ahora bien, los objetos de $\mathcal{C}^{\mathbf{1}}$ son los funtores de $\mathbf{1}$ en \mathcal{C} y los morfismos son las transformaciones naturales entre funtores. Por otra parte, en Cat , los morfismos son funtores entre categorías. Pongamos entonces $\tilde{F} : \mathcal{C}^{\mathbf{1}} \rightarrow \mathcal{C}$, $\tilde{F}(F) = F(*)$, $\tilde{F}(\eta) = \eta(*)$, entonces es claro que \tilde{F} es un funtor. Además $\hat{F} : \mathcal{C} \rightarrow \mathcal{C}^{\mathbf{1}}$ dado por $\hat{F}(x) = F_x$ y $\hat{F}(f) = \eta$ tal que $\eta(*) = f$ también es un funtor, y es fácil verificar que $\hat{F} \circ \tilde{F} = \text{Id}_{\mathcal{C}^{\mathbf{1}}}$, $\tilde{F} \circ \hat{F} = \text{Id}_{\mathcal{C}}$ con lo cual \tilde{F} es un isomorfismo de Cat . ■

7.2. Equivalencias de categorías

Definición 7.2.1. Sean \mathcal{C} y \mathcal{D} dos categorías. Una **equivalencia de categorías** entre \mathcal{C} y \mathcal{D} consiste de dos funtores $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ y dos isomorfismos naturales $\eta : \text{Id}_{\mathcal{C}} \rightarrow G \circ F$ y $\tau : \text{Id}_{\mathcal{D}} \rightarrow F \circ G$. En ese caso decimos que F (y análogamente G) **define una equivalencia** entre \mathcal{C} y \mathcal{D} .

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ f \downarrow & & \downarrow G(F(f)) \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array} \quad \begin{array}{ccc} A' & \xrightarrow{\tau_{A'}} & F(G(A')) \\ g \downarrow & & \downarrow F(G(g)) \\ B' & \xrightarrow{\tau_{B'}} & F(G(B')) \end{array}$$

Si existe una equivalencia de categorías entre \mathcal{C} y \mathcal{D} , decimos que \mathcal{C} y \mathcal{D} son **categorías equivalentes**.

Esencialmente, una equivalencia entre una categoría \mathcal{C} y una categoría \mathcal{D} mapea un objeto A de \mathcal{C} en uno de \mathcal{D} por F , y a su vez lo devuelve a un objeto A' de \mathcal{C} por G que es isomorfo a A . Es decir, \mathcal{C} y \mathcal{D} son esencialmente la misma categoría salvo objetos isomorfos.

Como existe un isomorfismo natural identidad de un funtor en si mismo (Ejemplo 7.1.2), la noción de equivalencia es “simétrica” (en el sentido que pueden intercambiarse los roles de los funtores F y G) y la composición de isomorfismos naturales es un isomorfismo natural (ver Ejemplo 7.1.5), tenemos el siguiente resultado, cuya prueba dejamos como **ejercicio**:

Lema 7.2.2. Sean \mathcal{C}_1 , \mathcal{C}_2 y \mathcal{C}_3 categorías.

1. \mathcal{C}_1 es equivalente a \mathcal{C}_1 .
2. Si \mathcal{C}_1 es equivalente a \mathcal{C}_2 entonces \mathcal{C}_2 es equivalente a \mathcal{C}_1 .
3. Si \mathcal{C}_1 es equivalente a \mathcal{C}_2 y \mathcal{C}_2 es equivalente a \mathcal{C}_3 , entonces \mathcal{C}_1 es equivalente a \mathcal{C}_3 .

La noción de categorías equivalentes generaliza la noción de categorías isomorfas. En efecto:

Teorema 7.2.3. *Sean \mathcal{C} y \mathcal{D} dos categorías. Si \mathcal{C} y \mathcal{D} son isomorfas, entonces son equivalentes.*

Demostración. Si \mathcal{C} y \mathcal{D} son isomorfas, existen funtores $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ tales que $F \circ G = \text{Id}_{\mathcal{D}}$ y $G \circ F = \text{Id}_{\mathcal{C}}$. Luego F , G y los isomorfismos naturales identidad de $F \circ G$ y $G \circ F$ determinan una equivalencia entre \mathcal{C} y \mathcal{D} . \square

Estableceremos ahora algunas propiedades sobre los funtores, que nos permitirán caracterizar cuándo un functor $F : \mathcal{C} \rightarrow \mathcal{D}$ define una equivalencia entre categorías.

Recordemos que un functor $F : \mathcal{C} \rightarrow \mathcal{D}$ es *fiel* (ver Definición 6.4.4) si para cada $f, g \in \text{mor } \mathcal{C}$, se tiene que

$$F(f) = F(g) \implies f = g.$$

Definición 7.2.4. *Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un functor. Decimos que:*

1. *F es **full** si para cada par de objetos A, B de \mathcal{C} , la función $\text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{D}}(F(A), F(B))$ es sobreyectiva.*
2. *F es **esencialmente sobreyectiva en objetos** si para cada objeto $D \in \mathcal{D}$, existe un objeto A en \mathcal{C} tal que D es isomorfo a $F(A)$.*

Lema 7.2.5. *Si $F : \mathcal{C} \rightarrow \mathcal{D}$ define una equivalencia de \mathcal{C} en \mathcal{D} , entonces F es fiel, full y esencialmente sobreyectivo en objetos.*

Demostración. Supongamos que $F : \mathcal{C} \rightarrow \mathcal{D}$ define una equivalencia y sean $G : \mathcal{D} \rightarrow \mathcal{C}$, η y τ los elementos que completan la definición.

Veamos primero que F es fiel. Sean $f, g \in \text{Hom}_{\mathcal{C}}(A, B)$ y supongamos que $F(f) = F(g)$. Luego $G(F(f)) = G(F(g))$ y los diagramas siguientes conmutan:

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ f \downarrow & & \downarrow G(F(f)) \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ g \downarrow & & \downarrow G(F(g)) \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array}$$

Pero como η_A y η_B son isomorfismos tenemos que

$$f = \eta_B^{-1} \circ G(F(f)) \circ \eta_A = \eta_B^{-1} \circ G(F(g)) \circ \eta_A = g.$$

Como los roles de F y G en la definición son simétricos, con la misma prueba resulta que G también es fiel.

Veamos ahora que F es full. Sea $g \in \text{Hom}_{\mathcal{D}}(F(A), F(B))$ y sea $k = G(g) \in \text{Hom}_{\mathcal{C}}(G(F(A)), G(F(B)))$. Pongamos $h = \eta_B^{-1} \circ k \circ \eta_A$, entonces nuevamente los siguientes diagramas conmutan:

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ h \downarrow & & \downarrow k \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ h \downarrow & & \downarrow G(F(h)) \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array}$$

Luego con el mismo argumento que antes, tenemos que $k = G(F(h))$ o sea $G(g) = G(F(h))$ y como G es fiel, $g = F(h)$.

Veamos finalmente que F es esencialmente sobreyectiva en objetos. Sea $D \in \mathcal{D}$ y sea $A = G(D) \in \mathcal{C}$. Entonces $\tau_D : D \rightarrow F(G(D)) = F(A)$ es un isomorfismo, con lo cual existe $A \in \mathcal{C}$ tal que D es isomorfo a $F(A)$. \square

Dos categorías equivalente pueden parecer muy distintas. La filosofía detrás de la noción de equivalencia es que en una categoría no interesan tanto los objetos en sí, sino los objetos *salvo isomorfismos*, que pueden considerarse como un único objeto. Es decir, detrás del concepto de equivalencia está escondida una noción de “pasar al cociente” objetos isomorfos. Observemos lo que ocurre en el siguiente ejemplo:

Ejemplo 7.2.6. La categoría $\mathbf{1}$ cuyo único objeto es $*$ y cuyo único morfismo es id_* es equivalente a la categoría \mathcal{D} con dos objetos A y B y cuatro morfismos: $\text{id}_A, \text{id}_B, f : A \rightarrow B$ y $g : B \rightarrow A$ tal que $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$. Observemos que en \mathcal{D} los objetos A y B son isomorfos, dado que f y g son isomorfismos, inverso uno del otro. Por lo tanto los objetos de \mathcal{D} no “modelan” más situaciones que el único objeto de $\mathbf{1}$, y tiene sentido que estas categorías sean equivalentes, aunque claramente no son isomorfas.

Podemos ver esto explícitamente definiendo $F : \mathbf{1} \rightarrow \mathcal{D}$, $F(*) = A$, $F(\text{id}_*) = \text{id}_A$ y $G : \mathcal{D} \rightarrow \mathbf{1}$, $G(A) = G(B) = *$, $G(\text{id}_A) = G(\text{id}_B) = G(f) = G(g) = \text{id}_*$. Es inmediato verificar que F es un funtor y, como $g \circ f = \text{id}_A$ y $f \circ g = \text{id}_B$, G también lo es.

Definamos ahora $\eta : \text{Id}_{\mathbf{1}} \rightarrow G \circ F$ como $\eta_* = \text{id}_*$, y $\tau : \text{Id}_{\mathcal{D}} \rightarrow F \circ G$ tal que $\tau_A = \text{id}_A$, $\tau_B = g$. Es inmediato que η es un isomorfismo natural. Para ver que τ también lo es, observemos que los siguientes diagramas conmutan:

$$\begin{array}{ccc} A & \xrightarrow{\tau_A = \text{id}_A} & A = F(G(A)) \\ \text{id}_A \downarrow & & \downarrow \text{id}_A = F(G(\text{id}_A)) \\ A & \xrightarrow{\tau_A = \text{id}_A} & A = F(G(A)) \\ \\ B & \xrightarrow{\tau_B = g} & A = F(G(B)) \\ \text{id}_B \downarrow & & \downarrow \text{id}_A = F(G(\text{id}_B)) \\ B & \xrightarrow{\tau_B = g} & A = F(G(B)) \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\tau_A = \text{id}_A} & A = F(G(A)) \\ f \downarrow & & \downarrow \text{id}_A = F(G(f)) \\ B & \xrightarrow{\tau_B = g} & A = F(G(B)) \\ \\ B & \xrightarrow{\tau_B = g} & A = F(G(B)) \\ g \downarrow & & \downarrow \text{id}_A = F(G(g)) \\ A & \xrightarrow{\tau_A = \text{id}_A} & A = F(G(A)) \end{array}$$

Por lo tanto $\mathbf{1}$ y \mathcal{D} son categorías equivalentes. \blacksquare

El ejemplo anterior puede generalizarse de la siguiente manera a una categoría arbitraria:

Definición 7.2.7. Sea \mathcal{C} una categoría. Un esqueleto de \mathcal{C} es una subcategoría full \mathcal{E} de \mathcal{C} (es decir, $\text{Hom}_{\mathcal{E}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$ para cada $A, B \in \text{ob } \mathcal{E}$) tal que cada objeto de \mathcal{C} es isomorfo a un único objeto de \mathcal{E} .

Observación 7.2.8. Una formulación equivalente a la noción de esqueleto es la siguiente: Una subcategoría \mathcal{E} de \mathcal{C} es un esqueleto, si \mathcal{E} es full, todo objeto de \mathcal{C} es isomorfo a un objeto de \mathcal{E} y dos objetos distintos cualesquiera de \mathcal{E} no son isomorfos entre sí.

Lema 7.2.9. Sea \mathcal{C} una categoría y \mathcal{E} un esqueleto de \mathcal{C} . Para cada $A \in \text{ob } \mathcal{C}$, sea $E(A) \in \text{ob } \mathcal{E}$ un objeto isomorfo a A y $\theta_A : A \rightarrow E(A)$ un isomorfismo. Si $f : A \rightarrow B \in \text{mor } \mathcal{C}$, pongamos $E(f) : E(A) \rightarrow E(B)$ tal que $E(f) = \theta_B \circ f \circ \theta_A^{-1}$, es decir, el siguiente diagrama conmuta:

$$(7.4) \quad \begin{array}{ccc} A & \xrightarrow{\theta_A} & E(A) \\ f \downarrow & & \downarrow E(f) \\ B & \xrightarrow{\theta_B} & E(B) \end{array}$$

Entonces $E : \mathcal{C} \rightarrow \mathcal{E}$ es un funtor y $\theta : \text{Id} \rightarrow E$ es un isomorfismo natural.

Demostración. Observemos primero que como \mathcal{E} es una categoría full, $E(f) \in \text{Hom}_{\mathcal{E}}(E(A), E(B))$ y por lo tanto E está bien definido. Ahora, dados dos morfismos $f : A \rightarrow B$ y $g : B \rightarrow C$, en el siguiente diagrama los dos cuadrados interiores son conmutativos:

$$\begin{array}{ccc} A & \xrightarrow{\theta_A} & E(A) \\ f \downarrow & & \downarrow E(f) \\ B & \xrightarrow{\theta_B} & E(B) \\ g \downarrow & & \downarrow E(g) \\ C & \xrightarrow{\theta_C} & E(C) \end{array}$$

Luego por el Lema 6.1, el cuadrado exterior también es conmutativo, es decir

$$(E(g) \circ E(f)) \circ \theta_A = \theta_C \circ (g \circ f) \Rightarrow E(g) \circ E(f) = \theta_C \circ (g \circ f) \circ \theta_A^{-1} = E(g \circ f).$$

Finalmente, $E(\text{id}_A) = \theta_A \circ \text{id}_A \circ \theta_A^{-1} = \text{id}_A$, con lo cual E es un funtor.

La última afirmación es inmediata de la conmutatividad de (7.4). □

Teorema 7.2.10. Sea \mathcal{E} un esqueleto de una categoría \mathcal{C} . Entonces \mathcal{C} y \mathcal{E} son categorías equivalentes.

Demostración. Dado que \mathcal{E} es una subcategoría de \mathcal{C} , podemos considerar el funtor $\text{inc} : \mathcal{E} \rightarrow \mathcal{C}$. Por otro lado, tenemos el funtor $E : \mathcal{C} \rightarrow \mathcal{E}$ dado en el Lema 7.2.

Ahora bien, $E \circ \text{inc} : \mathcal{E} \rightarrow \mathcal{E}$ es el funtor identidad $\text{Id}_{\mathcal{E}}$, y por lo tanto tenemos el isomorfismo natural identidad entre estos funtores. Por otra parte, por el Lema 7.2 $\theta : \text{ob } \mathcal{C} \rightarrow \text{mor } \mathcal{C}$ es un isomorfismo natural entre $\text{Id}_{\mathcal{C}}$ y $E = \text{inc} \circ E$.

Concluimos que $\text{inc} : \mathcal{E} \rightarrow \mathcal{C}$, $E : \mathcal{C} \rightarrow \mathcal{E}$, id_{Id} y θ definen una equivalencia de categorías. □

Teorema 7.2.11. Sean \mathcal{C} y \mathcal{D} dos categorías y sean $\mathcal{E}_{\mathcal{C}}$ y $\mathcal{E}_{\mathcal{D}}$ esqueletos de las categorías \mathcal{C} y \mathcal{D} . Entonces: \mathcal{C} y \mathcal{D} son categorías equivalentes si y sólo si $\mathcal{E}_{\mathcal{C}}$ y $\mathcal{E}_{\mathcal{D}}$ son categorías isomorfas.

Demostración. Supongamos primero que $\mathcal{E}_{\mathcal{C}}$ y $\mathcal{E}_{\mathcal{D}}$ son categorías isomorfas. Entonces tenemos la siguiente cadena de equivalencias: \mathcal{C} es equivalente a $\mathcal{E}_{\mathcal{C}}$ por el Teorema 7.2.10; $\mathcal{E}_{\mathcal{C}}$ es equivalente a $\mathcal{E}_{\mathcal{D}}$ por el Teorema 7.2.3; $\mathcal{E}_{\mathcal{D}}$ es equivalente a \mathcal{D} por el Teorema 7.2.10. Luego por el Teorema 7.2.2 resulta que \mathcal{C} y \mathcal{D} son equivalentes.

Supongamos ahora que \mathcal{C} y \mathcal{D} son equivalentes. Entonces como $\mathcal{E}_{\mathcal{C}}$ es equivalente a \mathcal{C} y $\mathcal{E}_{\mathcal{D}}$ es equivalente a \mathcal{D} , por el Lema 7.2.2 resulta que $\mathcal{E}_{\mathcal{C}}$ es equivalente a $\mathcal{E}_{\mathcal{D}}$. Sean $F : \mathcal{E}_{\mathcal{C}} \rightarrow \mathcal{E}_{\mathcal{D}}$, $G : \mathcal{E}_{\mathcal{D}} \rightarrow \mathcal{E}_{\mathcal{C}}$ y $\eta : \text{Id}_{\mathcal{E}_{\mathcal{C}}} \rightarrow G \circ F$ y $\tau : \text{Id}_{\mathcal{E}_{\mathcal{D}}} \rightarrow F \circ G$ isomorfismos naturales. Entonces para cada $A \in \mathcal{E}_{\mathcal{C}}$, $\eta_A : A \rightarrow G \circ F(A)$ es un isomorfismo. Pero en $\mathcal{E}_{\mathcal{C}}$ no hay ningún par de objetos distintos isomorfos, y por lo tanto $G \circ F(A) = A$. Luego el siguiente diagrama en $\mathcal{E}_{\mathcal{C}}$ conmuta:

$$(7.5) \quad \begin{array}{ccc} A & \xrightarrow{\eta_A} & A \\ f \downarrow & & \downarrow G \circ F(f) \\ B & \xrightarrow{\eta_B} & B \end{array}$$

En particular, si $A', B' \in \text{ob } \mathcal{E}_{\mathcal{D}}$, y $f' \in \text{Hom}_{\mathcal{E}_{\mathcal{D}}}(A', B')$, entonces el siguiente diagrama conmuta:

$$(7.6) \quad \begin{array}{ccc} G(A') & \xrightarrow{\eta_{G(A')}} & G(A') \\ G(f') \downarrow & & \downarrow G \circ F(G(f')) \\ G(B') & \xrightarrow{\eta_{G(B')}} & G(B') \end{array}$$

Pongamos $G' : \mathcal{E}_{\mathcal{D}} \rightarrow \mathcal{E}_{\mathcal{C}}$ definiendo

- $G'(A') = G(A')$ si $A' \in \text{ob } \mathcal{E}_{\mathcal{D}}$;
- $G'(f') = \eta_{G(B')} \circ G(f') \circ \eta_{G(A')}^{-1}$ si $f' \in \text{Hom}_{\mathcal{E}_{\mathcal{D}}}(A', B')$.

Entonces, con el mismo argumento que en el Lema 7.2.9, resulta que $G' : \mathcal{E}_{\mathcal{D}} \rightarrow \mathcal{E}_{\mathcal{C}}$ es un funtor.

Ahora, si $A \in \text{ob } \mathcal{E}_{\mathcal{C}}$, entonces $G'(F(A)) = G(F(A)) = A$ y si $f \in \text{Hom}_{\mathcal{E}_{\mathcal{C}}}(A, B)$, entonces como (7.5) conmuta,

$$G'(F(f)) = \eta_{G(F(B))} \circ G(F(f)) \circ \eta_{G(F(A))}^{-1} = \eta_B \circ (G \circ F(f)) \circ \eta_A^{-1} = f$$

Por lo tanto $G' \circ F = \text{Id}_{\mathcal{E}_{\mathcal{C}}}$.

Si ahora $A' \in \text{ob } \mathcal{E}_{\mathcal{D}}$, $F(G'(A')) = F(G(A'))$, y como en $\mathcal{E}_{\mathcal{D}}$ todo par de objetos distintos no son isomorfos y $\tau_{A'} : A' \rightarrow F(G(A'))$ es un isomorfismo, debe ser $F(G'(A')) = A'$.

Sea $f' \in \text{Hom}_{\mathcal{E}_{\mathcal{D}}}(A', B')$ y sean $A = G(A')$, $B = G(B')$. Entonces $F(A) = A'$, $F(B) = B'$. Como F es full, del Lema 7.2.5 debe existir $f \in \text{Hom}_{\mathcal{E}_{\mathcal{C}}}(A, B)$ tal que $F(f) = f'$. Luego, como $G' \circ F = \text{Id}_{\mathcal{E}_{\mathcal{C}}}$, resulta que

$$F(G'(f')) = F(G'(F(f))) = F(f) = f'$$

y por lo tanto $F \circ G' = \text{Id}_{\mathcal{E}_{\mathcal{D}}}$. □

Observación 7.2.12. Sobre el axioma de elección. El Lema 7.2.5 nos da una condición necesaria para que un funtor defina una equivalencia, y la comparación de esqueletos entre dos categorías nos permite identificar si estas categorías son equivalentes. Sin embargo no hemos probado ni la recíproca del Lema 7.2.5 ni que toda categoría admite un esqueleto. Para ambos resultados necesitamos una versión fuerte del axioma de elección. Sin entrar en detalles un axioma de elección suficientemente fuerte (existen diferentes versiones) permite elegir un objeto de cada subclase de una familia no vacía de subclases de una clase \mathcal{C} cualquiera, indexada por los objetos de una clase \mathcal{D} , y definir una función selectora entre clases que a cada objeto $D \in \mathcal{D}$ le asigne un elemento de \mathcal{C} que esté en la subclase indexada por D . Para más detalles puede consultarse la sección 2 de [1] o el Capítulo 36 en [18].

Teorema 7.2.13. Sea \mathcal{C} una categoría. Entonces \mathcal{C} tiene un esqueleto \mathcal{E} .

Demostración. Podemos “dividir” la clase $\text{ob } \mathcal{C}$ en clases disjuntas de objetos isomorfos. Si elegimos un objeto en cada clase, obtendremos una clase $\mathcal{E} \subseteq \text{ob } \mathcal{C}$ tal que dos objetos distintos de \mathcal{E} no son isomorfos. Si ahora definimos \mathcal{E} tal que $\text{ob } \mathcal{E} = \mathcal{E}$ y $\text{Hom}_{\mathcal{E}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$ para cada $A, B \in \mathcal{C}$, obtenemos una subcategoría full de \mathcal{C} que claramente es un esqueleto de \mathcal{C} . \square

Teorema 7.2.14. Sean \mathcal{C} y \mathcal{D} categorías y sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor. F define una equivalencia de \mathcal{C} en \mathcal{D} si y sólo si F es fiel, full y esencialmente sobreyectivo en objetos.

Demostración. Ya hemos probado una parte del Teorema en el Lema 7.2.5. Supongamos entonces que F es un funtor fiel, full y esencialmente sobreyectivo en objetos,

Sea $D \in \text{ob } \mathcal{D}$ y pongamos en \mathcal{D}_D la subclase formada por los objetos de \mathcal{D} isomorfos a D . Como F es esencialmente sobreyectivo en objetos, existe un objeto $A_D \in \mathcal{C}$ tal que D es isomorfo a $F(A_D)$, o sea, $F(A_D) \in \mathcal{D}_D$. Por el Axioma de elección podemos elegir para cada $D \in \text{ob } \mathcal{D}$ un objeto A_D de $\mathcal{D}_D \cap F(\text{ob } \mathcal{C})$ y un isomorfismo

$$(7.7) \quad \tau_D : D \rightarrow F(A_D)$$

Definamos $G : \text{ob } \mathcal{D} \rightarrow \text{ob } \mathcal{C}$ tal que $G(D) = A_D$. Si $f' \in \text{Hom}_{\mathcal{D}}(D, D')$, sea $f'' = \tau_{D'} \circ f' \circ \tau_D^{-1}(f')$, es decir, el siguiente diagrama en τ es conmutativo:

$$(7.8) \quad \begin{array}{ccc} D & \xrightarrow{\tau_D} & F(A_D) \\ \downarrow f' & & \downarrow f'' \\ D' & \xrightarrow{\tau_{D'}} & F(A_{D'}) \end{array}$$

Como F es full y fiel, existe un único morfismo $f \in \text{Hom}_{\mathcal{C}}(A_D, A_{D'})$ tal que $F(f) = f''$. Pongamos entonces $G(f') = f$. Dejamos como **ejercicio** probar que G así definido es un funtor de \mathcal{D} en \mathcal{C} .

Reemplazando en (7.9), tenemos que el siguiente diagrama es conmutativo:

$$(7.9) \quad \begin{array}{ccc} D & \xrightarrow{\tau_D} & F(G(D)) \\ \downarrow f' & & \downarrow F(G(f')) \\ D' & \xrightarrow{\tau_{D'}} & F(G(D')) \end{array}$$

y por lo tanto $\text{Id}_{\mathcal{D}} \xrightarrow{\tau} F \circ G$.

Solo nos queda probar que existe un isomorfismo natural $\eta : \text{Id}_{\mathcal{C}} \rightarrow G \circ F$. Sea $A \in \text{ob } \mathcal{C}$. Pongamos $D = F(A)$. Como $A_D = G(D) = G(F(A))$, reemplazando en (7.7) tenemos un isomorfismo

$$\tau_{F(A)} : F(A) \rightarrow F(G(F(A))).$$

Como F es full, existe un morfismo $\eta_A : A \rightarrow G(F(A))$ tal que $F(\eta_A) = \tau_{F(A)}$. Como F es fiel y full, por el Ejercicio 5 de este capítulo, η_A es un isomorfismo. Finalmente si $f : A \rightarrow B$ es un morfismo cualquiera, pongamos $g = \eta_B \circ f \circ \eta_A^{-1} : G(F(A)) \rightarrow G(F(B))$. Entonces el siguiente diagrama en \mathcal{C} es conmutativo:

$$(7.10) \quad \begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ f \downarrow & & \downarrow g \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array}$$

Aplicando F , obtenemos que el siguiente diagrama en \mathcal{D} es conmutativo:

$$\begin{array}{ccc} F(A) & \xrightarrow{\tau_{F(A)}} & F(G(F(A))) \\ F(f) \downarrow & & \downarrow F(g) \\ F(B) & \xrightarrow{\tau_{F(B)}} & F(G(F(B))) \end{array}$$

Poniendo $D = F(A)$, $D' = F(B)$, $f' = F(f)$ en (7.9), tenemos que el siguiente diagrama también es conmutativo en \mathcal{D} :

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

Como $\tau_{F(A)}$ y $\tau_{F(B)}$ son isomorfismos, tenemos que

$$F(g) = \tau_{F(B)} \circ F(f) \circ \tau_{F(A)}^{-1} = F(G(F(f)))$$

Pero como F es fiel, debe ser $g = G(F(f))$. Reemplazando en (7.10) resulta que $\text{Id}_{\mathcal{C}} \xrightarrow{\eta} G \circ F$. \square

Veremos a continuación que dos categorías equivalentes tienen esencialmente los mismos objetos iniciales, terminales, productos, coproductos, ecualizadores, coecualizadores, límites, colímites y exponenciales.

Notación 7.2.15. Dada una categoría \mathcal{C} , diremos que un objeto junto con, eventualmente, uno o más morfismos es una **estructura categórica** de \mathcal{C} si es un elemento inicial, terminal, un producto, un coproducto, un ecualizador, un coecualizador, un límite, un colímite o un exponencial. Esta denominación no es universalmente utilizada, pero nos servirá para simplificar los enunciados de las propiedades siguientes.

Lema 7.2.16. Si $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{C} \rightarrow \mathcal{D}$ definen una equivalencia entre \mathcal{C} y \mathcal{D} con $\text{Id}_{\mathcal{C}} \xrightarrow{\eta} G \circ F$ y $\text{Id}_{\mathcal{D}} \xrightarrow{\tau} F \circ G$, entonces F y G definen una equivalencia entre \mathcal{C}^{op} y \mathcal{D}^{op} con $\text{Id}_{\mathcal{C}^{op}} \xrightarrow{\eta^{-1}} G \circ F$ y $\text{Id}_{\mathcal{D}^{op}} \xrightarrow{\tau^{-1}} F \circ G$.

Demostración. Supongamos que $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ definen una equivalencia de \mathcal{C} a \mathcal{D} con isomorfismos naturales $\eta : \text{Id}_{\mathcal{C}} \rightarrow G \circ F$ y $\tau : \text{Id}_{\mathcal{D}} \rightarrow F \circ G$.

Sean $A, B \in \text{ob } \mathcal{C}^{op} = \text{ob } \mathcal{C}$ y $f \in \text{Hom}_{\mathcal{C}^{op}}(A, B)$. Entonces $f \in \text{Hom}_{\mathcal{C}}(B, A)$ y por lo tanto $F(f) \in \text{Hom}_{\mathcal{D}}(F(B), F(A)) = \text{Hom}_{\mathcal{D}^{op}}(F(A), F(B))$.

Además, si $f \in \text{Hom}_{\mathcal{C}^{op}}(A, B)$ y $g \in \text{Hom}_{\mathcal{C}^{op}}(B, C)$, entonces

$$F(g \circ^{op} f) = F(f \circ g) = F(f) \circ F(g) = F(g) \circ^{op} F(f)$$

Como $F(\text{id}_A) = \text{id}_{F(A)}$, resulta que $F : \mathcal{C}^{op} \rightarrow \mathcal{D}^{op}$ (y análogamente $G : \mathcal{D}^{op} \rightarrow \mathcal{C}^{op}$) es un funtor.

Sean nuevamente $A, B \in \text{ob } \mathcal{C}^{op}$ y $f \in \text{Hom}_{\mathcal{C}^{op}}(A, B)$. Entonces en \mathcal{C} tenemos que el siguiente diagrama conmuta:

$$\begin{array}{ccc} B & \xrightarrow{\eta_B} & G(F(B)) \\ f \downarrow & & \downarrow G(F(f)) \\ A & \xrightarrow{\eta_A} & G(F(A)) \end{array}$$

y por lo tanto el siguiente diagrama conmuta en \mathcal{C}^{op} :

$$\begin{array}{ccc} A & \xleftarrow{\eta_A} & G(F(A)) \\ f \downarrow & & \downarrow G(F(f)) \\ B & \xleftarrow{\eta_B} & G(F(B)) \end{array}$$

Es decir,

$$G(F(f)) = \eta_B^{-1} \circ^{op} f \circ^{op} \eta_A = (\eta_B^{-1}) \circ^{op} f \circ^{op} (\eta_A^{-1})^{-1}$$

y por lo tanto el siguiente diagrama en \mathcal{C}^{op} también conmuta:

$$\begin{array}{ccc} A & \xrightarrow{\eta_A^{-1}} & G(F(A)) \\ f \downarrow & & \downarrow G(F(f)) \\ B & \xrightarrow{\eta_B^{-1}} & G(F(B)) \end{array}$$

Concluimos que η^{-1} es un isomorfismo natural tal que $\text{Id}_{\mathcal{C}^{op}} \xrightarrow{\eta^{-1}} G \circ F$. De manera análoga se prueba que $\text{Id}_{\mathcal{D}^{op}} \xrightarrow{\tau^{-1}} F \circ G$. \square

Teorema 7.2.17. Si $F : \mathcal{C} \rightarrow \mathcal{D}$ define una equivalencia de categorías, entonces F mapea estructuras categóricas en \mathcal{C} en las respectivas estructuras categóricas en \mathcal{D} .

Demostración. Haremos la prueba sólo para objetos iniciales y límites. Con éste último habremos probado que F mapea productos en productos y ecualizadores en ecualizadores (ver Ejemplos 6.8.2 y 6.8.3). Por otra parte, del Lema 7.2.16 $F : \mathcal{C}^{op} \rightarrow \mathcal{D}^{op}$ también define una equivalencia, con lo cual habremos probado el teorema para objetos terminales y colímites, y en consecuencia para coproductos y coecualizadores. La prueba para los exponenciales es similar y la dejamos como **ejercicio**.

Supongamos que \mathcal{C} y \mathcal{D} son equivalentes, con funtores $F : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{D} \rightarrow \mathcal{C}$ e isomorfismos naturales $\eta : \text{id}_{\mathcal{C}} \rightarrow G \circ F$ y $\tau : \text{Id}_{\mathcal{D}} \rightarrow F \circ G$.

Supongamos que \mathcal{C} tiene un objeto inicial 0 y sea $0' = F(0)$. Veamos que $0'$ es un objeto inicial de \mathcal{D} . Sea A' un objeto de \mathcal{D} y $A = G(A')$. Entonces existe un único morfismo $f_A : 0 \rightarrow A$, que se mapea por F en un morfismo $F(f_A) : 0' \rightarrow F(A)$. Ahora bien, $F(A) = F(G(A'))$ no necesariamente es A' , pero existe un isomorfismo $\tau_{A'} : A' \rightarrow F(G(A')) = F(A)$. Por lo tanto poniendo $g_{A'} = \tau_{A'}^{-1} \circ F(f_A)$, tenemos un morfismo de $0'$ en A' .

$$\begin{array}{ccc} 0' & & \\ \downarrow g_{A'} & \searrow F(f_A) & \\ A' & \xleftarrow{\tau_{A'}^{-1}} & F(A) \end{array}$$

Supongamos ahora que existe otro morfismo $h : 0' \rightarrow A'$. Entonces $\tau_{A'} \circ h : 0' \rightarrow F(A)$ es un morfismo de $0'$ en $F(A)$.

$$\begin{array}{ccc} 0' & & \\ \downarrow h & \searrow \tau_{A'} \circ h & \\ A' & \xrightarrow{\tau_{A'}} & F(A) \end{array}$$

Por el Lema 7.2.5, existe $f : 0 \rightarrow A$ tal que $F(f) = \tau_{A'} \circ h$. Pero el único morfismo de 0 en A es f_A , con lo cual $\tau_{A'} \circ h = F(f_A)$ y por lo tanto $h = \tau_{A'}^{-1} \circ F(f_A) = g_{A'}$. Luego $0'$ es un objeto inicial de \mathcal{D} .

Sea ahora \mathcal{D} un diagrama en \mathcal{C} y sea $(X, \mathcal{F}_{\mathcal{D}})$ un cono para \mathcal{D} . Si $\mathcal{F}_{\mathcal{D}} = \{f_A : X \rightarrow A : A \in \text{ob } \mathcal{D}\}$, pongamos $F(\mathcal{F}_{\mathcal{D}}) = \{F(f_A) : F(X) \rightarrow F(A) : A \in \text{ob } \mathcal{D}\}$. Observemos que $(F(X), F(\mathcal{F}_{\mathcal{D}}))$ es un cono para $F(\mathcal{D})$. En efecto, para cada par de objetos $A, B \in \mathcal{D}$ y cada morfismo $f : A \rightarrow B \in \text{mor } \mathcal{D}$, el diagrama de la izquierda en \mathcal{C} es conmutativo. Como $F : \mathcal{C} \rightarrow \mathcal{D}$ es un funtor, el diagrama de la derecha en \mathcal{D} también conmuta:

$$\begin{array}{ccc} & X & \\ f_A \swarrow & & \searrow f_B \\ A & \xrightarrow{f} & B \end{array} \qquad \begin{array}{ccc} & F(X) & \\ F(f_A) \swarrow & & \searrow F(f_B) \\ F(A) & \xrightarrow{F(f)} & F(B) \end{array}$$

Consideremos las categorías $\text{Cone}(\mathcal{D})$ y $\text{Cone}(F(\mathcal{D}))$ (ver Ejemplo 6.8.6). Recordemos que un morfismo de conos $k : (X', \mathcal{F}'_{\mathcal{D}}) \rightarrow (X, \mathcal{F}_{\mathcal{D}})$ está dado por un morfismo $k : X' \rightarrow X$ tal que

$$\begin{array}{ccc} X' & \xrightarrow{k} & X \\ & \searrow f'_D & \swarrow f_D \\ & D & \end{array}$$

conmuta para cada $D \in \text{ob } \mathcal{D}$. Como F es un funtor, es inmediato que $F(k) : F(X') \rightarrow F(X)$ define un morfismo de conos de $(F(X'), F(\mathcal{F}'_{\mathcal{D}}))$ en $(F(X), F(\mathcal{F}_{\mathcal{D}}))$. Dejamos como **ejercicio** verificar que entonces F define un funtor $F : \text{Cone}(\mathcal{D}) \rightarrow \text{Cone}(F(\mathcal{D}))$. No es difícil ver que como $F : \mathcal{C} \rightarrow \mathcal{D}$ define una equivalencia, $F : \text{Cone}(\mathcal{D}) \rightarrow \text{Cone}(F(\mathcal{D}))$ es fiel, full y esencialmente sobreyectivo en objetos. Por lo tanto

define una equivalencia. Si ahora $(X, \mathcal{F}_{\mathcal{D}})$ es un límite para \mathcal{D} , entonces es un objeto terminal en $\text{Cone}(\mathcal{D})$. Por lo tanto $(F(X), F(\mathcal{F}_{\mathcal{D}}))$ es un objeto terminal en $\text{Cone}(F(\mathcal{D}))$ y entonces es un límite para $F(\mathcal{D})$. \square

7.3. Adjunciones.

Las equivalencias entre categorías son el concepto más adecuado para identificar dos categorías “casi iguales”, en el sentido de que si bien no son isomorfas, comparten las mismas propiedades categóricas y comparten esqueletos isomorfos.

Esta noción es sin embargo demasiado restrictiva, dado que no es tan común encontrar categorías equivalentes. Existe una noción aún más débil que la de equivalencia, pero que resulta muy útil en muchas aplicaciones. Se trata de las *adjunciones*. Trataremos este tema en modo resumido, presentando las principales propiedades. Para más detalles recomendamos consultar [14], [17] o [18].

Definición 7.3.1. Sean \mathcal{C} y \mathcal{D} dos categorías. Una **adjunción** de \mathcal{C} en \mathcal{D} consiste de dos funtores $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$

$$\mathcal{C} \begin{array}{c} \xrightarrow{F} \\ \xleftarrow{G} \end{array} \mathcal{D}$$

y de una transformación natural $\eta : \text{Id}_{\mathcal{C}} \rightarrow (G \circ F)$

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & G(F(A)) \\ h \downarrow & & \downarrow G \circ F(h) \\ B & \xrightarrow{\eta_B} & G(F(B)) \end{array}$$

tal que vale la siguiente propiedad universal: Para cada $X \in \text{ob } \mathcal{C}$, cada $Y \in \text{ob } \mathcal{D}$ y cada $f \in \text{Hom}_{\mathcal{C}}(X, G(Y))$, existe un único morfismo $f^\# : F(X) \rightarrow Y$ tal que el siguiente diagrama conmuta:

$$(7.11) \quad \begin{array}{ccc} X & \xrightarrow{\eta_X} & G(F(X)) \\ & \searrow f & \downarrow G(f^\#) \\ & & G(Y) \end{array}$$

En este caso, decimos que F **define una adjunción** de \mathcal{C} a \mathcal{D} , que F es un **adjunto a izquierda** de G y G es un **adjunto a derecha** de F . La transformación natural η se denomina **unidad** de la adjunción.

Lema 7.3.2. Toda equivalencia de categorías define una adjunción. Es decir, si $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ definen una equivalencia con $\text{Id}_{\mathcal{C}} \xrightarrow{\eta} G \circ F$, entonces F es un adjunto a derecha de G y η es una unidad adjunción.

Demostración. Si \mathcal{C} y \mathcal{D} son equivalentes con funtores $F : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{D} \rightarrow \mathcal{C}$ e isomorfismos naturales η y τ , entonces en particular η es una transformación natural de $\text{Id}_{\mathcal{C}}$ en $G \circ F$. Para ver que es una adjunción, consideremos un objeto X de \mathcal{C} , un objeto Y de \mathcal{D} y un morfismo $f \in \text{Hom}_{\mathcal{C}}(X, G(Y))$. Pongamos

$k : G(F(X)) \rightarrow G(Y)$, $k = f \circ \eta_X^{-1}$. Entonces k hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & G(F(X)) \\ & \searrow f & \downarrow k \\ & & G(Y) \end{array}$$

Por el Lema 7.2.5 G es fiel y full y existirá un único morfismo $f^\# : F(X) \rightarrow Y$ tal que $G(f^\#) = k$.

Observemos ahora que si $h : F(X) \rightarrow Y$ es un morfismo que hace conmutar el diagrama

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & G(F(X)) \\ & \searrow f & \downarrow G(h) \\ & & G(Y) \end{array}$$

resulta $G(h) = f \circ \eta_X^{-1} = k$, con lo cual $h = f^\#$. □

Ejemplo 7.3.3. Conexiones de Galois. Como hemos verificado hasta el momento, cada propiedad de un poset P puede pensarse a través de alguna propiedad de la categoría \mathcal{C}_P . Consideremos ahora dos posets P y Q y un par de morfismos de orden $F : P \rightarrow Q$ y $G : Q \rightarrow P$. Decimos que el par (F, G) es una *conexión de Galois (monótona)* si para cada $x \in P$, $y \in Q$,

$$(7.12) \quad F(x) \preceq_Q y \iff x \preceq_P G(y).$$

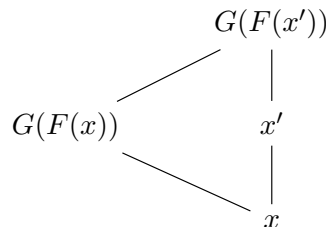
Sean ahora \mathcal{C}_P , \mathcal{C}_Q las categorías asociadas a P y Q . Recordemos que si $x, x' \in P = \text{ob } \mathcal{C}_P$, existe un morfismo de x en x' si y sólo si $x \preceq_P x'$ y por lo tanto todo morfismo de orden $F : P \rightarrow Q$ induce un funtor $F : \mathcal{C}_P \rightarrow \mathcal{C}_Q$, poniendo $F(x, x') = (F(x), F(x'))$ cada vez que $(x, x') \in \text{Hom}_{\mathcal{C}_P}(x, x')$ (ver Ejemplo 6.3.6).

Probaremos que (F, G) es una conexión de Galois si y sólo si existe una adjunción η de F en G .

Comencemos analizando cuándo existe una unidad de adjunción $\eta : \text{Id}_{\mathcal{C}_P} \rightarrow G \circ F$. Como una unidad de adjunción debe ser una transformación natural, el diagrama

$$\begin{array}{ccc} x & \xrightarrow{\eta_x} & G(F(x)) \\ (x, x') \downarrow & & \downarrow G \circ F(x, x') \\ x' & \xrightarrow{\eta_{x'}} & G(F(x')) \end{array}$$

debe ser conmutativo para cualquier par de objetos x, x' tales que $x \preceq_P x'$. A su vez, esto ocurre si y sólo si el diagrama de Hasse de (P, \preceq_P) tiene como subdiagrama a:



Ahora bien, como $G \circ F : P \rightarrow P$ es un morfismo de orden, tendremos automáticamente que si $x \preceq_P x'$, entonces $G(F(x)) \preceq_P G(F(x'))$. Por lo tanto, existirá una transformación natural $\eta : \text{Id}_{\mathcal{C}_P} \rightarrow G \circ F$ si y sólo si

$$(7.13) \quad \forall x \in P, \quad x \preceq_P G(F(x)).$$

Por otra parte, la transformación natural η será una unidad de adjunción si y sólo si para cada $x \in P = \text{ob } \mathcal{C}_P$ y cada $y \in Q = \text{ob } \mathcal{C}_Q$, si existe un morfismo $f : x \rightarrow G(y)$ (o sea, si $x \preceq_P G(y)$), existe un morfismo $f^\# : F(x) \rightarrow y$ (o sea, $F(x) \preceq_Q y$) tal que conmuta

$$\begin{array}{ccc} x & \xrightarrow{\eta_x} & G(F(x)) \\ & \searrow f & \downarrow G(f^\#) \\ & & G(y) \end{array}$$

Esto es, η será una unidad de adjunción si y sólo si η es una transformación natural tal que

$$(7.14) \quad x \preceq_P G(y) \implies F(x) \preceq_Q y \wedge x \preceq_P G(F(x)) \preceq_P G(y)$$

Es decir, η es una unidad de adjunción si y sólo si valen (7.13) y (7.14). Como la condición $F(x) \preceq_Q y$ junto con (7.13) y el hecho que G es un morfismo de orden implican la condición $x \preceq_P G(F(x)) \preceq_P G(y)$ concluimos que existe una unidad de adjunción η de F en G si y sólo si para cada $x \in P$ y cada $y \in G$ se verifica

$$(7.15) \quad \begin{cases} x \preceq_P G(F(x)) \\ x \preceq_P G(y) \implies F(x) \preceq_Q y. \end{cases}$$

Supongamos entonces que (F, G) es una conexión de Galois (o sea vale (7.12)) entonces vale inmediatamente la segunda condición en (7.15). Por otra parte, si (F, G) es una conexión de Galois, vale

$$F(x) \preceq_Q y \implies x \preceq_P G(y)$$

y por lo tanto tomando $y = F(x)$, como $F(x) \preceq_Q F(x)$, resulta que $x \preceq_P G(F(x))$ cualquiera sea $x \in P$. Luego vale (7.15) y existe una adjunción η de F en G .

Recíprocamente, si existe una adjunción η de F en G , entonces por (7.15) tenemos la implicación

$$x \preceq_P G(y) \implies F(x) \preceq_Q y$$

para cada $x \in P$, $y \in Q$. Supongamos ahora que $x \in P$, $y \in Q$ son tales que $F(x) \preceq_Q y$. Como G es un morfismo de orden, $G(F(x)) \preceq_P G(y)$. Pero por (7.15) $x \preceq_P G(F(x))$ y por transitividad resulta

$$x \preceq_P G(F(x)) \preceq_P G(y).$$

Hemos probado entonces que

$$F(x) \preceq_Q y \implies x \preceq_P G(y)$$

con lo cual (F, G) es una conexión de Galois. ■

En muchos ejemplos importantes es más simple encontrar una transformación natural $\varepsilon : (G \circ F) \rightarrow \text{Id}_{\mathcal{D}}$ antes que una unidad de adjunción. Veremos que, bajo ciertas condiciones, ambas construcciones son equivalentes.

Definición 7.3.4. Sean $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ dos funtores. Una **counidad de adjunción** entre F y G es una transformación natural $\varepsilon : F \circ G \rightarrow \text{Id}_{\mathcal{D}}$ tal que para cada objeto X de \mathcal{C} , cada objeto Y de \mathcal{D} y cada morfismo $g : F(X) \rightarrow Y$, existe un único morfismo $g^* : X \rightarrow G(Y)$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} F(G(Y)) & \xrightarrow{\varepsilon_Y} & Y \\ \uparrow F(g^*) & \nearrow g & \\ F(X) & & \end{array}$$

Lema 7.3.5. Toda unidad de adjunción η define una counidad de adjunción y, recíprocamente, toda counidad de adjunción ε define una adjunción.

Demostración. Sean $F : \mathcal{C} \rightarrow \mathcal{D}$ dos funtores y $\eta : \text{Id}_{\mathcal{C}} \rightarrow G \circ F$ una unidad de adjunción.

Construiremos una counidad de adjunción $\varepsilon : F \circ G \rightarrow \text{Id}_{\mathcal{D}}$.

Consideremos $X = G(Y)$ y el morfismo identidad $\text{id}_{G(Y)} : G(Y) \rightarrow G(Y)$. Como η es una unidad de adjunción, existe un único morfismo $\varepsilon_Y = (\text{id}_{G(Y)})^\# : F(X) = F(G(Y)) \rightarrow Y$ tal que el siguiente diagrama conmuta

$$(7.16) \quad \begin{array}{ccc} X & \xrightarrow{\eta_X} & G(F(X)) \\ \searrow \text{id}_{G(Y)} & & \downarrow G(\varepsilon_Y) \\ & & G(Y) \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} G(Y) & \xrightarrow{\eta_{G(Y)}} & G(F(G(Y))) \\ \searrow \text{id}_{G(Y)} & & \downarrow G(\varepsilon_Y) \\ & & G(Y) \end{array}$$

Veamos que ε es una transformación natural. Sean Y, Y' objetos de \mathcal{D} y sea $g : Y \rightarrow Y'$ un morfismo. Debemos probar que el siguiente diagrama conmuta:

$$\begin{array}{ccc} F(G(Y)) & \xrightarrow{\varepsilon_Y} & Y \\ F(G(g)) \downarrow & & \downarrow g \\ F(G(Y')) & \xrightarrow{\varepsilon_{Y'}} & Y' \end{array}$$

Para ello consideremos el siguiente diagrama:

$$\begin{array}{ccccc} G(Y) & \xrightarrow{G(g)} & G(Y') & & \\ \downarrow \text{id}_{G(Y)} & \searrow \eta_{G(Y)} & \downarrow \eta_{G(Y')} & & \\ & G(F(G(Y))) & \xrightarrow{G(F(G(g)))} & G(F(G(Y'))) & \\ \swarrow G(\varepsilon_Y) & & \downarrow \text{id}_{G(Y')} & \swarrow G(\varepsilon_{Y'}) & \\ G(Y) & \xrightarrow{G(g)} & G(Y') & & \end{array}$$

Por (7.16), el diagrama triangular \mathcal{T}_1 con vértices $G(Y)$, $G(Y)$ y $G(F(G(Y)))$ y el diagrama triangular \mathcal{T}_2 con vértices $G(Y')$, $G(Y')$ y $G(F(G(Y')))$ conmutan. El rectángulo \mathcal{R}_1 de vértices $G(Y)$, $G(Y)$, $G(Y')$, $G(Y')$ conmuta trivialmente.

El rectángulo \mathcal{R}_2

$$\begin{array}{ccc} G(Y) & \xrightarrow{G(g)} & G(Y') \\ \downarrow \eta_{G(Y)} & & \downarrow \eta_{G(Y')} \\ G(F(G(Y))) & \xrightarrow{G(F(G(g)))} & G(F(G(Y'))) \end{array}$$

conmuta pues $\eta : \text{Id}_{\mathcal{C}} \rightarrow G \circ F$ es una transformación natural. Por lo tanto

$$\begin{aligned} G(\varepsilon_{Y'}) \circ [G(F(G(g))) \circ \eta_{G(Y)}] &\stackrel{\mathcal{R}_2}{=} G(\varepsilon_{Y'}) \circ [\eta_{G(Y')} \circ G(g)] \\ &\stackrel{asoc}{=} [G(\varepsilon_{Y'}) \circ \eta_{G(Y')}] \circ G(g) \\ &\stackrel{\mathcal{T}_2}{=} \text{id}_{G(Y')} \circ G(g) \\ &= \boxed{G(g)} \\ &\stackrel{\mathcal{R}_1}{=} G(g) \circ \text{id}_{G(Y)} \\ &\stackrel{\mathcal{T}_1}{=} G(g) \circ [G(\varepsilon_Y) \circ \eta_{G(Y)}] \end{aligned}$$

donde sobre el símbolo igual se indica qué diagrama conmutativo se debe utilizar.

Luego, como G es un funtor y la composición es asociativa, concluimos que

$$G(\varepsilon_{Y'} \circ F(G(g))) \circ \eta_{G(Y)} = G(g) = G(g \circ \varepsilon_Y) \circ \eta_{G(Y)}$$

Así, obtenemos que tanto $G(\varepsilon_{Y'} \circ F(G(g)))$ como $G(g \circ \varepsilon_Y)$ hacen que conmute el diagrama

$$\begin{array}{ccc} G(Y) & \xrightarrow{\eta_{G(Y)}} & G(F(G(Y))) \\ & \searrow G(g) & \downarrow \text{---} \\ & & G(Y') \end{array}$$

y por propiedades de la adjunción η sigue que

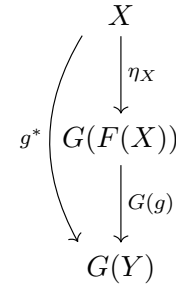
$$\varepsilon_{Y'} \circ F(G(g)) = g \circ \varepsilon_Y$$

como queríamos probar.

Consideremos ahora un objeto X cualquiera de \mathcal{C} , un objeto Y cualquiera de \mathcal{D} y un morfismo $g : F(X) \rightarrow Y$. Buscamos $g^* : X \rightarrow G(Y)$ tal que conmuta el diagrama

$$\begin{array}{ccc} F(G(Y)) & \xrightarrow{\varepsilon_Y} & Y \\ \uparrow F(g^*) & \nearrow g & \\ F(X) & & \end{array}$$

Si existe tal g^* , entonces usando la definición de ε_Y y que η es transformación natural, tenemos

$$\begin{aligned}
 g^* &= \text{id}_{G(Y)} \circ g^* \\
 &= G(\varepsilon_Y) \circ \eta_{G(Y)} \circ g^* \\
 &= G(\varepsilon_Y) \circ G(F(g^*)) \circ \eta_X \\
 &= G(\varepsilon_Y \circ F(g^*)) \circ \eta_X \\
 &= G(g) \circ \eta_X
 \end{aligned}$$


Lo cual muestra la existencia y la unicidad. \square

Ejemplo 7.3.6. Sea \mathcal{C} una categoría con productos y exponenciales, $A \in \mathcal{C}$ un objeto fijo y consideremos la transformación natural $\varepsilon : F_A \rightarrow \text{Id}$ dada en el Ejemplo 7.1.4, con $F_A = \times^A \circ \exp_A$. Recordemos que $F_A(X) = X^A \times A$, $F_A(f) = f^A \times \text{id}_A$ y $\varepsilon_X = \text{eval}_X : X^A \times A \rightarrow X$. Veamos que ε es una counidad de adjunción entre $F : \mathcal{C} \rightarrow \mathcal{C}$, $F = \times^A$ y $G : \mathcal{C} \rightarrow \mathcal{C}$, $G = \exp_A$.

Sea Y un objeto de \mathcal{C} y $g \in \text{Hom}(F(X), Y) = \text{Hom}(X \times A, Y)$. Dado que $G = \exp_A$, debemos definir un morfismo $g^* : X \rightarrow G(Y) = Y^A$, de modo que conmute

$$\begin{array}{ccc}
 F(G(Y)) & \xrightarrow{\varepsilon_Y} & Y \\
 \uparrow F(g^*) & \nearrow g & \\
 F(X) & &
 \end{array}
 \quad \rightsquigarrow \quad
 \begin{array}{ccc}
 Y^A \times A & \xrightarrow{\text{eval}_Y} & Y \\
 \uparrow g^* \times \text{id}_A & \nearrow g & \\
 X \times A & &
 \end{array}$$

Observemos que $g^* = \text{curry}(g)$ es el único morfismo que satisface esta condición. Concluimos que \exp_A es un adjunto a derecha de \times^A , o \times^A es un adjunto a izquierda de \exp_A . \blacksquare

Teorema 7.3.7. Sean \mathcal{C} y \mathcal{D} categorías localmente pequeñas y sean $F : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{D} \rightarrow \mathcal{C}$ dos funtores adjuntos uno del otro. Sea η una unidad de adjunción y ε la correspondiente counidad de adjunción entre F y G . Entonces la función

$$\varphi : \text{Hom}_{\mathcal{C}}(X, G(Y)) \rightarrow \text{Hom}_{\mathcal{D}}(F(X), Y), \quad \varphi(f) = f^\#$$

es biyectiva (un isomorfismo en Set) con inversa

$$\varphi^{-1} : \text{Hom}_{\mathcal{D}}(F(X), Y) \rightarrow \text{Hom}_{\mathcal{C}}(X, G(Y)), \quad \varphi^{-1}(g) = g^*$$

para cada $X \in \text{ob } \mathcal{C}$, $Y \in \text{ob } \mathcal{D}$.

Demostración. Es inmediata de la definición de adjunción. Dejamos los detalles como ejercicio. \square

Notación 7.3.8. En muchos textos si existe una adjunción entre F y G suele denotarse por $\frac{X \rightarrow G(X)}{F(X) \rightarrow Y}$ o bien $F \dashv G$.

Una de las propiedades fundamentales de las adjunciones (que no demostraremos) es que las adjuntas a derecha mapean límites en límites y las adjuntas a izquierda mapean colímites en colímites. La prueba puede consultarse en el Capítulo 9 de [2]. Más precisamente:

Teorema 7.3.9. Sean $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ dos funtores tales que existe una adjunción η de F en G .

1. Sea \mathcal{D} un diagrama en \mathcal{D} que admite un límite $(Y, \mathcal{F}_{\mathcal{D}})$. Entonces $(G(Y), G(\mathcal{G}_{\mathcal{D}}))$ es un límite para $G(\mathcal{D})$ en \mathcal{C} .
2. Sea \mathcal{D} un diagrama en \mathcal{C} que admite un colímite $(X, \mathcal{G}_{\mathcal{D}})$. Entonces $(F(X), F(\mathcal{G}_{\mathcal{D}}))$ es un colímite para $F(\mathcal{D})$ en \mathcal{D} .

Como ecualizadores, coecualizadores, productos y coproductos son casos particulares de límites o colímites tenemos:

Corolario 7.3.10. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ tal que F admite una adjunta a derecha $G : \mathcal{D} \rightarrow \mathcal{C}$. Entonces

1. G mapea ecualizadores y productos en \mathcal{D} en ecualizadores y productos en \mathcal{C} .
2. F mapea coecualizadores y coproductos en \mathcal{C} en coecualizadores y coproductos en \mathcal{D} .

Observación 7.3.11. Como las equivalencias entre categorías admiten adjuntos a izquierda y derecha, el Teorema 7.3.9 es válido para cualquier equivalencia $F : \mathcal{C} \rightarrow \mathcal{D}$. Por lo tanto podemos obtener el Teorema 7.2.17 como consecuencia del Teorema 7.3.9.

7.4. Mónadas

Definición 7.4.1. Una **mónada** sobre una categoría \mathcal{C} consiste de un funtor $T : \mathcal{C} \rightarrow \mathcal{C}$ (denominado un **endofuntor**) y dos transformaciones naturales

- $\eta : \text{id}_{\mathcal{C}} \rightarrow T$ (unidad)
- $\mu : T^2 \rightarrow T$ (multiplicación)

(donde T^n denota la composición de T con sí mismo n -veces) tales que

$$\mu \circ \mu_T = \mu \circ T\mu, \quad \mu \circ \eta_T = \text{id}_T = \mu \circ T\eta$$

donde id_T indica el isomorfismo natural del Ejemplo 7.1.2, $T\eta : \text{ob } \mathcal{C} \rightarrow \text{mor } \mathcal{C}$, $T\eta(X) = T(\eta_X)$, y similarmente $T\mu(X) = T(\mu_X)$, y η_T, μ_T son transformaciones naturales que se definen como $\eta_T(x) = \eta_{T(x)}$, $\mu_T(X) = \mu_{T(X)}$ O sea, los siguientes diagramas son conmutativos.

$$\begin{array}{ccc} T^3 & \xrightarrow{T\mu} & T^2 \\ \mu_T \downarrow & & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array} \quad \begin{array}{ccccc} T & \xrightarrow{\eta_T} & T^2 & \xleftarrow{T\eta} & T \\ & \searrow \text{id}_T & \downarrow \mu & \swarrow \text{id}_T & \\ & & T & & \end{array}$$

Se la denota usualmente por (T, η, μ) cuando \mathcal{C} está sobreentendida.

Ejemplo 7.4.2. Mónadas a partir de adjunciones. Sea η una adjunción de $F : \mathcal{C} \rightarrow \mathcal{D}$ en $G : \mathcal{D} \rightarrow \mathcal{C}$. Consideremos el endofuntor $T = G \circ F : \mathcal{C} \rightarrow \mathcal{C}$.

Tenemos asociadas a T dos transformaciones naturales:

- $\eta : \text{id}_{\mathcal{C}} \rightarrow T$ (unidad de adjunción)

- $\mu : T^2 \rightarrow T$ que se define como sigue:
 - $\varepsilon : F \circ G \rightarrow \text{id}_{\mathcal{D}}$ es una counidad de adjunción asociada a η , con lo cual para cada $X \in \text{ob } \mathcal{C}$, $\varepsilon_{F(X)} : F(G(F(X))) \rightarrow F(X)$
 - Ponemos entonces $\mu_X := G(\varepsilon_{F(X)}) : \underbrace{G(F(G(F(X))))}_{T^2(X)} \rightarrow \underbrace{G(F(X))}_{T(X)}$

Dejamos como ejercicio verificar que $\mu : T^2 \rightarrow T$ es efectivamente una transformación natural.

Veamos que para cada X , conmuta el diagrama

$$\begin{array}{ccc}
 T(T(T(X))) & \xrightarrow{T(\mu_X)} & T(T(X)) \\
 \mu_{T(X)} \downarrow & & \downarrow \mu_X \\
 T(T(X)) & \xrightarrow{\mu_X} & T(X) \\
 \mu_X \circ \mu_{T(X)} & \stackrel{?}{=} & \mu_X \circ T(\mu_X)
 \end{array}$$

O sea, hay que ver que

$$G(\varepsilon_{F(X)}) \circ G(\varepsilon_{F(G(F(X)))}) = G(\varepsilon_{F(X)}) \circ G(F(G(\varepsilon_{F(X)})))$$

Para ello observemos que como $\varepsilon : F \circ G \rightarrow \text{id}_{\mathcal{D}}$ es una transformación natural, el diagrama

$$\begin{array}{ccc}
 F(G(F(G(F(X)))))) & \xrightarrow{\varepsilon_{F(G(F(X)))}} & F(G(F(X))) \\
 F(G(\varepsilon_{F(X)})) \downarrow & & \downarrow \varepsilon_{F(X)} \\
 F(G(F(X))) & \xrightarrow{\varepsilon_{F(X)}} & F(X)
 \end{array}$$

conmuta. Aplicado el funtor G obtenemos lo que queríamos probar. Dejamos como ejercicio probar que

$$\begin{array}{ccccc}
 T & \xrightarrow{\eta_T} & T^2 & \xleftarrow{T\eta} & T \\
 & \searrow \text{id}_T & \downarrow \mu & \swarrow \text{id}_T & \\
 & & T & &
 \end{array}$$

conmuta, y por lo tanto $T : \mathcal{C} \rightarrow \mathcal{C}$ es una mónada sobre \mathcal{C} . ■

Ejemplo 7.4.3. El conjunto de partes como mónada. Consideremos el funtor $T : \text{Set} \rightarrow \text{Set}$ tal que $T(X) = \mathcal{P}(X)$ (el conjunto de partes de X) y si $f : X \rightarrow Y$ es una función, $T(f) : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ es tal que $T(f)(W) = f(W)$ para cada $W \subset X$. Dejamos como primer ejercicio probar que T es efectivamente un endofunctor de Set y que T es una mónada sobre Set con unidad de adjunción

$$\eta_A : A \rightarrow T(A), \quad a \mapsto \{a\}$$

y multiplicación

$$\mu_A(\mathcal{P}(\mathcal{P}(A))) \rightarrow \mathcal{P}(A), \quad \mathcal{X} \mapsto \bigcup \mathcal{X}$$

(Por ejemplo, si $A = \{a, b, c\}$, $\mathcal{X} = \{\{a\}, \{b\}, \{a, b\}\}$, entonces $\mu_A(\mathcal{X}) = \{a, b\}$). ■

Las mónadas y las adjunciones están íntimamente relacionadas. Referimos a [2] para una prueba del siguiente resultado:

Teorema 7.4.4. *Toda mónada proviene de adjunción (es decir, puede ser obtenida como en el Ejemplo 7.4.2). Más aún dada una mónada*

$$(T, \eta, \mu), \quad T : \mathcal{C} \rightarrow \mathcal{C}$$

uno puede formar la categoría $\text{Adj}(\mathcal{C}, T)$ de todas las adjunciones F, G tales que

$$(T, \eta, \mu) = (G \circ F, \eta, G \varepsilon F)$$

en donde η y ε son la unidad y counidad de la adjunción, respectivamente. La categoría $\text{Adj}(\mathcal{C}, T)$ tiene

- *objeto inicial: categoría de Kleisli*
- *objeto terminal: categoría de Eilenberg-Moore*

7.5. Lema de Yoneda

Finalizaremos esta unidad presentando el Lema de Yoneda. La filosofía de este resultado se basa en poder “presentar” una categoría abstracta \mathcal{C} dentro de una categoría más sencilla. Entre las categorías que mejor entendemos se encuentra Set , ya que sus objetos son conjuntos y sus morfismos son funciones usuales entre conjuntos.

Para poder estudiar una categoría \mathcal{C} dentro de Set , necesitamos considerar los funtores de \mathcal{C} en Set . Recordemos que:

- Los funtores de \mathcal{C} en Set forman una categoría: $\text{Set}^{\mathcal{C}}$ (los morfismos de esta categoría son las transformaciones naturales, ver Ejemplo 7.1.6).
- Si \mathcal{C} es una categoría localmente pequeña, para cada objeto A de \mathcal{C} tenemos definido el funtor covariante hom_A (ver Ejemplo 6.3.5) tal que

$$\text{hom}_A : \mathcal{C} \rightarrow \text{Set}$$

$$\text{hom}_A(X) = \text{Hom}_{\mathcal{C}}(A, X)$$

$$\text{hom}_A(f : X \rightarrow X') \in \text{Hom}_{\text{Set}}(\text{Hom}_{\mathcal{C}}(A, X), \text{Hom}_{\mathcal{C}}(A, X')) \quad \text{es tal que} \quad \boxed{\text{hom}_A(f)(g) = f \circ g}$$

$$\begin{array}{ccc} & A & \\ g \swarrow & & \searrow f \circ g \\ X & \xrightarrow{f} & X' \end{array} \quad \text{hom}_A(f) : \underbrace{\text{Hom}_{\mathcal{C}}(A, X)}_{\ni g} \rightarrow \underbrace{\text{Hom}_{\mathcal{C}}(A, X')}_{\ni f \circ g}$$

Si $F : \mathcal{C} \rightarrow \text{Set}$ es un funtor, denotemos por $\text{Nat}(\text{hom}_A, F)$ el conjunto de transformaciones naturales de hom_A en F . Es decir, $\eta \in \text{Nat}(\text{hom}_A, F)$ si η es una familia de funciones (morfismos en Set)

$$\{\eta_B : \text{hom}_A(B) \rightarrow F(B) : B \in \text{ob } \mathcal{C}\}$$

tal que para cada $f : \text{Hom}_{\mathcal{C}}(B, C)$, el siguiente diagrama conmuta:

$$(7.17) \quad \begin{array}{ccc} \text{hom}_A(B) & \xrightarrow{\eta_B} & F(B) \\ \text{hom}_A(f) \downarrow & & \downarrow F(f) \\ \text{hom}_A(C) & \xrightarrow{\eta_C} & F(C) \end{array}$$

Lema 7.5.1 (Lema de Yoneda). *Sean \mathcal{C} una categoría localmente pequeña, y $F : \mathcal{C} \rightarrow \text{Set}$ un funtor (covariante) arbitrario. Fijemos un objeto A de \mathcal{C} cualquiera. Entonces, las transformaciones naturales de hom_A en F están en correspondencia biyectiva con los elementos de $F(A)$:*

$$\text{Nat}(\text{hom}_A, F) \simeq F(A).$$

Demostración. Consideremos una transformación natural $\eta : \text{hom}_A \rightarrow F$. En particular,

$$\eta_A : \text{Hom}_{\mathcal{C}}(A, A) \rightarrow F(A).$$

Pongamos $a = \eta_A(\text{id}_A)$, entonces a es un elemento del conjunto $F(A)$. Observemos que η queda completamente determinada por el elemento a . En efecto, dado un objeto $X \in \text{ob } \mathcal{C}$, y dado $f \in \text{hom}_A(X) = \text{Hom}_{\mathcal{C}}(A, X)$ tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \text{hom}_A(A) & \xrightarrow{\eta_A} & F(A) \\ \text{hom}_A(f) \downarrow & & \downarrow F(f) \\ \text{hom}_A(X) & \xrightarrow{\eta_X} & F(X) \end{array}$$

y como $f = f \circ \text{id}_A = \text{hom}_A(f)(\text{id}_A)$, resulta

$$\eta_X(f) = \eta_X(\text{hom}_A(f)(\text{id}_A)) = (\eta_X \circ \text{hom}_A(f))(\text{id}_A) = (F(f) \circ \eta_A)(\text{id}_A) = F(f)(a)$$

Es decir, como F y f son datos, conociendo a podemos calcular $\eta_X(f)$.

Recíprocamente, cada elemento en $F(A)$ determina una transformación natural $\eta : \text{hom}_A \rightarrow F$ de esta misma forma. \square

Ejemplo 7.5.2. Todo grupo es isomorfo a un grupo de biyecciones (Teorema de Cayley). Sea G un grupo y sea \mathcal{C}_G la categoría asociada. O sea, $\text{ob } \mathcal{C}_G = \{*\}$ y $\text{mor } \mathcal{C}_G = \text{Hom}_{\mathcal{C}_G}(*, *) = G$. Consideremos el funtor $F = \text{hom}_* : \mathcal{C}_G \rightarrow \text{Set}$. Entonces $F(*) = G$ y si $g \in G = \text{Hom}_{\mathcal{C}_G}(*, *)$,

$$\text{hom}_*(g)(h) = gh$$

El Lema de Yoneda nos dice que existe un isomorfismo en Set entre $\text{Nat}(\text{hom}_*, \text{hom}_*)$ y el conjunto $\text{hom}_*(*) = G$. Ahora bien, como \mathcal{C}_G tiene un único objeto, $*$, una transformación natural entre hom_* y hom_* consta de un único morfismo $\eta_* : \text{hom}_*(*) \rightarrow \text{hom}_*(*)$, es decir, una función $\eta_* : G \rightarrow G$ tal que el

siguiente diagrama conmuta:

$$\begin{array}{ccc} G & \xrightarrow{\eta_*} & G \\ \text{hom}_*(g) \downarrow & & \downarrow \text{hom}_*(g) \\ G & \xrightarrow{\eta_*} & G \end{array}$$

O sea, para cada $h \in G$,

$$g\eta_*(h) = \text{hom}_*(g) \circ \eta_*(h) = \eta_* \circ \text{hom}_*(g)(h) = \eta_*(gh)$$

Es decir, una transformación natural $\eta_* : \text{hom}_*(*) \rightarrow \text{hom}_*(*)$ no es otra cosa que una función **equivariante** de G en G (o sea, funciones $f : G \rightarrow G$ tales que $f(gh) = gf(h)$ para cada $f, g \in G$). Recíprocamente, es fácil ver (de manera completamente análoga a lo anterior) que toda función equivariante de G en G define una transformación natural $\mu_* : \text{hom}_* \rightarrow \text{hom}_*$. Pongamos $\text{Equiv}(G)$ el conjunto de funciones equivariantes de G en G , tenemos entonces que

$$\text{Nat}(\text{hom}_*, \text{hom}_*) \simeq \text{Equiv}(G).$$

Observemos que η_* debe ser biyectiva:

- es inyectiva: si $\eta_*(h_1) = \eta_*(h_2)$, entonces

$$h_1\eta_*(e) = \eta_*(h_1e) = \eta_*(h_2) = h_2\eta_*(e) \Rightarrow h_1 = h_2$$

- es sobreyectiva: dado $h_2 \in G$, pongamos $h_1 = h_2\eta_*(e)^{-1}$, entonces

$$\eta_*(h_1) = h_1\eta_*(e) = (h_2\eta_*(e)^{-1})\eta_*(e) = h_2.$$

Dejamos como ejercicio probar que el conjunto de las funciones equivariante de G en G es un subgrupo de $(\mathcal{B}(G), \circ)$, el grupo de biyecciones de G en G .

Por el Lema de Yoneda existe una biyección

$$\text{Equiv}(G) \rightarrow G$$

y no es difícil ver que se trata de un homomorfismos de grupos (dejamos los detalles como ejercicio). Por lo tanto G puede pensarse como un grupo de subgrupo del grupo de transformaciones biyectivas de un conjunto en otro. ■

7.6. Ejercicios

1. Sea \mathcal{C} una categoría con productos, coproductos y exponenciales y $A \in \text{ob}(\mathcal{C})$. Probar que las siguientes aplicaciones pueden extenderse con estructura funtorial:
 - a) $\Delta : \mathcal{C} \rightarrow \mathcal{C} \times \mathcal{C}$ tal que $\Delta(B) = (B, B)$.
 - b) $- \times A : \mathcal{C} \rightarrow \mathcal{C}$ tal que $(- \times A)(B) = B \times A$.
 - c) $-^A \times A : \mathcal{C} \rightarrow \mathcal{C}$ tal que $(-^A \times A)(B) = B^A \times A$.
 - d) $\prod : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ tal que $\prod(B, C) = B \times C$.
 - e) $\sum : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ tal que $\sum(B, C) = B + C$.
 - f) $A^{A^-} : \mathcal{C} \rightarrow \mathcal{C}$ tal que $(A^{A^-})(B) = A^{A^B}$.

2. Dado un conjunto X , definimos el conjunto $\text{List}(X)$ de las listas finitas de elementos de X .
 - a) Probar que $\text{List} : \text{Set} \rightarrow \text{Set}$ es un funtor.
 - b) Considerando ahora $\text{List}(X)$ como un monoide, probar que $\text{List} : \text{Set} \rightarrow \text{Mon}$ es un funtor.
 - c) Determinar si List preserva productos. **Ayuda:** pensar en cuál monoide es isomorfo $\text{List}(X)$ cuando X es un conjunto con un solo elemento.
 - d) Considerar el funtor $\text{List} : \text{Set} \rightarrow \text{Set}$. Mostrar que puede construirse un isomorfismo natural $\text{rev} : \text{List} \rightarrow \text{List}$ tal que rev_X es la función que invierte las palabras de $\text{List}(X)$. ¿Se puede hacer lo mismo con el funtor $\text{List} : \text{Set} \rightarrow \text{Mon}$?
3. Sean $F, G, H : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{D} \rightarrow \mathcal{C}$ funtores.
 - a) Probar que si $F \xrightarrow{\eta} G$, entonces $G \xrightarrow{\eta^{-1}} F$, donde $\eta_A^{-1} = (\eta_A)^{-1}$.
 - b) Probar que si $F \xrightarrow{\eta} G$ y $G \xrightarrow{\theta} H$, entonces $F \xrightarrow{\theta \circ \eta} H$.
4. Sea \mathcal{C} una categoría. Probar que si \mathcal{E} y \mathcal{E}' son esqueletos de \mathcal{C} , entonces \mathcal{E} y \mathcal{E}' son categorías isomorfas.
5. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ un funtor fiel y full. Sea $f : A \rightarrow B$ un morfismo en \mathcal{C} . Probar que f es un isomorfismo si y sólo si $F(f)$ es un isomorfismo en \mathcal{D} .
6. Dada una categoría pequeña \mathcal{C} , mostrar que las categorías \mathcal{C}^2 y $\mathcal{C}^{\rightarrow}$ son isomorfas en Cat .
7. Sea (S, \cdot) un semigrupo y sea $M_S = S \sqcup \{e_S\}$ la unión disjunta de S con un elemento abstracto e_S . Entonces M_S es un monoide con la operación $*$ dada por

$$x * y = x \cdot y \text{ si } x, y \in S, \quad e_S * x = x * e_S = x, \quad \forall x \in S, \quad e_S * e_S = e_S.$$

- a) Definir un funtor $F : \text{Sgrp} \rightarrow \text{Mon}$ tal que, a nivel de objetos, $F(S) = M_S$.
- b) Considerar el funtor $\text{inc} : \text{Mon} \rightarrow \text{Sgrp}$. Probar que F y inc son adjuntos uno del otro.
8. Definir una unidad de adjunción entre el funtor $\text{List} : \text{Set} \rightarrow \text{Set}$ y el funtor olvido $\text{fgt} : \text{Mon} \rightarrow \text{Set}$.
Dado un conjunto de símbolos Σ y la función constante $f : \Sigma \rightarrow U(\mathbb{N}_0)$ tal que $f(x) = 1$, explicitar el morfismo de monoides asociado $\tilde{f} : \text{List}(\Sigma) \rightarrow \mathbb{N}_0$.
9. Sea \mathcal{C} una categoría con productos. Dar una relación de adjunción entre \prod y Δ . Dar un resultado análogo respecto al funtor $\Sigma(X, Y) = X + Y$ cuando \mathcal{C} tiene coproductos.
10. Dada una categoría \mathcal{C} y un objeto A de \mathcal{C} . Probar que $- \times A \dashv -^A$.
11. Sea $F : \mathcal{C} \rightarrow \mathcal{D}$ y $G : \mathcal{D} \rightarrow \mathcal{C}$ dos funtores (\mathcal{C} y \mathcal{D} localmente pequeñas).
 - a) Explicar cómo se definen los funtores.

$$\text{Hom}_{\mathcal{D}}(F(-), -) : \mathcal{C}^{\text{op}} \times \mathcal{D} \rightarrow \text{Set}$$

$$\text{Hom}_{\mathcal{C}}(-, G(-)) : \mathcal{C}^{\text{op}} \times \mathcal{D} \rightarrow \text{Set}$$

- b) Probar que F es adjunto a izquierda de G si y solo si $\text{Hom}_{\mathcal{D}}(F(-), -)$ es naturalmente isomorfo a $\text{Hom}_{\mathcal{C}}(-, G(-))$.
12. Explicar qué es una adjunción en el caso de que las categorías en cuestión sean conjuntos ordenados vistos como categorías.

13. Considere un poset P visto como categoría y un endofunctor $T: P \rightarrow P$. Probar que si T admite estructura monádica, i.e. transformaciones naturales η y μ tal que los axiomas de mónadas se cumplan, entonces $x \leq T(x)$ y $T(T(x)) = T(x)$ para todo $x \in P$.
14. Considere el endofunctor $T: \text{Set} \rightarrow \text{Set}$ definido por $T(X) = \mathcal{P}(X)$ y $T(f: X \rightarrow X')$ es la función que asigna a cada $A \in \mathcal{P}(X)$ el conjunto $f(A) = \{f(a) : a \in A\} \in \mathcal{P}(X')$. Dar estructura monádica a T .
15. Sea (M, \otimes, e) un monoide. Se define el endofunctor $F(X) = M \times X$ sobre Set . Dar estructura monádica a F .
16. Una tupla (M, μ) es una semi-mónada sobre \mathcal{C} cuando $M: \mathcal{C} \rightarrow \mathcal{C}$ es un functor, y $\mu: M \circ M \rightarrow M$ es una transformación natural tal que $\mu \circ \mu_M = \mu \circ M\mu$. Decimos que una semi-mónada (M, μ) se puede extender via $\eta: \text{id}_{\mathcal{C}} \rightarrow M$ a una mónada si la tripla (M, μ, η) es una mónada. Probar que si una semi-mónada (M, μ) admite una extensión a una mónada via η , entonces η es única.
17. Sea **Form** el conjunto de fórmulas de la lógica proposicional. $\mathcal{P}(\mathbf{Form})$ forma un poset, y por ende, se lo puede interpretar como una categoría. Dar un ejemplo de mónada sobre $\mathcal{P}(\mathbf{Form})$.
18. a) Sea (T, η, μ) una mónada sobre una categoría \mathcal{C} . Definimos la *categoría Kleisli* (denotada \mathcal{C}_T) del modo siguiente:
 - $\text{ob } \mathcal{C}_T = \text{ob } \mathcal{C}$.
 - Para cada $A, B \in \text{ob } \mathcal{C}_T$, $\text{Hom}_{\mathcal{C}_T}(A, B) = \text{Hom}_{\mathcal{C}}(A, T(B))$.
 b) Definir la composición en \mathcal{C}_T , y probar que efectivamente \mathcal{C}_T es una categoría.
 c) Definir un functor $F: \mathcal{C} \rightarrow \mathcal{C}_T$ que en los objetos se comporte como $F(A) = A$.
 d) Definir un functor $G: \mathcal{C}_T \rightarrow \mathcal{C}$ que en los objetos se comporte $G(A) = T(A)$.

Bibliografía

- [1] Adámek, J; Herrlich, H; Strecker, G. E., *Abstract and concrete categories. The joy of cats*, Dover Publications (2009). Disponible en <http://katmat.math.uni-bremen.de/acc/>
- [2] Awodey, S., *Category Theory*, Oxford Logic Guides 52, Second Edition, Oxford University Press (2010).
- [3] Banakh, T., *Classical Set Theory*, Disponible en <https://arxiv.org/pdf/2006.01613>
- [4] Becker, M. E.; Pietrocola, N.; Sanchez, C., *Aritmética*, Red Olímpica (2001).
- [5] Cignoli, Roberto. *Teoría axiomática de conjuntos: Una introducción*, Cursos de grado, Fascículo 8, FCEN, UBA (2016). Disponible en <https://cms.dm.uba.ar/depto/public/grado/fascgrado8.pdf>
- [6] Davey, B. A.; Priestley, H. A., *Introduction to Lattices and Order*, 2 Ed., Cambridge University Press (2002).
- [7] Eisenberg, M. *Axiomatic Theory of Sets and Classes*, Holt, Rinehart and Winston Inc. (1971).
- [8] Givant, S.; Halmos, P., *Intorudction to Boolean Algebras*, Springer (2009).
- [9] Grillet, P. A., *Abstract Algebra*, 2 Ed., Springer (2007).
- [10] Grimaldi, R. P., *Matemáticas discretas y combinatoria* (3. edición), Prentice Hall (1998).
- [11] Halmos, P. R., *Naive Set Theory*, Springer (1974).
- [12] Hungerford, T. W., *Algebra*, Springer (1973).
- [13] Krick, Teresa, *Álgebra I*, Cursos de grado, Fasciculo 9, DM-FCEyN-UBA (2017). Disponible en <https://cms.dm.uba.ar/depto/public/grado/fascgrado9.pdf>
- [14] Leinster, T., *Basic category theory*, Cambridge Studies in Advanced Mathematics (2014). Disponible en <https://arxiv.org/pdf/1612.09375>
- [15] Linderholm, C. E., *A Group Epimorphism is Surjective*, The American Mathematical Monthly, 77:2 (1970), 176–177.
- [16] Mc Lane, S., *Categories for the working mathematician*, Segunda Edición, Springer (1978)
- [17] Pierce, B. C., *Basic category theory for computer scientists*, MIT pres (1991).
- [18] Smith, P. *Introducing Category Theory*, Logic matters, Cambridge (2024), disponible en <https://www.logicmatters.net/resources/pdfs/SmithCat.pdf>
- [19] Stillwell, J., *Elements of number theory*, Springer (2003).
- [20] Suarez Alvarez, M. *Notas de Álgebra*, disponible en https://cms.dm.uba.ar/academico/materias/1ercuat2019/algebra_I/NotasAlg1SuarezAlvarez.pdf
- [21] Suarez Alvarez, M. *El Lema de Zorn*, disponible en <https://mate.dm.uba.ar/~aldoc9/Clases/2019/Calculo/Notas/zorn.pdf>