BENEMÉRITA UNIVERSIDAD
AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS FÍSICO
MATEMÁTICAS

SEMIGRUPOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN MATEMÁTICAS

PRESENTA:

LUIS ANTONIO HUERTA SÁNCHEZ

ASESORADO POR:

DR. CARLOS ALBERTO LÓPEZ ANDRADE

PUEBLA JUNIO 2023

Trabajo dedicado a José Guillermo Manuel Sánchez Peña, Guillermina Ramírez Cerón y a todos los abuelos del mundo ...

¡Gracias!

La conclusión de mis estudios universitarios no hubiese sido posible sin el valioso apoyo de las personas y entidades que a continuación menciono y a las cuales, expreso mis más sinceros agradecimientos:

En primera instancia debo agradecer a mis padres José Luis y María Dolores no solo por su apoyo a lo largo de esta etapa académica, si no también por todo el soporte que me han brindado a lo largo de mi vida. Les agradezco de sobremanera todo el esfuerzo que han hecho por mis hermanos y por mi. Espero que la obtención de este grado académico me permita devolverles un poco de lo bastante que ustedes me han ofrecido. Tengo confianza en que vendrán tiempos mejores. Los quiero mucho.

A mis hermanos Eduardo y Karina, les agradezco su apoyo en la etapa final de mi licenciatura, en particular a Eduardo por ayudarme a pagar el examen de inglés. Ustedes fueron los mejores amigos que en la infancia pude tener. Estoy orgulloso de ambos.

A Arianna, por ser parte de mi vida, por creer en mi, por darme ánimos, por tu infinito cariño, por tu tiempo, por tu compañía. Eres causante de las mejores experiencias que me llevo de mi estancia en la universidad, y en general, de las mejores experiencias de mi vida. Estoy sumamente orgulloso de ti. Gracias por levantarme una y otra vez.

A Miguel (Mike), Cornelio, Javier Meneses, Victor, Rocío, Fernanda Nicole, Elizabeth, Manuel (antenas) y Jesús (cosmo), les agradezco haberme adoptado como uno de los suyos y por su amistad. Infinitas gracias por confiar en mis habilidades y por habernos apoyado mutuamente. Les saludo hasta donde quiera que estén y espero, algún día, volvernos a ver. Los recuerdos de nosotros haciendo cualquier cosa en las palapas o en la *pendiente* quedarán siempre en mi memoria.

A los profesores: Rubén Vélez, Jhony Eredi Ramírez, Daniel Jiménez, Julio Poisot, Fernando Velázquez, Agustín Contreras y Alejandro Ramírez, les agradezco profundamente las palabras de aliento que me ofrecieron las veces que fui parte de alguna de sus clases. Posiblemente ustedes nunca lleguen a leer estas líneas, y en caso de que si, quizá mi nombre no figure dentro de su memoria, pero su influencia dentro de mi formación profesional quedará siempre marcada.

A mi asesor de tesis, el profesor Carlos Alberto López Andrade y al cual hay mucho que agradecer. Primeramente, agradezco el haberme tomado en cuenta como su alumno. Des-

pués, le agradezco por todo el tiempo que me regaló durante el lapso que pude trabajar bajo su supervisión, y en especial, le agradezco por haberme dado la oportunidad de escucharme exponer las cosas que me parecían interesantes. Agradezco también el trato amable que he recibido de su parte, pero por sobre todas las cosas le agradezco profundamente toda la confianza que en mí ha depositado y todo el ánimo que me ha otorgado. He de decir que a veces, la confianza y las palabras de aliento son mucho más determinantes que cualquier otro estímulo. De todo el tiempo que he podido formarme bajo su tutela han surgido algunas de las mejores experiencias que me llevo de la universidad, y estoy seguro de que sea lo que sea que yo haga en el futuro, todas las enseñanzas que de usted me llevo serán importantes herramientas que a partir de ahora puedo usar. ¡Muchas gracias por todo profesor!

Agradecimientos sinceros también para mis sinodales: Juan Angoa, Fernando Vilchis y Carlos Guillén por las valiosas sugerencias, correcciones y observaciones que emitieron a mi trabajo. Muchas gracias por haber aceptado leer todas las tediosas líneas de mi tesis.

Finalmente, agradezco a la Vicerrectoría de Investigación y Estudios de Posgrado (VIEP) por su apoyo brindado al proyecto "Descomposiciones hiperarbóreas y eficiencia computacional" con ID: 00185.

Introducción

Los objetos de estudio de este trabajo son dos estructuras algebraicas que llevan por nombre semigrupo y monoide. Tales estructuras son más laxas que otras conocidas como lo son los grupos, anillos, etc, en el sentido de que las primeras solo son conjuntos equipados de una operación binaria asociativa, y en el mejor de los casos, también de un elemento neutro. A pesar de las carencias, los semigrupos y monoides resultan tener propiedades interesantes, además de que proporcionan ejemplos de atractivas construcciones. En la presente obra de tesis se pretende dar testimonio de lo anteriormente dicho. Para tal efecto, se ha organizado el escrito en diez capítulos. El primero de ellos contiene conceptos y resultados bastante conocidos sobre relaciones de equivalencia, relaciones de orden y funciones. Su propósito es proporcionar las herramientas matemáticas esenciales para comprender y a la vez fundamentar los resultados de los capítulos posteriores. En el segundo capítulo se encuentran conceptos y resultados básicos de la teoría de categorías tales como la propia definición de categoría, morfismos y funtores, entre otros. Su objetivo es proporcionar lo mínimo necesario sobre categorías con lo que se tratará en la parte primordial de la tesis. En el tercer capítulo se inicia con la parte principal de la obra. Aquí, el objeto de estudio serán los semigrupos y monoides. Se inicia estableciendo definiciones y resultados generales para después estudiar, en el cuarto capítulo, al primer ejemplo concreto de semigrupo: los semigrupos libres. A continuación, en el quinto capítulo, se ve que la clase de todos los semigrupos junto con los morfismos de semigrupos dan lugar a una categoría. Se revisan entonces algunas de sus propiedades. Posteriormente en los capítulos restantes, se lleva a cabo un estudio de cierta clase de semigrupos a los que se les llamará semigrupos regulares. Dentro de tales semigrupos se encontrarán a los semigrupos completamente regulares, completamente simples, ortodoxos, inversos y de Clifford. Finalmente, se estudian otros ejemplos concretos de semigrupos como lo son las bandas rectangulares, los semigrupos matriz de Rees y el monoide bicíclico. Cabe mencionar que esta tesis está basada en el primer capítulo de [1] y tiene por objetivo proporcionar las demostraciones que sus autores omiten (que resulta ser la mayoría) o bien citan en otros textos. Sobre los resultados que se ofrecen en el presente escrito se puede decir lo siguiente: los enunciados de algunos resultados fueron tomados de [2], algunos otros fueron producto de la propia investigación y de las necesidades que escribir este trabajo implicó y otros tantos aparecen como ejercicios propuestos en la demás bibliografía. Dentro de estos últimos se destacan el problema 3.2.12 página 77 de [7] (ver Teorema 1.4.31) y el problema 7H página 129 de [5] (ver Ejemplo 2.2.17 y Proposiciónes 2.2.16 y 5.2.13) cuyas soluciones se basaron en las sugerencias

que los autores de aquellos libros indican. Salvo estas dos excepciones, todas las pruebas presentadas en el presente trabajo son propias del autor. Por otra parte, a pesar de lo voluminoso que pudiera parecer este trabajo de tesis una rápida mirada a [2] indica que lo que aquí se presenta es solo una introducción al tema. A lo largo del desarrollo del texto se utilizará el símbolo • para indicar el final de una definición, observación o ejemplo y se utilizará, como es costumbre, el símbolo □ para indicar el final de la demostración de un teorema, proposición o corolario. Finalmente, cabe mencionar que el presente trabajo ha sido revisado por un director de tesis y por una comisión de sinodales, los cuales emitieron valiosas observaciones, correciones y sugerencias a fin de presentar el mejor resultado posible. Sin embargo, a pesar de que quien escribe trató de atender la totalidad de inquietudes, es posible que aún permanezcan errores. Debe ser claro que todos aquellos fallos que todavía permanezcan en esta tesis son responsabilidad entera del autor.

Tesis de licenciatura

Luis Antonio Huerta Sánchez

Junio 2023

Índice general

Capítulo 1

Preliminares

El contenido de este capítulo es bastante conocido, sin embargo, constituye la "caja de herramientas" matemáticas fundamentales para la mejor comprensión del presente trabajo, y con el fin de hacer de éste lo más autocontenido posible, se presentan con demostración la mayor parte de las proposiciones enunciadas, esperando también que pueda ser de utilidad para algún lector interesado. Cabe mencionar que se tendrá oportunidad de utilizar la información aquí presentada en los capítulos posteriores.

1.1. Conjuntos y Relaciones

Sean A y B dos conjuntos, recordar que el producto cartesiano de A por B denotado por $A \times B$ es:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

En general, si $n \in \mathbb{N}$, $n \geq 2$ y A_1 , A_2 , . . . , A_n son n conjuntos,

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, ..., a_n) \mid a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n\}.$$

Ademas, para cada $(a_1, a_2, ..., a_n), (x_1, x_2, ..., x_n) \in A_1 \times A_2 \times \cdots \times A_n$

$$(a_1, a_2, ..., a_n) = (x_1, x_2, ..., x_n) \text{ si y solo si } a_i = x_i \text{ para cada } 1 \leq i \leq n.$$

Recuérdese también que el conjunto potencia de A, denotado por cualquiera de los símbolos $\wp(A)$ ó 2^A es:

$$\wp(A) := 2^A := \{X \mid X \subseteq A\}.$$

Con esto en mente se tiene la siguiente:

Definición 1.1.1.

Sean A y B dos conjuntos. Una **relación binaria** (o simplemente relación) de A en B es cualquier subconjunto de $A \times B$.
Si $A = B$, a cualquier relación de A en A se le llamará simplemente relación en A •

Observación 1.1.2.

- Notar entonces que el conjunto $\wp(A \times B)$ tiene por miembros a todas las posibles relaciones de A en B .
- Si $R \subseteq A \times B$, suele usarse la notación aRb para indicar que $(a, b) \in R$.
- Al conjunto $\wp(A \times A)$ se le denotará usando el símbolo $\mathcal{B}(A)$, que es el conjunto de todas las relaciones binarias en A •

Definición 1.1.3.

Sea $R \subseteq A \times B$.

- El **dominio** de la relación R, denotado $Dom(R)$, es :

$$Dom(R) := \{a \in A \,|\, (a, b) \in R \quad \text{para algún} \quad b \in B\}$$

- El **rango ó imagen** de la relación R, denotado $Ran(R)$ ó $Im(R)$ es:

$$Im(R) := \{b \in B \,|\, (a, b) \in R \quad \text{para algún} \quad a \in A\} \bullet$$

Observación 1.1.4.

Sea $R \subseteq A \times B$. Si $(a, b) \in R$ entonces $a \in Dom(R)$ y $b \in Im(R)$. Así $(a, b) \in Dom(R) \times Im(R)$ y por lo tanto $R \subseteq Dom(R) \times Im(R)$. Puede suceder que $R \subsetneq Dom(R) \times Im(R)$, pues para $R = \{(x, x) \,|\, x \in \mathbb{R}\}$ se tiene que $Dom(R) = \mathbb{R} = Im(R)$. Así $(2, 3) \in \mathbb{R} \times \mathbb{R} = Dom(R) \times Im(R)$ pero $(2, 3) \notin R$, por consiguiente $R \subsetneq Dom(R) \times Im(R)$ •

Aquellas relaciones R tales que $R = Dom(R) \times Im(R)$ reciben un nombre especial:

Definición 1.1.5.

Sea $R \subseteq A \times B$. Se dice que R es una **relación rectangular** si R verifica lo siguente:

$$(a, b) \in R \quad \text{y} \quad (c, d) \in R \Longrightarrow (a, d) \in R \bullet$$

Puede caracterizarse a las relaciones rectangulares de la siguiente manera:

Proposición 1.1.6.

$R \subseteq A \times B$ es una relación rectangular si y solo si $R = Dom(R) \times Im(R)$.

Demostración. $\Longrightarrow$) Suponga que R es relación rectangular.
Sea $(a,b) \in Dom(R) \times Im(R)$. Luego $a \in Dom(R)$ y $b \in Im(R)$, de donde $(a,y) \in R$ y $(x,b) \in R$ para algunos $x \in A$ y $y \in B$. Así, como R es relación rectangular se sigue que $(a,b) \in R$ y por tanto $Dom(R) \times Im(R) \subseteq R$. En consecuencia $Dom(R) \times Im(R) = R$.
$\Longleftarrow$) Suponga que $Dom(R) \times Im(R) = R$ y sean $(a,b) \in R \quad$ y $\quad (c,d) \in R$. Entonces $a \in Dom(R)$ y $d \in Im(R)$, de donde $(a,d) \in Dom(R) \times Im(R) = R$. Por consiguiente R es relación rectangular. □

Ejemplo 1.1.7.

- $R = \{(x,x) \,|\, x \in \mathbb{R}\}$ no es relación rectangular.
- $R = \{(m,n) \in \mathbb{N} \times \mathbb{N} \,|\, m \quad$ es par y $\quad n \quad$ es impar$\}$ si es relación rectangular •

A partir de dos relaciones puede obtenerse una tercera:

Definición 1.1.8.

Sean $R \subseteq A \times B$ y $S \subseteq B \times C$. Se define la relación $S \circ R$, leída R seguida de S, como sigue:

$$S \circ R := \{(a,c) \in A \times C \,|\, (a,b) \in R \quad \text{y} \quad (b,c) \in S \quad \text{para algún} \quad b \in B\}\bullet$$

Observación 1.1.9.

- De acuerdo a la Definición 1.1.8, observar que $S \circ R$ es una relación de A en C.
- Sea A un conjunto. A la relación

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

  se le llama la **diagonal** en A.
- Para cada $R \subseteq A \times B$ se verifica que $R \circ \Delta_A = R$ y $\Delta_B \circ R = R$. En efecto, sea $(a,b) \in R$. Como $(b,b) \in \Delta_B$, entonces $(a,b) \in \Delta_B \circ R$, y por tanto $R \subseteq \Delta_B \circ R$.
  Si $(a,b) \in \Delta_B \circ R$, entonces existe $c \in B$ tal que $(a,c) \in R$ y $(c,b) \in \Delta_B$. Así $b = c$ y $(a,b) \in R$. Por lo tanto $\Delta_B \circ R \subseteq R$ y $R = \Delta_B \circ R$. La otra igualdad se verifica de manera similar •

Proposición 1.1.10.

Sean $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$. Entonces la siguiente igualdad se cumple:

$$T \circ (S \circ R) = (T \circ S) \circ R$$

Demostración. Sea $(a,d) \in T \circ (S \circ R)$. Luego, existe $c \in C$ tal que $(a,c) \in S \circ R$ y $(c,d) \in T$. Ahora bien , como $(a,c) \in S \circ R$, debe haber un $b \in B$ para el cuál $(a,b) \in R$ y $(b,c) \in S$. Así se tiene a la vez que $(a,b) \in R$ y $(b,c) \in S$ y $(c,d) \in T$. De ahí que $(a,b) \in R$ y $(b,d) \in T \circ S$ y por lo tanto $(a,d) \in (T \circ S) \circ R$. Se sigue entonces que $T \circ (S \circ R) \subseteq (T \circ S) \circ R$. Ahora bien, si $(a,d) \in (T \circ S) \circ R$, entonces existe $b \in B$ tal que $(a,b) \in R$ y $(b,d) \in T \circ S$. Como $(b,d) \in T \circ S$, entonces $(b,c) \in S$ y $(c,d) \in T$ para algún $c \in C$, así se tiene a la vez que $(a,b) \in R$ y $(b,c) \in S$ y $(c,d) \in T$, de donde $(a,c) \in S \circ R$ y $(c,d) \in T$. Por lo tanto $(a,d) \in T \circ (S \circ R)$ y $(T \circ S) \circ R \subseteq T \circ (S \circ R)$. □

A continuación se enuncia la siguiente definición.

Definición 1.1.11.

Sea A un conjunto y sea $R \in \mathcal{B}(A)$. Se dice que R es:

- **reflexiva**, si $(a,a) \in R$ para cada $a \in A$.
- **irreflexiva**, si $(a,a) \notin R$ para cada $a \in A$.
- **simétrica**, si para cada $a, b \in A$ se verifica lo siguiente:
  $(a,b) \in R \Longrightarrow (b,a) \in R$.
- **asimétrica**, si para cada $a, b \in A$ se verifica lo siguiente:
  $(a,b) \in R \Longrightarrow (b,a) \notin R$.
- **antisimétrica**, si para cada $a, b \in A$ se verifica lo siguiente:
  $(a,b) \in R \quad \text{y} \quad (b,a) \in R \Longrightarrow a = b$.
- **transitiva**, si para cada $a, b, c \in A$ se verifica lo siguiente:
  $(a,b) \in R \quad \text{y} \quad (b,c) \in R \Longrightarrow (a,c) \in R$ •

1.2. Relaciones de equivalencia

Se empieza esta subsección con la siguiente definición.

Definición 1.2.1.

Sea A un conjunto y sea $R \in \mathcal{B}(A)$.

- Se dice que R es **relación de equivalencia** sobre A o simplemente una **equivalencia** sobre A si R es a la vez reflexiva, simétrica y transitiva.
  (ver Definición 1.1.11)
- A la colección de todas las equivalencias sobre A se le denota usando el símbolo $\mathcal{E}(A)$.

- Si $a \in A$, la **clase de equivalencia** de a con respecto de R, denotada $[a]_R$, es:

$$[a]_R := \{x \in A \,|\, (x, a) \in R\}.$$

  Si $b \in [a]_R$, se dice entonces que b es un **representante** de la clase $[a]_R$.

- El **conjunto cociente** A sobre R, denotado $\frac{A}{R}$, es:

$$\tfrac{A}{R} := \{\, [a]_R \,|\, a \in A\} \bullet$$

Observación 1.2.2.

Para cada conjunto A la diagonal Δ_A es una relación de equivalencia. Más aún, si R es una equivalencia en el conjunto A, entonces $\Delta_A \subseteq R$ •

Ejemplo 1.2.3.

Sea $A \neq \emptyset$ y $K \subseteq A$. Se define la siguiente relación:

$$\rho_K = \{(x, y) \in A \times A \,|\, x, y \in K \quad ó \quad x = y\}.$$

ρ_K es reflexiva, pues para cada $x \in A$ se tiene que $x = x$.
ρ_K es simétrica, pues si $(x, y) \in \rho_K$ entonces $x, y \in K \quad ó \quad x = y$, o lo que es lo mismo $y, x \in K \quad ó \quad y = x$. Por consiguiente $(y, x) \in \rho_K$.
ρ_K es transitiva, pues si $(x, y) \in \rho_K$ y $(y, z) \in \rho_K$, entonces se tiene lo siguiente:

$$(x, y \in K \quad ó \quad x = y) \quad \text{y} \quad (y, z \in K \quad ó \quad y = z)$$

lo cuál es equivalente a que

$$(x, y \in K \quad y \quad y, z \in K) \quad \text{ó} \quad (y, z \in K \quad y \quad x = y) \quad \text{ó} \quad (x, y \in K \quad y \quad y = z) \quad \text{ó} \quad (x = y \quad y \quad y = z).$$

En cualquiera de los casos se concluye que $x, z \in K \quad ó \quad x = z$. Por consiguiente $(x, z) \in \rho_K$. Así ρ_K es transitiva y por lo tanto una equivalencia en A.
A ρ_K se le llama **equivalencia de Rees** generada por K.
Si $x \in A$ se tiene que

$$[x]_{\rho_K} := \{y \in A \,|\, x, y \in K \quad \text{ó} \quad x = y\} = \{y \in A \,|\, x, y \in K\} \cup \{x\}$$

Observe que si $x \in K$ entonces $K = \{y \in A \,|\, x, y \in K\}$ y por tanto $[x]_{\rho_K} = K$.
Mientras que si $x \notin K$, $\quad \{y \in A \,|\, x, y \in K\} = \emptyset$ y por lo tanto $[x]_{\rho_K} = \{x\}$.
Así, para cada $x \in A$:

$$[x]_{\rho_K} = \begin{cases} K & si \quad x \in K \\ \{x\} & si \quad x \notin K \end{cases}$$

Se concluye que $\frac{A}{\rho_K} = \{K\} \cup \{\{x\} \,|\, x \notin K\}$ •

Observación 1.2.4.

En el ejemplo anterior, si $K = \emptyset$ entonces $\rho_K = \Delta_A$ •

Proposición 1.2.5.

Sean $A \neq \emptyset$, $R \in \mathcal{E}(A)$ y $a, b \in A$. Son equivalentes los siguientes enunciados:

1. $[a]_R = [b]_R$.
2. $[a]_R \cap [b]_R \neq \emptyset$.
3. aRb.

Demostración. 1) $\Longrightarrow$ 2). Suponga que $[a]_R = [b]_R$, entonces $[a]_R \cap [b]_R = [a]_R$. Además , como R es reflexiva , $a \in [a]_R = [b]_R$, luego $[a]_R \cap [b]_R \neq \emptyset$.
2) $\Longrightarrow$ 3) Suponga que $[a]_R \cap [b]_R \neq \emptyset$ y sea $c \in [a]_R \cap [b]_R$. Luego cRa y cRb, pero como R es simétrica entonces aRc y cRb. Así, como R es transitiva se sigue que aRb.
3) $\Longrightarrow$ 1) Suponga que aRb y sea $c \in [a]_R$. Entonces cRa, pero también aRb, luego como R es transitiva , cRb y por tanto $c \in [b]_R$. Así $[a]_R \subseteq [b]_R$.
Que $[b]_R \subseteq [a]_R$ se sigue de manera similar. Por lo tanto $[a]_R = [b]_R$.

□

Definición 1.2.6.

Sea $A \neq \emptyset$ y $\emptyset \neq \mathcal{F} \subseteq \wp(A)$. Se dice que $\mathcal{F}$ es una **partición** de A si se verifica lo siguiente:

- $A = \bigcup \mathcal{F}$.
- Para cada $X \in \mathcal{F}$, $X \neq \emptyset$.
- Si $X, Y \in \mathcal{F}$ y $X \neq Y$ entonces $X \cap Y = \emptyset$, es decir, los elementos de $\mathcal{F}$ son disjuntos por pares •

Proposición 1.2.7.

Sea $A \neq \emptyset$ y $R \in \mathcal{E}(A)$. Entonces $\frac{A}{R} := \{[a]_R \,|\, a \in A\}$ es una partición de A.

Demostración. Observar que todo elemento de $\frac{A}{R}$ es no vacío, pues como R es reflexiva, se tiene que $a \in [a]_R$ para cada $a \in A$. Más aún, de esto también se sigue que para cada $a \in A$, $a \in [a]_R \subseteq \bigcup \frac{A}{R}$ y por lo tanto $A = \bigcup \frac{A}{R}$.
Finalmente, que los elementos de $\frac{A}{R}$ sean disjuntos por pares se sigue de la Proposición 1.2.5.

□

De acuerdo a la proposición anterior toda equivalencia en A da lugar a una partición de A. El recíproco también se verifica por la siguiente proposición:

Proposición 1.2.8.

Sea $A \neq \emptyset$ y $\mathcal{F}$ una partición de A. Entonces

$$R_{\mathcal{F}} := \{(a,b) \in A \times A \,|\, a,b \in X \quad \text{para algún} \quad X \in \mathcal{F}\}$$

es una relación de equivalencia en A.

Demostración. Como $\mathcal{F}$ es partición de A entonces $A = \bigcup \mathcal{F}$. Así, para cada $a \in A$ existe $X \in \mathcal{F}$ tal que $a \in X$. Por lo tanto $(a,a) \in R_{\mathcal{F}}$ para cada $a \in A$ y $R_{\mathcal{F}}$ es reflexiva. Ahora bien, si $(a,b) \in R_{\mathcal{F}}$, entonces existe $X \in \mathcal{F}$ para el cuál $a,b \in X$, o lo que es lo mismo $b,a \in X$. De ahí que $(b,a) \in R_{\mathcal{F}}$ y $R_{\mathcal{F}}$ es simétrica. Finalmente, si $(a,b) \in R_{\mathcal{F}}$ y $(b,c) \in R_{\mathcal{F}}$ entonces existen $X, Y \in \mathcal{F}$ tales que $a,b \in X$ y $b,c \in Y$. Luego $b \in X \cap Y$ y por tanto $X \cap Y \neq \emptyset$. Así que como los elementos de $\mathcal{F}$ son disjuntos por pares debe ser entonces que $X = Y$. De ahí que $a,c \in X$ y $(a,c) \in R_{\mathcal{F}}$. Por consiguiente $R_{\mathcal{F}}$ es transitiva y por lo tanto $R_{\mathcal{F}}$ es una equivalencia.

□

Observación 1.2.9.

De acuerdo a las Proposiciones 1.2.7 y 1.2.8 toda equivalencia da lugar a una partición y toda partición da lugar a una equivalencia. Más aún , puede probarse (aunque no se hace aquí) que hay una correspondencia biyectiva entre todas las equivalencias de un conjunto dado y todas las particiones de éste •

1.3. Relaciones de orden

Esta sección consta en su mayoría de definiciones, empezando por:

Definición 1.3.1.

- Sea A un conjunto y $\leq \in \mathcal{B}(A)$ (Véase Observación 1.1.2). Se dice que $\leq$ es una **relación de orden parcial** en A si $\leq$ es a la vez reflexiva, antisimétrica y transitiva (ver Definición 1.1.11).
- Un **conjunto parcialmente ordenado** ó **copo** es un par ordenado $(A, \leq)$ donde A es un conjunto y $\leq$ es una relación de orden parcial en A •

Observación 1.3.2.

- Las relaciones de orden parcial suelen denotarse usando los símbolos $\leq, \preccurlyeq$ o parecidos.
- Si $(A, \leq)$ es un copo y $a,b \in A$, se escribe $a < b$ para indicar que $a \leq b$ pero $a \neq b$ •

Ejemplo 1.3.3.

Si A es un conjunto, entonces $(\mathcal{B}(A), \subseteq)$ es un copo. •

Si $(A, \leq)$ es un copo y $a, b \in A$, puede suceder que $a \not\leq b$, por ejemplo, en el copo $(\wp(\mathbb{N}), \subseteq)$ se tiene para $X = \{1\}$ y $Y = \{2\}$ que $X \not\subseteq Y$. Esto da lugar a la siguiente :

Definición 1.3.4.

Sea $(A, \leq)$ un copo.

- Si $a, b \in A$, se dice que a y b son $\leq$- **comparables** o simplemente **comparables** si $a \leq b$ ó $b \leq a$.
- Se dice que $X \subseteq A$ es una $\leq$-**cadena** o simplemente una **cadena**, si cualesquiera dos elementos de X son comparables.
- Si $X = A$ es una $\leq$-cadena, se dice entonces que $\leq$ es un **orden total** y que $(A, \leq)$ es un **conjunto totalmente ordenado** •

Ejemplo 1.3.5.

$(\mathbb{R}, \leq)$ es un conjunto totalmente ordenado, donde $\leq$ denota el orden usual entre números reales •

Definición 1.3.6.

Sea $(A, \leq)$ un copo y $X \subseteq A$. Decimos que $x_0 \in X$ es:

1. Elemento **minimal** de X si para cada $a \in X$ se verifica lo siguiente:

$$a \leq x_0 \Longrightarrow a = x_0$$

2. Elemento **mínimo** de X si para cada $a \in X$, $x_0 \leq a$.
3. Elemento **maximal** de X si para cada $a \in X$ se verifica lo siguiente:

$$x_0 \leq a \Longrightarrow a = x_0$$

4. Elemento **máximo** de X si para cada $a \in X$, $a \leq x_0$ •

Proposición 1.3.7.

Sea $(A, \leq)$ un copo y $X \subseteq A$. Entonces:

1. Todo elemento mínimo (máximo) de X (en caso de haber) es también elemento minimal (maximal).

2. Si X tiene elemento mínimo (máximo) entonces éste debe ser único.

Demostración. 1) Suponga que $x_0 \in X$ es elemento mínimo de X y sea $a \in X$ tal que $a \leq x_0$. Como x_0 es mínimo, entonces $x_0 \leq a$, de manera que al ser $\leq$ antisimétrica se sigue que $a = x_0$ y por tanto x_0 es minimal.
2) Suponga que $x_0, y_0 \in X$ son elementos mínimos de X. Luego $x_0 \leq y_0$ y $y_0 \leq x_0$, de donde $x_0 = y_0$.
La demostración para elementos máximos es análoga.

□

A continuación se enuncia una definición parecida a la anterior:

Definición 1.3.8.

Sea $(A, \leq)$ un copo y $X \subseteq A$. Decimos que $c \in A$ es:

1. **cota superior** de X si para cada $a \in X$, $a \leq c$.
2. **supremo** de X si c es elemento mínimo del conjunto

$$\{w \in A \mid \ w \text{ es cota superior de } X\} .$$

3. **cota inferior** de X si para cada $a \in X$, $c \leq a$.
4. **ínfimo** de X si c es elemento máximo del conjunto

$$\{w \in A \mid \ w \text{ es cota inferior de } X\} \bullet$$

Observación 1.3.9.

- Si $X \subseteq A$ tiene supremo (ínfimo), entonces éste debe ser único según la Proposición 1.3.7.
- Si $X \subseteq A$ tiene supremo, entonces este suele denotarse usando los símbolos $\vee X$ ó $supX$.
  En caso de tener ínfimo este se denota con cualquiera de los símbolos $\wedge X$ ó $infX$
  $\bullet$

Definición 1.3.10.

Un **conjunto bien ordenado** es un copo $(A, \leq)$ en el que todo subconjunto no vacío de A tiene elemento mínimo $\bullet$

Ejemplo 1.3.11.

Si $\leq$ denota el orden usual en $\mathbb{N}$, entonces $(\mathbb{N}, \leq)$ es un conjunto bien ordenado •
Una clase especial de copos es la siguiente:

Definición 1.3.12.

Decimos que un copo $(A, \leq)$ es una :

1. **semiretícula inferior** si para cada $a, b \in A$ el conjunto $\{a, b\}$ tiene ínfimo.
2. **semiretícula inferior completa** si todo subconjunto no vacío de A tiene ínfimo.
3. **semiretícula superior** si para cada $a, b \in A$ el conjunto $\{a, b\}$ tiene supremo.
4. **semiretícula superior completa** si todo subconjunto no vacío de A tiene supremo.
5. **retícula** si es a la vez una semiretícula inferior y superior.
6. **retícula completa** si es a la vez una semiretícula inferior completa y una semiretícula superior completa •

Algunas propiedades de las semiretículas son las siguientes:

Proposición 1.3.13.

Sea $(A, \leq)$ una semiretícula superior (inferior) y para cada $a, b \in A$ sea $a \vee b$ ($a \wedge b$) el supremo (ínfimo) de $\{a, b\}$. Entonces:

1. Para cada $a \in A$, $a \vee a = a$ ($a \wedge a = a$) .
2. Para cada $a, b, c \in A$, $a \vee (b \vee c) = (a \vee b) \vee c$ ($a \wedge (b \wedge c) = (a \wedge b) \wedge c$).
3. Para cada $a, b \in A$, $a \vee b = b \vee a$ ($a \wedge b = b \wedge a$).

Demostración. 1) Sea $a \in A$. Está claro que a es cota superior de $\{a, a\}$. Además , si $c \in A$ es una cota superior de $\{a, a\}$, entonces $a \leq c$. Por lo tanto $a = a \vee a$.
2) Sean $a, b, c \in A$. Como $a \vee (b \vee c)$ es el supremo de $\{a, b \vee c\}$, entonces se tiene que $a \leq a \vee (b \vee c)$ y $b \vee c \leq a \vee (b \vee c)$. Por otra parte, también $b \leq b \vee c$ y $c \leq b \vee c$.
De manera que $b \leq a \vee (b \vee c)$ y $c \leq a \vee (b \vee c)$.
Así, se tiene a la vez lo siguiente:

$$a \leq a \vee (b \vee c) \quad \text{y} \quad b \leq a \vee (b \vee c) \quad \text{y} \quad c \leq a \vee (b \vee c)$$

De las dos primeras relaciones se sigue que $a \vee (b \vee c)$ es cota superior de $\{a, b\}$ y en consecuencia $a \vee b \leq a \vee (b \vee c)$. Por lo tanto $a \vee b \leq a \vee (b \vee c)$ y $c \leq a \vee (b \vee c)$.
De ahí que $a \vee (b \vee c)$ es cota superior de $\{a \vee b, c\}$.
Sea $d \in A$ una cota superior de $\{a \vee b, c\}$. Entonces $a \vee b \leq d$ y $c \leq d$.
Ahora bien, como $a \leq a \vee b$ y $b \leq a \vee b$, se sigue que

$$a \leq d \quad \text{y} \quad b \leq d \quad \text{y} \quad c \leq d.$$

De las dos últimas relaciones se ve que d es cota superior de $\{b, c\}$ y por tanto $b \vee c \leq d$. De esto último y de que $a \leq d$ se sigue que d es cota superior de $\{a, b \vee c\}$ y entonces $a \vee (b \vee c) \leq d$. De todo lo anterior se concluye que $a \vee (b \vee c)$ es el supremo de $\{a \vee b, c\}$ y así $a \vee (b \vee c) = (a \vee b) \vee c$.
3) $a \vee b$ denota al supremo de $\{a, b\}$, mientras que $b \vee a$ denota al supremo de $\{b, a\}$, y como $\{a, b\} = \{b, a\}$, entonces $a \vee b = b \vee a$.
La demostración para ínfimos es análoga.

□

1.4. Funciones

El concepto de función resulta de bastante importancia dentro de las matemáticas:

Definición 1.4.1.

Sean A y B conjuntos y $f \subseteq A \times B$. Se dice que f es una **función** de A en B si se verifica lo siguiente:

1. $Dom(f) = A$.
2. Para cada $a \in A$ y cada $b_1, b_2 \in B$:

$$(a, b_1) \in f \quad \text{y} \quad (a, b_2) \in f \Longrightarrow b_1 = b_2 \bullet$$

Observación 1.4.2.

- Se escribe $f : A \longrightarrow B$ para indicar que f es una función de A en B.
- Dos funciones $f, g : A \longrightarrow B$ son **la misma función**, es decir, iguales, cuando f y g son el mismo subconjunto de $A \times B$.
- Si $f : A \longrightarrow B$ es una función, al conjunto B se le llama **codominio** de f.
- Si $f : A \longrightarrow B$ es una función, entonces de acuerdo con la Definición 1.4.1, para cada $a \in A$ debe existir un único $b \in B$ tal que $(a, b) \in f$.
  Así, si $a \in A$, al único $b \in B$ tal que $(a, b) \in f$ se le denota escribiendo $b = f(a)$ y se dice que b es la imagen de a bajo f.
- De acuerdo a la notación establecida en el punto anterior se tiene que las funciones $f, g : A \longrightarrow B$ serán iguales si y solo si para cada $a \in A$, $f(a) = g(a)$.
- Si $f : A \longrightarrow B$ es una función y $A \neq \emptyset$, entonces $B \neq \emptyset$.

- De manera intuitiva, una función es una "regla" que asigna a cada elemento de un conjunto dado un único elemento de otro conjunto dado.
- En la práctica, una función es definida a través de una "regla de asignación" en lugar de a través de una colección de parejas ordenadas •

Ejemplo 1.4.3.

Para cada conjunto A, la diagonal en A, Δ_A, es una función de A en A.
Δ_A es llamada la función **identidad** en A y se la denota escribiendo id_A, esto es $id_A := \Delta_A$ •

Definición 1.4.4.

Si A y B son conjuntos, se define:

$$B^A := \{f \subseteq A \times B \mid f \text{ es función}\} \bullet$$

Nótese que toda función es en particular una relación entre dos conjuntos. Así , si $f \in B^A$ y $g \in C^B$, tiene sentido entonces según la Definición 1.1.8 considerar a la relación $g \circ f$. Veamos que de hecho $g \circ f \in C^A$:

Proposición 1.4.5.

Sean A , B y C conjuntos. Si $f \in B^A$ y $g \in C^B$, entonces $g \circ f \in C^A$.

Demostración. Observe que $Dom(g \circ f) \subseteq A$, pues $g \circ f$ es una relación de A en C. Sea $a \in A$. Como $Dom(f) = A$, entonces existe $b \in B$ tal que $(a, b) \in f$. Por otra parte, como $Dom(g) = B$, entonces para b existe $c \in C$ tal que $(b, c) \in g$. Así $(a, b) \in f$ y $(b, c) \in g$, de donde $(a, c) \in g \circ f$ y por tanto $a \in Dom(g \circ f)$. En consecuencia $A \subseteq Dom(g \circ f)$, y por consiguiente $Dom(g \circ f) = A$. Suponga ahora que $(a, c) \in g \circ f$ y $(a, c') \in g \circ f$. Entonces existen $b, b' \in B$ tales que

$$(a, b) \in f \quad \text{y} \quad (b, c) \in g \quad \text{y} \quad (a, b') \in f \quad \text{y} \quad (b', c') \in g.$$

De esto se obtiene lo siguiente:

1. $(a, b) \in f \quad \text{y} \quad (a, b') \in f$.
2. $(b, c) \in g \quad \text{y} \quad (b', c') \in g$.

De 1. se sigue que $b = b'$, lo que combinado con 2. resulta en que $(b, c) \in g \quad \text{y}$ $(b, c') \in g$. Por lo tanto $c = c'$ y $g \circ f \in C^A$.

□

Proposición 1.4.6.

Sean A y B conjuntos. Para cada $f \in B^A$, $f \circ id_A = f$ y $id_B \circ f = f$.

Demostración. Se sigue de la Observación 1.1.9. □

Proposición 1.4.7.

Sean A, B y C conjuntos. Si $f \in B^A$ y $g \in C^B$, entonces para cada $a \in A$:

$$(g \circ f)(a) = g(f(a)).$$

Demostración. Sea $a \in A$ arbitrario. Como $g \circ f \in C^A$, entonces $(g \circ f)(a)$ denota al único elemento de C para el cuál $(a, (g \circ f)(a)) \in g \circ f$. Por otro lado, también $(a, f(a)) \in f$ y $(f(a), g(f(a)) \in g$, luego $(a, g(f(a)) \in g \circ f$ y por lo tanto $(g \circ f)(a) = g(f(a))$.

□

Hay diferentes tipos de funciones, empezando por:

Definición 1.4.8.

Se dice que una función $f : A \longrightarrow B$ es **inyectiva** si para cada $a_1, a_2 \in A$ y $b \in B$ se verifica lo siguiente:

$$(a_1, b) \in f \quad \text{y} \quad (a_2, b) \in f \Longrightarrow a_1 = a_2.$$

(O lo que es lo mismo: $f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$) •

Definición 1.4.9.

- Si $f : A \longrightarrow B$ es una función y $X \subseteq A$, entonces

  $$f_{|X} := \{(a, b) \in f \mid a \in X\}$$

  es una función de X en B llamada la **restricción** de f en X.
- Cuando $A = B$ y $f = id_A$, a la función $id_{A|X}$ se le llama la **inclusión** de X en A.
- Para cada $X \subseteq A$, la inclusión de X en B es una función inyectiva •

Puede caracterizarse a las funciones inyectivas de acuerdo a la siguiente proposición:

Proposición 1.4.10.

Sea $f : A \longrightarrow B$ una función con $A \neq \emptyset$. Los siguientes enunciados son equivalentes:

1. f es inyectiva.
2. Existe una función $g : B \longrightarrow A$ tal que $g \circ f = id_A$.

3. Para cada conjunto C y funciones $\alpha, \beta : C \longrightarrow A$ se verifica lo siguiente:

$$f \circ \alpha = f \circ \beta \Longrightarrow \alpha = \beta.$$

Demostración. 1) $\Longrightarrow$ 2) Tomemos un $a_0 \in A$ y dejémoslo fijo. Como f es inyectiva, entonces para cada $b \in Im(f)$ existe un único $a \in A$ tal que $f(a) = b$. Así, para cada $b \in Im(f)$ sea a_b el único elemento de A para el cuál $f(a_b) = b$. Considerese a la función $g : B \longrightarrow A$ definida como sigue:

$$g(b) := \begin{cases} a_b & si \quad b \in Im(f) \\ a_0 & si \quad b \notin Im(f) \end{cases}$$

Sea $x \in A$ arbitrario. Es claro que $f(x) \in Im(f)$. Además, en este caso se tiene que $a_{f(x)} = x$. Luego

$$\begin{aligned} g(f(x)) &= a_{f(x)} \\ &= x \\ &= id_A(x). \end{aligned}$$

De ahí que $g \circ f = id_A$.
2) $\Longrightarrow$ 3) Sea C un conjunto y $\alpha, \beta : C \longrightarrow A$ funciones tales que $f \circ \alpha = f \circ \beta$. Entonces $g \circ (f \circ \alpha) = g \circ (f \circ \beta)$, de manera que de la Proposición 1.1.10 se sigue que $(g \circ f) \circ \alpha = (g \circ f) \circ \beta$, o bien $id_A \circ \alpha = id_A \circ \beta$ y por lo tanto $\alpha = \beta$.
3) $\Longrightarrow$ 1) Sean $a_1, a_2 \in A$ tales que $f(a_1) = f(a_2)$.
Sea $C = \{0, 1\}$ y considérese a las funciones $\alpha, \beta : C \longrightarrow A$ definidas como sigue:

$$\alpha(x) := \begin{cases} a_1 & si \quad x = 0. \\ a_2 & si \quad x = 1. \end{cases}$$

y

$$\beta(x) := \begin{cases} a_2 & si \quad x = 0. \\ a_1 & si \quad x = 1. \end{cases}$$

Entonces

$$f(\alpha(0)) = f(a_1) = f(a_2) = f(\beta(0))$$

mientras que

$$f(\alpha(1)) = f(a_2) = f(a_1) = f(\beta(1)).$$

Por lo tanto $f \circ \alpha = f \circ \beta$ y en consecuencia $\alpha = \beta$. En particular debe ser que $\alpha(0) = \beta(0)$, de donde $a_1 = a_2$ y f es inyectiva.

□

Otra proposición referente a funciones inyectivas es la siguiente:

Proposición 1.4.11.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ funciones.

1. Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.
2. Si $g \circ f$ es inyectiva, entonces f es inyectiva.

Demostración. 1)
Como f y g son inyectivas, entonces existen funciones $g' : C \longrightarrow B$ y $f' : B \longrightarrow A$ tales que $f' \circ f = id_A$ y $g' \circ g = id_B$. Así que se tiene lo siguiente:

$$\begin{aligned}(f' \circ g') \circ (g \circ f) &= f' \circ (g' \circ g) \circ f \\ &= f' \circ id_B \circ f \\ &= f' \circ f \\ &= id_A\end{aligned}$$

De ahí que $g \circ f$ es inyectiva.
2) Como $g \circ f$ es inyectiva, entonces existe una función $h : C \longrightarrow A$ tal que $h \circ (g \circ f) = id_A$, luego $(h \circ g) \circ f = id_A$ y f es inyectiva.

□

Otro tipo importante de funciones es el siguiente:

Definición 1.4.12.

Se dice que una función $f : A \longrightarrow B$ es una función **sobreyectiva** si ocurre que $Im(f) = B$, o lo que es lo mismo, si para cada $b \in B$ existe $a \in A$ tal que $b = f(a)$ •

Hay una proposición análoga a la Proposición 1.4.10 pero ahora referente a funciones sobreyectivas. Sin embargo, para establecerla se necesita hacer uso del llamado axioma de elección que a continuación se enuncia:

Axioma de elección:
Para cada familia $\mathcal{F} \neq \emptyset$ cuyos miembros sean conjuntos no vacios, existe una función $\phi : \mathcal{F} \longrightarrow \bigcup \mathcal{F}$ con la siguiente propiedad:

$$\phi(A) \in A \text{ para cada } A \in \mathcal{F} \bullet$$

Haciendo uso de este axioma puede establecerse la siguiente proposición.

Proposición 1.4.13.

Los siguientes enunciados son equivalentes para una función $f : A \longrightarrow B$ con $A \neq \emptyset$:

1. f es sobreyectiva.

2. Existe una función $g : B \longrightarrow A$ tal que $f \circ g = id_B$.

3. Para cada conjunto C y funciones $\alpha, \beta : B \longrightarrow C$ se verifica lo siguiente:

$$\alpha \circ f = \beta \circ f \Longrightarrow \alpha = \beta.$$

Demostración. 1) $\Longrightarrow$ 2) Para cada $b \in B$ sea $f^{-1}(b) := \{a \in A | f(a) = b\}$. Como f es sobreyectiva entonces para cada $b \in B$ resulta que $f^{-1}(b) \neq \emptyset$. Considerar la familia $\mathcal{F} := \{f^{-1}(b) | b \in B\}$ cuyos miembros son conjuntos no vacios. Por el axioma de elección debe haber una función $\phi : \mathcal{F} \longrightarrow \bigcup \mathcal{F}$ tal que $\phi(f^{-1}(b)) \in f^{-1}(b)$ para cada $b \in B$. Tómese $a_b := \phi(f^{-1}(b))$ y considere la función $g : B \longrightarrow A$ definida por $g(b) := a_b$. Entonces si $b \in B$, $f(g(b)) = f(a_b) = b$. De ahí que $f \circ g = id_B$.
2) $\Longrightarrow$ 3) Sea C un conjunto y $\alpha, \beta : B \longrightarrow C$ funciones tales que $\alpha \circ f = \beta \circ f$. Entonces $(\alpha \circ f) \circ g = (\beta \circ f) \circ g$ de donde $\alpha \circ (f \circ g) = \beta \circ (f \circ g)$ o bien $\alpha \circ id_B = \beta \circ id_B$ y por lo tanto $\alpha = \beta$.
3) $\Longrightarrow$ 1) Sea $C = \{0, 1\}$ y considerense a las funciones $\alpha, \beta : B \longrightarrow C$ definidas como sigue:

$$\alpha(b) := \begin{cases} 0 & si \quad b \notin Im(f). \\ 1 & si \quad b \in Im(f). \end{cases}$$

y

$$\beta(b) := 1 \quad \text{para cada } b \in B.$$

Si $a \in A$, entonces $f(a) \in Im(f)$ de manera que $\alpha(f(a)) = 1 = \beta(f(a))$. De ahí que $\alpha \circ f = \beta \circ f$ y por lo tanto $\alpha = \beta$. Sea $b \in B$, si $b \notin Im(f)$, entonces $\alpha(b) = 0$, pero $\alpha = \beta$, luego $0 = \alpha(b) = \beta(b) = 1$ lo cuál es una contradicción. Se concluye que $B = Im(f)$ y f es sobreyectiva.

□

Proposición 1.4.14.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ funciones.

1. Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

2. Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

Demostración. 1) Como f y g son sobreyectivas, entonces existen funciones $g' : C \longrightarrow B$ y $f' : B \longrightarrow A$ tales que $f \circ f' = id_B$ y $g \circ g' = id_C$. Así que se tiene lo siguiente:

$$\begin{aligned} (g \circ f) \circ (f' \circ g') &= g \circ (f \circ f') \circ g' \\ &= g \circ id_B \circ g' \\ &= g \circ g' \\ &= id_C \end{aligned}$$

De ahí que $g \circ f$ es sobreyectiva.
2) Como $g \circ f$ es sobreyectiva, entonces existe una función $h : C \longrightarrow A$ tal que $(g \circ f) \circ h = id_C$, luego $g \circ (f \circ h) = id_C$ y g es sobreyectiva.

□

Definición 1.4.15.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow A$ funciones. Se dice que g es una:

1. **inversa izquierda** de f si $g \circ f = id_A$.
2. **inversa derecha** de f si $f \circ g = id_B$.
3. **inversa** de f si $g \circ f = id_A$ y $f \circ g = id_B$ •

Observación 1.4.16.

- De acuerdo con la Proposición 1.4.10 las funciones inyectivas son aquellas que poseen al menos una inversa izquierda.
- El axioma de elección implica según la Proposición 1.4.13 que toda función sobreyectiva posee al menos una inversa derecha. •

A aquellas funciones que son a la vez inyectivas y sobreyectivas se les da un nombre especial:

Definición 1.4.17.

Se dice que una función $f : A \longrightarrow B$ es una función **biyectiva** si f tiene al menos una función inversa •

Proposición 1.4.18.

Toda función biyectiva posee exactamente una función inversa.

Demostración. Sea $f : A \longrightarrow B$ una función biyectiva y supongase que $\alpha, \beta : B \longrightarrow A$ son ambas inversas de f. Se tiene entonces lo siguiente:

$$\begin{aligned} \alpha &= \alpha \circ id_B \\ &= \alpha \circ (f \circ \beta) \\ &= (\alpha \circ f) \circ \beta \\ &= id_A \circ \beta \\ &= \beta. \end{aligned}$$

□

Proposición 1.4.19.

Los siguientes enunciados son equivalentes para una función $f : A \longrightarrow B$:

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

Demostración. 1) $\Longrightarrow$ 2)
Si $g : B \longrightarrow A$ es la inversa de f, entonces $g \circ f = id_A$ y $f \circ g = id_B$. Así, de las Proposiciones 1.4.10 y 1.4.13 se sigue lo pedido.
2) $\Longrightarrow$ 1)
Si f es inyectiva y sobreyectiva, entonces según las Proposiciones 1.4.10 y 1.4.13, existen funciones $\alpha, \beta : B \longrightarrow A$ tales que $\alpha \circ f = id_A$ y $f \circ \beta = id_B$. Luego

$$\begin{aligned} \alpha &= \alpha \circ id_B \\ &= \alpha \circ (f \circ \beta) \\ &= (\alpha \circ f) \circ \beta \\ &= id_A \circ \beta \\ &= \beta. \end{aligned}$$

Por lo tanto $\alpha = \beta$ es la inversa de f y f es biyectiva.

□

Corolario 1.4.20.

Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son biyectivas, entonces $g \circ f : A \longrightarrow C$ es también biyectiva.

Demostración. Se sigue de las Proposiciones 1.4.19, 1.4.11 y 1.4.14. □

A partir del concepto de función puede definirse el producto cartesiano de una familia arbitraria de conjuntos:

Definición 1.4.21.

Sea $\mathcal{F} = (A_i)_{i \in I}$ una familia de conjuntos indexada por el conjunto I.
Se define el **producto cartesiano** de la familia $\mathcal{F}$, denotado $\prod_{i \in I} A_i$, como sigue:

$$\prod_{i \in I} A_i := \{f : I \longrightarrow \bigcup_{i \in I} A_i \mid f(i) \in A_i \quad \text{para cada} \quad i \in I\} \bullet$$

Si $\mathcal{F} = (A_i)_{i \in I}$ es una familia de conjuntos, $\prod_{i \in I} A_i$ es su producto cartesiano e $i \in I$, entonces a la función

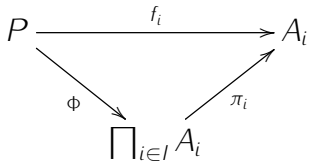
$$\pi_i : \prod_{i \in I} A_i \longrightarrow A_i$$

definida por $\pi_i(f) := f(i)$ se le llama la **i-ésima proyección.** El producto cartesiano de una familia de conjuntos junto con las proyecciones tienen la siguiente propiedad:

Proposición 1.4.22.

Sea $\mathcal{F} = (A_i)_{i\in I}$ una familia de conjuntos y $\prod_{i\in I} A_i$ su producto cartesiano. Entonces para cada conjunto P y cada familia de funciones $\{f_i : P \longrightarrow A_i\}_{i\in I}$, existe una única función $\Phi : P \longrightarrow \prod_{i\in I} A_i$ con la siguiente propiedad:

$$\text{Para cada } i \in I,\ f_i = \pi_i \circ \Phi.$$



Demostración. Sean $p \in P$ e $i \in I$ arbitrarios. Como cada función f_i va de P en el conjunto A_i, entonces $f_i(p) \in A_i$. Tiene sentido así considerar a la función $\phi_p : I \longrightarrow \bigcup_{i\in I} A_i$ definida por $\phi_p(i) := f_i(p)$. Ahora bien, como para cada $i \in I$ se tiene que $f_i(p) \in A_i$, se sigue que $\phi_p \in \prod_{i\in I} A_i$. De acuerdo con esto, es prudente considerar a la función $\Phi : P \longrightarrow \prod_{i\in I} A_i$ definida por $\Phi(p) := \phi_p$.
Afirmación: Para cada $i \in I$, $\quad f_i = \pi_i \circ \Phi$. En efecto, si $p \in P$ e $i \in I$, entonces

$$\pi_i(\Phi(p)) = \pi_i(\phi_p) = \phi_p(i) = f_i(p).$$

De ahí que $f_i = \pi_i \circ \Phi$ y la afirmación se sigue. Supongase ahora que la función $\psi : P \longrightarrow \prod_{i\in I} A_i$ es tal que para cada $i \in I$, $\quad f_i = \pi_i \circ \psi$. Sea $p \in P$ arbitrario. Entonces para cada $i \in I$:

$$\begin{aligned} \psi(p)(i) &= \pi_i(\psi(p)) \\ &= f_i(p) \\ &= \pi_i(\Phi(p)) \\ &= \Phi(p)(i). \end{aligned}$$

Por lo tanto $\psi(p) = \Phi(p)$ para cada $p \in P$ y $\psi = \Phi$. □

La siguiente proposición afirma que bajo ciertas hipótesis, la unión de una colección de funciones es de nuevo una función:

Proposición 1.4.23.

Sean $\mathcal{F} = (A_i)_{i\in I}$ una familia de conjuntos disjuntos por pares, (esto es, tal que si $i, j \in I$ e $i \neq j$, entonces $A_i \cap A_j = \emptyset$), B un conjunto y $\{f_i : A_i \longrightarrow B\}_{i\in I}$ una familia de funciones. Entonces $\bigcup_{i\in I} f_i$ es una función de $\bigcup_{i\in I} A_i$ en B.
Más aún, si $a \in A_i$, entonces $(\bigcup_{i\in I} f_i)(a) = f_i(a)$.

Demostración. Veamos que $Dom(\bigcup_{i\in I} f_i) = \bigcup_{i\in I} A_i$: Si $a \in Dom(\bigcup_{i\in I} f_i)$, entonces $(a,b) \in \bigcup_{i\in I} f_i$ para algún $b \in B$. De ahí que existe $i \in I$ para el cuál $(a,b) \in f_i$, y por tanto $a \in Dom(f_i) = A_i \subseteq \bigcup_{i\in I} A_i$. Por otro lado, si $a \in \bigcup_{i\in I} A_i$, entonces $a \in A_i$ para algún $i \in I$, pero $Dom(f_i) = A_i$, pues f_i es una función. Así que $a \in Dom(f_i)$ y por tanto existe $b \in B$ tal que $(a,b) \in f_i \subseteq \bigcup_{i\in I} f_i$. Se sigue que $(a,b) \in \bigcup_{i\in I} f_i$ y con ello que $a \in Dom(\bigcup_{i\in I} f_i)$. Por consiguiente $Dom(\bigcup_{i\in I} f_i) = \bigcup_{i\in I} A_i$. Ahora bien, si $a \in \bigcup_{i\in I} A_i$ y $b_1, b_2 \in B$ son tales que

$$(a,b_1) \in \bigcup_{i\in I} f_i \quad \text{y} \quad (a,b_2) \in \bigcup_{i\in I} f_i$$

entonces

$$(a,b_1) \in f_i \quad \text{y} \quad (a,b_2) \in f_j$$

para algunos $i, j \in I$. Lo anterior implíca que $a \in Dom(f_i) = A_i$ y $a \in Dom(f_j) = A_j$, y como $\mathcal{F} = (A_i)_{i\in I}$ es una familia de conjuntos disjuntos por pares, entonces debe ser que $i = j$. De esto se sigue que

$$(a,b_1) \in f_i \quad \text{y} \quad (a,b_2) \in f_i$$

así, como f_i es una función, entonces $b_1 = b_2$ y $\bigcup_{i\in I} f_i$ es una función de $\bigcup_{i\in I} A_i$ en B. Finalmente, si $a \in A_i$, entonces $(a, f_i(a)) \in f_i \subseteq \bigcup_{i\in I} f_i$, luego $(a, f_i(a)) \in \bigcup_{i\in I} f_i$ y por lo tanto $(\bigcup_{i\in I} f_i)(a) = f_i(a)$.

□

Sea, de nuevo, $\mathcal{F} = (A_i)_{i\in I}$ una familia de conjuntos indexada por el conjunto I. Defínase, a partir de $\mathcal{F}$, a la siguiente familia:

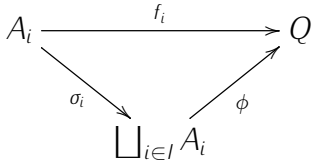
$$\mathcal{F}' := (A_i \times \{i\})_{i\in I}$$

Observe que los elementos de $\mathcal{F}'$ son disjuntos por pares. Sea $\bigsqcup_{i\in I} A_i := \bigcup_{i\in I} A_i \times \{i\}$ y para cada $i \in I$ considerar la función $\sigma_i : A_i \longrightarrow \bigsqcup_{i\in I} A_i$ definida por $\sigma_i(a) := (a,i)$. El conjunto $\bigsqcup_{i\in I} A_i$ junto con las funciones $\sigma_i : A_i \longrightarrow \bigsqcup_{i\in I} A_i$ tienen la siguiente propiedad:

Proposición 1.4.24.

Sea $\mathcal{F} = (A_i)_{i\in I}$ una familia de conjuntos. Entonces para cada conjunto Q y cada familia de funciones $\{f_i : A_i \longrightarrow Q\}_{i\in I}$ existe una única función $\phi : \bigsqcup_{i\in I} A_i \longrightarrow Q$ con la siguiente propiedad:

$$\text{Para cada } i \in I,\ f_i = \phi \circ \sigma_i.$$



Demostración. Para cada $i \in I$ considerar a la función $\bar{f}_i : A_i \times \{i\} \longrightarrow Q$ definida por $\bar{f}_i(a, i) := f_i(a)$. Como $\mathcal{F}' := (A_i \times \{i\})_{i\in I}$ es una familia de conjuntos disjuntos por pares, entonces de la Proposición 1.4.23 se sigue que $\bigcup_{i\in I} \bar{f}_i$ es una función de $\bigcup_{i\in I} A_i \times \{i\}$ en Q. Sea $\phi := \bigcup_{i\in I} \bar{f}_i$ y tómese $i \in I$, entonces, para cada $a \in A_i$:

$$\phi(\sigma_i(a)) = \phi(a, i) = f_i(a).$$

Se sigue así que $f_i = \phi \circ \sigma_i$. Suponga que $\psi : \bigsqcup_{i\in I} A_i \longrightarrow Q$ es una función tal que para cada $i \in I$, $\quad f_i = \psi \circ \sigma_i$.
Si $(a, i) \in A_i \times \{i\}$, entonces:

$$\begin{aligned} \psi(a, i) &= \psi(\sigma_i(a)) \\ &= f_i(a) \\ &= \phi(\sigma_i(a)) \\ &= \phi(a, i). \end{aligned}$$

Por lo tanto $\phi = \psi$ y la proposición se sigue.

□

Definición 1.4.25.

Al conjunto $\bigsqcup_{i\in I} A_i := \bigcup_{i\in I} A_i \times \{i\}$ se le llama **coproducto** de la familia $\mathcal{F} = (A_i)_{i\in I}$ •

Aunque quizá debió haberse hecho antes, se aprovecha ahora para enunciar la siguiente definición:

Definición 1.4.26.

Si $f : A \longrightarrow B$ es una función , $X \subseteq A$ y $Y \subseteq B$, a los conjuntos

$$f^{-1}(Y) := \{a \in A \,|\, f(a) \in Y\} \quad \text{y} \quad f(X) := \{f(a) \,|\, a \in X\}$$

se les llama **imagen inversa de** Y **bajo** f e **imagen directa de** X **bajo** f respectivamente •

Algunas propiedades de la imagen inversa y directa de una función son las siguientes:

Proposición 1.4.27.

Sea $f : A \longrightarrow B$ una función , $X, Y \subseteq A$ y $U, V \subseteq B$. Entonces:

1. $f(X \cup Y) = f(X) \cup f(Y)$.
2. $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$.
3. $f(X \cap Y) \subseteq f(X) \cap f(Y)$.
4. $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$.

5. $f(X) \subseteq f(Y)$, si $X \subseteq Y$.

6. $f^{-1}(U) \subseteq f^{-1}(V)$, si $U \subseteq V$.

7. $X \subseteq f^{-1}(f(X))$, dándose la igualdad cuando f es inyectiva.

8. $f(f^{-1}(U)) \subseteq U$, dándose la igualdad cuando f es sobreyectiva.

Demostración. Solo se probarán 7. y 8.
7. Si $x \in X$ entonces, $f(x) \in f(X)$ y por lo tanto $x \in f^{-1}(f(X))$. De ahí que $X \subseteq f^{-1}(f(X))$. Si en adición se supone que f es inyectiva entonces ocurre lo siguiente: Si $x \in f^{-1}(f(X))$, entonces $f(x) \in f(X)$, de manera que $f(x) = f(a)$ para algún $a \in X$ y por tanto $x = a \in X$, así $f^{-1}(f(X)) \subseteq X$ y en este caso $X = f^{-1}(f(X))$.
8. Si $y \in f(f^{-1}(U))$, entonces $y = f(x)$ para algún $x \in f^{-1}(U)$, así que $f(x) \in U$ y por tanto $y \in U$. De ahí que $f(f^{-1}(U)) \subseteq U$. Si en adición se supone que f es sobreyectiva, entonces ocurre lo siguiente: Sea $y \in U$. Como f es sobreyectiva, entonces $y = f(x)$ para algún $x \in A$. Así que $f(x) \in U$ y por tanto $x \in f^{-1}(U)$. En consecuencia $y = f(x) \in f(f^{-1}(U))$. Se concluye en este caso que $f(f^{-1}(U)) = U$. □

El siguiente concepto es también importante dentro de las matemáticas:

Definición 1.4.28.

Sean A y B conjuntos. Se dice que A es **equipotente** a B si existe al menos una función biyectiva de A en B •

La equipotencia entre conjuntos tiene la siguiente propiedad:

Proposición 1.4.29.

Sean A , B y C conjuntos. Entonces:

1. A es equipotente consigo mismo.

2. Si A es equipotente a B, entonces B es equipotente a A.

3. Si A es equipotente a B y B es equipotente a C, entonces A es equipotente a C.

Demostración. Se sigue de que id_A es biyectiva, de que la inversa de una función biyectiva es también biyectiva y del Corolario 1.4.20. □

Un resultado notable con respecto a la equipotencia de conjuntos es el Teorema de Cantor-Bernstein. Con el fin de establecer dicho resultado nos ayudaremos de la proposición que a continuación se enuncia:

Proposición 1.4.30.

Sea A un conjunto y $f : \wp(A) \longrightarrow \wp(A)$ una función. Supongase que f tiene la siguiente propiedad:

$$\text{Para cada } X, Y \in \wp(A) : X \subseteq Y \Longrightarrow f(X) \subseteq f(Y).$$

Entonces existe $S \in \wp(A)$ tal que $S = f(S)$.

Demostración. Considere la familia $\mathcal{F} := \{R \in \wp(A) | R \subseteq f(R)\}$ y sea $S := \bigcup \mathcal{F}$. Veamos que $S = f(S)$: Si $x \in S$, entonces $x \in R$ para algún $R \in \mathcal{F}$, así, se tiene que $R \subseteq f(R)$ y por tanto $x \in f(R)$. Por otro lado, como $R \in \mathcal{F}$ entonces $R \subseteq \bigcup \mathcal{F} = S$ y de la hipótesis se sigue por tanto que $f(R) \subseteq f(S)$, de donde $x \in f(S)$ y $S \subseteq f(S)$. De esto último se sigue que $f(S) \subseteq f(f(S))$ y con ello que $f(S) \in \mathcal{F}$. Por tanto $f(S) \subseteq \bigcup \mathcal{F} = S$ y en definitiva $S = f(S)$.

□

Teorema. 1.4.31. *(Cantor-Bernstein.)*

Sean A y B conjuntos y sean $f : A \longrightarrow B$ y $g : B \longrightarrow A$ un par de funciones. Si f y g son inyectivas, entonces A es equipotente a B.

Demostración. Es preciso mostrar que existe una función biyectiva de A en B. Para tal fin considere la función $h : \wp(A) \longrightarrow \wp(A)$ definida por $h(X) := A - g(B - f(X))$. Observar que entonces:

$$\begin{aligned} X \subseteq Y \subseteq A &\Longrightarrow f(X) \subseteq f(Y) \\ &\Longrightarrow B - f(Y) \subseteq B - f(X) \\ &\Longrightarrow g(A - f(Y)) \subseteq g(A - f(X)) \\ &\Longrightarrow A - g(A - f(X)) \subseteq A - g(A - f(Y)) \\ &\Longrightarrow h(X) \subseteq h(Y). \end{aligned}$$

Así, de la Proposición 1.4.30 se sigue que $h(S) = S$ para algún $S \subseteq A$, o lo que es lo mismo, $A - g(B - f(S)) = S$. Observar que de esto se sigue que $g(B - f(S)) = A - S$.
Afirmación 1: Para cada $a \in A - S$ existe un único $b_a \in B - f(S)$ tal que $a = g(b_a)$. En efecto, si $a \in A - S$, la existencia de un $b_a \in B - f(S)$ tal que $a = g(b_a)$ se sigue de que $g(B - f(S)) = A - S$. Sea $b \in B - f(S)$ tal que $a = g(b)$. Entonces $g(b_a) = a = g(b)$ y de la inyectividad de g se concluye que $b = b_a$.

Usando lo anterior puede considerarse a la función $k : A \longrightarrow B$ definida como sigue:

$$k(a) := \begin{cases} f(a) & si \quad a \in S. \\ b_a & si \quad a \in A - S. \end{cases}$$

Afirmación 2: Si $k(a) = k(a')$, entonces $a, a' \in S$ ó $a, a' \in A - S$. En efecto, si $k(a) = k(a')$, entonces no puede suceder que $a \in S$ y $a' \in A - S$, pues de ser así, $k(a) = f(a) \in f(S)$ y $k(a') = b_{a'} \in B - f(S)$ con $f(S) \cap (B - f(S)) = \emptyset$. De igual manera se ve que tampoco puede suceder que $a' \in S$ y $a \in A - S$. Por lo tanto debe ocurrir que $a, a' \in S$ ó $a, a' \in A - S$.
Afirmación 3: k es inyectiva. En efecto, sean $a, a' \in A$ tales que $k(a) = k(a')$. Entonces $a, a' \in S$ ó $a, a' \in A - S$. Si $a, a' \in S$, se tiene que $f(a) = k(a) = k(a') = f(a')$, y de la inyectividad de f se sigue que $a = a'$. Si $a, a' \in A - S$, entonces $b_a = k(a) = k(a') = b_{a'}$ de manera que $a = g(b_a) = g(b_{a'}) = a'$.
Afirmación 4: k es sobreyectiva. En efecto, observe que $B = f(S) \cup (B - f(S))$. Sea $b \in B$. Si $b \in f(S)$, entonces $b = f(a)$ para algún $a \in S$, de donde $b = k(a)$. Si $b \in B - f(S)$, entonces como $g(B - f(S)) = A - S$, se sigue que $a := g(b) \in A - S$. Ahora bien, usando la afirmación 1 se ve que $b_a = b$, de donde $k(a) := b_a = b$ y k es sobreyectiva. Se concluye que $k : A \longrightarrow B$ es biyectiva y el teorema queda establecido.

□

Una vez que ya se ha discutido el concepto de relación de equivalencia (ver Definición 1.2.1) y el de función (ver Definición 1.4.1), podemos relacionar a ambos mediante la siguiente proposición.

Proposición 1.4.32.

Toda función induce una relación de equivalencia sobre su dominio.

Demostración. Sea $f : A \longrightarrow B$ una función y considere la siguiente relación en A:

$$Ker(f) := \{(a_1, a_2) \in A \times A \,|\, f(a_1) = f(a_2)\}.$$

$Ker(f)$ es reflexiva pues para cada $a \in A$, $f(a) = f(a)$.
$Ker(f)$ es simétrica pues si $(a_1, a_2) \in Ker(f)$, entonces $f(a_1) = f(a_2)$, o lo que es lo mismo $f(a_2) = f(a_1)$, de donde $(a_2, a_1) \in Ker(f)$.
$Ker(f)$ es transitiva, pues si $(a_1, a_2) \in Ker(f)$ y $(a_2, a_3) \in Ker(f)$, entonces $f(a_1) = f(a_2)$ y $f(a_2) = f(a_3)$, luego $f(a_1) = f(a_3)$ y $(a_1, a_3) \in Ker(f)$.
Se concluye que $Ker(f)$ es una equivalencia en A.

□

Definición 1.4.33.

- Si $f : A \longrightarrow B$ es una función, al conjunto $Ker(f) := \{(a_1, a_2) \in A \times A \,|\, f(a_1) = f(a_2)\}$ se le llama **kernel de** f.
- Sea A un conjunto y $\rho \subseteq A \times A$ una equivalencia sobre A. A la función $\pi_\rho : A \longrightarrow \frac{A}{\rho}$ definida por $\pi_\rho(a) := [a]_\rho$ se le llama la **proyección canónica** con respecto de ρ •

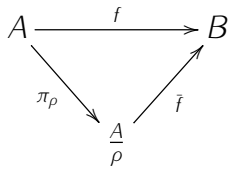
Observación 1.4.34.

Es fácil ver que la proyección canónica $\pi_\rho : A \longrightarrow \frac{A}{\rho}$ es una función sobreyectiva •

A continuación se enuncia un resultado que relaciona el concepto de función, el de relación de equivalencia, el de kernel de una función y el de proyección canónica:

Teorema. 1.4.35. *(De homomorfismo para funciones.)*

Sean $f : A \longrightarrow B$ una función y $\rho \subseteq A \times A$ una equivalencia sobre A tal que $\rho \subseteq Ker(f)$. Entonces existe una única función $\bar{f} : \frac{A}{\rho} \longrightarrow B$ tal que $f = \bar{f} \circ \pi_\rho$. Más aún, si $\rho = Ker(f)$, entonces $\bar{f}$ es inyectiva, y si f es sobreyectiva, entonces $\bar{f}$ es también sobreyectiva.



Demostración. Considerar la función $\bar{f} : \frac{A}{\rho} \longrightarrow B$ definida por $\bar{f}([a]_\rho) := f(a)$. Observar que los elementos del dominio de $\bar{f}$ son clases de equivalencia, y como una clase de equivalencia puede tener, en general, varios representantes, se debe verificar entonces que el valor de $\bar{f}$ en cualquier clase de equivalencia no depende del representante que se tome. Usualmente, al hacer esto suele decirse que hay que verificar que $\bar{f}$ ***está bien definida.*** Supongase que $[a]_\rho = [b]_\rho$, entonces por la Proposición 1.2.5 se sigue que $(a, b) \in \rho \subseteq Ker(f)$, así que $(a, b) \in Ker(f)$ y $f(a) = f(b)$. Por lo tanto $\bar{f}([a]_\rho) = \bar{f}([b]_\rho)$ y $\bar{f}$ está bien definida. Para cada $a \in A$, se tiene lo siguiente:

$$\bar{f}(\pi_\rho(a)) = \bar{f}([a]_\rho) = f(a).$$

Se sigue entonces que $f = \bar{f} \circ \pi_\rho$. Suponga que la función $g : \frac{A}{\rho} \longrightarrow B$ es tal que $f = g \circ \pi_\rho$. Entonces:

$$\begin{aligned} g([a]_\rho) &= g(\pi_\rho(a)) \\ &= f(a) \\ &= \bar{f}(\pi_\rho(a)) \\ &= \bar{f}([a]_\rho). \end{aligned}$$

De ahí que $\bar{f} = g$. Ahora bien, en el caso en que $\rho = Ker(f)$ se tiene que

$$\begin{aligned} \bar{f}([a]_\rho) = \bar{f}([b]_\rho) &\Longrightarrow f(a) = f(b) \\ &\Longrightarrow (a, b) \in Ker(f) = \rho \\ &\Longrightarrow [a]_\rho = [b]_\rho. \end{aligned}$$

Así, $\bar{f}$ es inyectiva. Si f es sobreyectiva, y $b \in B$, entonces $b = f(a)$ para algún $a \in A$. Además, observe que $b = f(a) = \bar{f}([a]_\rho)$, de donde $\bar{f}$ es sobreyectiva.

□

Se termina este capítulo con el siguiente corolario.

Corolario 1.4.36.

Toda función es la composición de una función sobreyectiva seguida de una inyectiva.

Demostración. Sea $f : A \longrightarrow B$ una función y sea $\rho = Ker(f)$. De la Proposición 1.4.35 se tiene que $f = \bar{f} \circ \pi_\rho$ con $\bar{f}$ inyectiva. Ahora bien, del hecho de que la proyección canónica π_ρ sea sobreyectiva se sigue lo pedido. □

.

Capítulo 2

Categorías

En este capítulo se revisan algunas definiciones, conceptos y resultados de la teoría de categorías que serán de utilidad en la parte principal de este trabajo. Haremos uso aquí de algunos de los resultados presentados en el apartado anterior.

2.1. Definición de Categoría

Definición 2.1.1.

Una **categoría** $\mathcal{A}$ es un objeto matemático compuesto por:

1. Una clase $\mathcal{O}$.
2. Para cada $A, B \in \mathcal{O}$, un conjunto $Hom_{\mathcal{A}}(A, B)$.
3. Para cada $A, B, C \in \mathcal{O}$, una función (llamada ley de composición)

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

   con $\circ(f, g) := g \circ f$.
4. Para cada $A \in \mathcal{O}$, un elemento $id_A \in Hom_{\mathcal{A}}(A, A)$.

Además, todo lo anterior debe estar sujeto a lo siguiente:

C1: Para cada $A, B, C, D \in \mathcal{O}$ y cada $f \in Hom_{\mathcal{A}}(A, B)$, $g \in Hom_{\mathcal{A}}(B, C)$ y $h \in Hom_{\mathcal{A}}(C, D)$:

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

C2: Para cada $A, B \in \mathcal{O}$ y cada $f \in Hom_{\mathcal{A}}(A, B)$:

$$id_B \circ f = f \quad \text{y} \quad f \circ id_A = f \bullet$$

Observación 2.1.2.

En el contexto de la Definición 2.1.1:

- La clase $\mathcal{O}$ es denotada por $Ob(\mathcal{A})$ y a sus elementos se les llama **objetos** de $\mathcal{A}$.
- La clase de morfismos de $\mathcal{A}$, denotada por $Mor(\mathcal{A})$, se define como sigue:

$$Mor(\mathcal{A}) := \bigcup_{(A,B)\in Ob(\mathcal{A})\times Ob(\mathcal{A})} Hom_{\mathcal{A}}(A, B) \ .$$

- Si $A, B \in Ob(\mathcal{A})$, a cualquier elemento de $Hom_{\mathcal{A}}(A, B)$ se le llama **morfismo (o flecha)** de A en B. Además, se escribe $f : A \longrightarrow B$ para indicar que $f \in Hom_{\mathcal{A}}(A, B)$.
- Escribir $f : A \longrightarrow B$ puede significar entonces que f es una función del conjunto A en el conjunto B (ver Observación 1.4.2) o que $f \in Hom_{\mathcal{A}}(A, B)$ para alguna categoría $\mathcal{A}$ y algunos $A, B \in Ob(\mathcal{A})$. Se observa en un ejemplo posterior (ver Ejemplos 2.1.2) que toda función entre dos conjuntos es un morfismo entre dos objetos de una categoría, sin embargo, no todo morfismo entre dos objetos de una categoría tiene que ser necesariamente una función. Así, debe tenerse claro el contexto en el cuál se usa la notación $f : A \longrightarrow B$.
- Si $A \in Ob(\mathcal{A})$, al morfismo $id_A \in Hom_{\mathcal{A}}(A, A)$ se le llama **morfismo identidad** en A $\bullet$

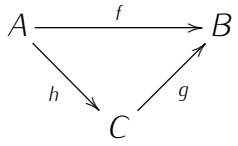
2.1.1. Diagramas conmutativos

Suponga que $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : D \longrightarrow C$ e $i : A \longrightarrow D$ son morfismos de una categoría $\mathcal{A}$. Entonces, suele representarse esta situación dibujando un diagrama de objetos y morfismos como el siguiente:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle g} \\ D & \xrightarrow[h]{} & C \end{array}$$

Un tal diagrama se dice que es **conmutativo (o que conmuta)** si $g \circ f = h \circ i$.

Más generalmente, dada una categoría $\mathcal{A}$, se dice que un diagrama de objetos y morfismos de ésta es **conmutativo (o conmuta)** si siempre que existan dos caminos entre dos objetos, digamos A y B del diagrama, el morfismo resultante de componer los morfismos del primer camino coincide con el morfismo resultante de componer los morfismos del segundo camino. Por ejemplo, el diagrama



será conmutativo si $f = g \circ h$.

2.1.2. Algunos ejemplos

1. Denotemos por V a la clase de todos los conjuntos.

   - Sea $\mathcal{O} = V$.
   - Para cada $A, B \in V$, sea $Hom(A, B) := B^A$.
   - Sea $\circ$ la composición entre funciones.
   - Para cada $A \in V$ sea $id_A \in A^A$ la función identidad.

   De las Proposiciones 1.1.10, 1.4.5 y 1.4.6 se sigue que todo lo anterior da lugar a una categoría llamada la **categoría de conjuntos** que es denotada por SET.

2. Sea M un monoide con elemento neutro $e \in M$. Se define lo siguiente:

   - $\mathcal{O} := \{M\}$.
   - $Hom(M, M) := M$.
   - Sea $\circ$ la operación en el monoide M.
   - $id_M := e$.

   De que la operación en el monoide M sea cerrada y asociativa y de las propiedades de $e \in M$ se sigue que todo lo anterior da lugar a una categoría denotada por $C(M)$. Observar que esta es una categoría con un solo objeto, y además, los morfismos de ella son los elementos del monoide M. (Más adelante se discute con más detalle el concepto de monoide.)

3. Considérese a lo siguiente:

   - Denotemos por $\mathcal{O}$ a la clase de todos los grupos.
   - Para cada $G, H \in \mathcal{O}$ sea

     $$Hom(G, H) := \{f : G \longrightarrow H \mid f \text{ es morfismo de grupos}\}.$$

   - Sea $\circ$ la composición entre funciones.
   - Para cada $G \in \mathcal{O}$ sea id_G la función identidad.

De que la composición entre dos morfismos de grupos es también un morfismo de grupos, de que id_G es un morfismo de grupos y de las Proposiciones 1.1.10 y 1.4.6 se ve que todo lo anterior forma una categoría llamada la **categoría de grupos** que es denotada por GRP.

4. Sea $\mathbb{F}$ un campo y considerese lo siguiente:

   - Sea $\mathcal{O}$ la clase de todos los $\mathbb{F}-$espacios vectoriales de dimensión finita.
   - Para cada $V, W \in \mathcal{O}$ sea

     $$Hom(V, W) := \{T : V \longrightarrow W \mid T \text{ es transformación lineal}\}$$

   - Sea $\circ$ la composición entre funciones.
   - Para cada $V \in \mathcal{O}$ sea id_V la función identidad.

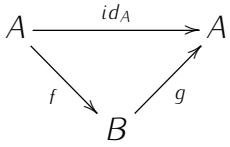
   De que la composición entre dos transformaciones lineales es también una transformación lineal, de que id_V es una transformación lineal y de las Proposiciones 1.1.10 y 1.4.6 se ve que todo lo anterior forma una categoría llamada la **categoría de $\mathbb{F}-$ espacios vectoriales de dimensión finita** que es denotada por $Vec\mathbb{F}$.

2.2. Tipos de morfismos

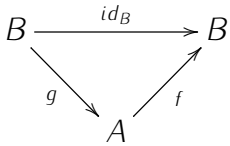
Definición 2.2.1.

Sea $\mathcal{A}$ una categoría y $f \in Hom_{\mathcal{A}}(A, B)$. Se dice que f es una:

1. **sección**, si existe $g \in Hom_{\mathcal{A}}(B, A)$ tal que el siguiente diagrama conmuta:



2. **retracción**, si existe $g \in Hom_{\mathcal{A}}(B, A)$ tal que el siguiente diagrama conmuta:



•

Ejemplos 2.2.2.

- Según las Proposiciones 1.4.10 y 1.4.13 en la categoría SET las funciones inyectivas son las secciones y las sobreyectivas las retracciones.
- Si G es un grupo, entonces puesto que cualquier elemento de G tiene un inverso, se sigue que cualquier morfismo de la categoría $C(G)$ es una sección y una retracción •

A los morfismos que son a la vez secciones y retracciones se les da un nombre especial:

Definición 2.2.3.

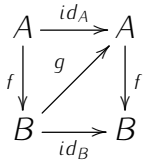
Sea $\mathcal{A}$ una categoría y $f \in Hom_{\mathcal{A}}(A, B)$. Se dice que f es un **$\mathcal{A}$-isomorfismo (o simplemente isomorfismo)** si f es a la vez una sección y una retracción. Si entre los objetos A y B existe al menos un isomorfismo de A en B, entonces se dice que A es **isomorfo** a B y se escribe $A \cong B$ para indicar eso •

Puede caracterizarse a los isomorfismos de una categoría como lo muestra la siguiente proposición:

Proposición 2.2.4.

Sea $\mathcal{A}$ una categoría y $f \in Hom_{\mathcal{A}}(A, B)$. Los siguientes enunciados son equivalentes para f:

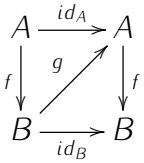
1. f es un isomorfismo.
2. Existe $g \in Hom_{\mathcal{A}}(B, A)$ tal que el siguiente diagrama conmuta:



Demostración. 1) $\Longrightarrow$ 2) Si f es isomorfismo, entonces existen $g, g' : B \longrightarrow A$ tales que $g \circ f = id_A$ y $f \circ g' = id_B$. Luego,

$$\begin{aligned} g &= g \circ id_B \\ &= g \circ (f \circ g') \\ &= (g \circ f) \circ g' \\ &= id_A \circ g' \\ &= g'. \end{aligned}$$

Así $g \circ f = id_A$ y $f \circ g = id_B$ y el diagrama siguente conmuta:

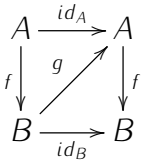


2) $\Longrightarrow$ 1) Se sigue de las Definiciones 2.2.1 y 2.2.3.

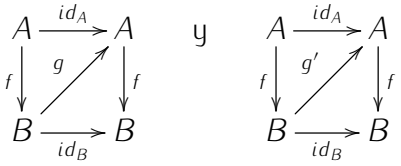
□

Proposición 2.2.5.

Sea $\mathcal{A}$ una categoría y $f \in Hom_{\mathcal{A}}(A, B)$ un isomorfismo. Entonces existe un único $g \in Hom_{\mathcal{A}}(B, A)$ que hace conmutativo al siguiente diagrama:



Demostración. La existencia de un morfismo con las características indicadas se sigue de 2.2.4. Sean $g, g' \in Hom_{\mathcal{A}}(B, A)$ tales que los siguientes diagramas conmutan:



Entonces:

$$\begin{aligned} g &= g \circ id_B \\ &= g \circ (f \circ g') \\ &= (g \circ f) \circ g' \\ &= id_A \circ g' \\ &= g'. \end{aligned}$$

□

Ejemplos 2.2.6.

- Según la Definición 1.4.17 y la Proposición 2.2.4 en la categoría SET las funciones biyectivas son los isomorfismos.
- En la categoría SET dos conjuntos A y B son isomorfos si y solo si son equipotentes (ver Definición 1.4.28).

- Si G es un grupo, entonces cualquier morfismo de la categoría $C(G)$ es una sección y una retracción y por lo tanto un isomorfismo.
- Si A es un objeto de la categoría $\mathcal{A}$, entonces id_A es un isomorfismo, pues $id_A \circ id_A = id_A$ •

Una propiedad de los morfismos descritos es la siguiente:

Proposición 2.2.7.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos morfismos de una categoría $\mathcal{A}$.

1. Si f y g son secciones, entonces $g \circ f$ es sección.
2. Si f y g son retracciones, entonces $g \circ f$ es retracción.
3. Si f y g son isomorfismos, entonces $g \circ f$ es isomorfismo.

Demostración. 1) Como f y g son secciones, entonces existen morfismos $g' : C \longrightarrow B$ y $f' : B \longrightarrow A$ tales que $f' \circ f = id_A$ y $g' \circ g = id_B$. Así que se tiene lo siguiente:

$$\begin{aligned}(f' \circ g') \circ (g \circ f) &= f' \circ (g' \circ g) \circ f \\ &= f' \circ id_B \circ f \\ &= f' \circ f \\ &= id_A\end{aligned}$$

De ahí que $g \circ f$ es sección.
2) Como f y g son retracciones entonces existen morfismos $g' : C \longrightarrow B$ y $f' : B \longrightarrow A$ tales que $f \circ f' = id_B$ y $g \circ g' = id_C$. Así que se tiene lo siguiente:

$$\begin{aligned}(g \circ f) \circ (f' \circ g') &= g \circ (f \circ f') \circ g' \\ &= g \circ id_B \circ g' \\ &= g \circ g' \\ &= id_C\end{aligned}$$

De ahí que $g \circ f$ es retracción.
3) Se sigue de los incisos anteriores. □

Otro tipo importante de morfismos son los siguientes:

Definición 2.2.8.

Sea $\mathcal{A}$ una categoría y $f \in Hom_{\mathcal{A}}(A, B)$. Se dice que f es un:

1. **monomorfismo** si para cada $C \in Ob(\mathcal{A})$ y morfismos $\alpha, \beta : C \longrightarrow A$ se verifica lo siguiente:

   Si el diagrama $\begin{array}{ccc} C & \xrightarrow{\alpha} & A \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[f]{} & B \end{array}$ conmuta, entonces $\alpha = \beta$.

   O lo que es lo mismo, $f \circ \alpha = f \circ \beta \Longrightarrow \alpha = \beta$.

2. **epimorfismo** si para cada $C \in Ob(\mathcal{A})$ y morfismos $\alpha, \beta : B \longrightarrow C$ se verifica lo siguiente:

   Si el diagrama $\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle\alpha} \\ B & \xrightarrow[\beta]{} & C \end{array}$ conmuta, entonces $\alpha = \beta$.

   O lo que es lo mismo, $\alpha \circ f = \beta \circ f \Longrightarrow \alpha = \beta$ •

Resulta que la composición entre dos monomorfismos (epimorfismos) es también un monomorfismo (epimorfismo). Más formalmente se tiene lo siguiente:

Proposición 2.2.9.

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos morfismos de una categoría $\mathcal{A}$.

1. Si f y g son monomorfismos, entonces $g \circ f$ es monomorfismo.
2. Si f y g son epimorfismos, entonces $g \circ f$ es epimorfismo.

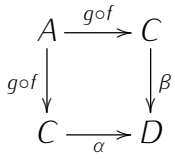
Demostración. 1) Sean $D \in Ob(\mathcal{A})$ y $\alpha, \beta : D \longrightarrow A$ tales que el siguiente cuadrado conmuta:

$$\begin{array}{ccc} D & \xrightarrow{\beta} & A \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle g\circ f} \\ A & \xrightarrow[g\circ f]{} & C \end{array}$$

Entonces se tiene que:

$$\begin{aligned} & (g \circ f) \circ \alpha = (g \circ f) \circ \beta \\ \Longrightarrow \quad & g \circ (f \circ \alpha) = g \circ (f \circ \beta) \\ \Longrightarrow \quad & f \circ \alpha = f \circ \beta \\ \Longrightarrow \quad & \alpha = \beta. \end{aligned}$$

2) Sean $D \in Ob(\mathcal{A})$ y $\alpha, \beta : C \longrightarrow D$ tales que el siguiente cuadrado conmuta:



Entonces se tiene que:

$$\begin{aligned} & \alpha \circ (g \circ f) = \beta \circ (g \circ f) \\ \Longrightarrow \quad & (\alpha \circ g) \circ f = (\beta \circ g) \circ f \\ \Longrightarrow \quad & \alpha \circ g = \beta \circ g \\ \Longrightarrow \quad & \alpha = \beta. \end{aligned}$$

□

Proposición 2.2.10.

En cualquier categoría toda sección es un monomorfismo y toda retracción es un epimorfismo.

Demostración. Sea $f : A \longrightarrow B$ un morfismo de la categoría $\mathcal{A}$. Supóngase que f es una sección y sean $C \in Ob(\mathcal{A})$ y $\alpha, \beta : C \longrightarrow A$ tales que $f \circ \alpha = f \circ \beta$. Como f es una sección entonces existe un morfismo $g : B \longrightarrow A$ tal que $g \circ f = id_A$, de manera que se tiene lo siguiente:

$$\begin{aligned} & f \circ \alpha = f \circ \beta \\ \Longrightarrow \quad & g \circ (f \circ \alpha) = g \circ (f \circ \beta) \\ \Longrightarrow \quad & (g \circ f) \circ \alpha = (g \circ f) \circ \beta \\ \Longrightarrow \quad & id_A \circ \alpha = id_A \circ \beta \\ \Longrightarrow \quad & \alpha = \beta. \end{aligned}$$

De ahí que f es un monomorfismo. La prueba para retracciones es similar y se omite. □

Observación 2.2.11.

En general, no todo monomorfismo (epimorfismo) es una sección (retracción).
En efecto, considerar al monoide $\mathbb{Z} - \{0\}$ con operación el producto usual entre números enteros. A partir de esto considerar a la categoría $C(\mathbb{Z} - \{0\})$ (ver Ejemplos 2.1.2). Se tiene que $2 \in Hom(\mathbb{Z} - \{0\}, \mathbb{Z} - \{0\})$ es un monomorfismo, pues para cada $m, n \in Hom(\mathbb{Z} - \{0\}, \mathbb{Z} - \{0\})$:

$$2n = 2m \Longrightarrow n = m.$$

Sin embargo, $2 \in Hom(\mathbb{Z} - \{0\}, \mathbb{Z} - \{0\})$ no es una sección, pues no existe $k \in Hom(\mathbb{Z} - \{0\}, \mathbb{Z} - \{0\})$ tal que $2k = 1$ •

2.2.1. Ejemplos

Ejemplo 2.2.12. *monomorfismos y epimorfismos en SET.*

Con base en las Proposiciones 1.4.10 y 1.4.13 se deduce que los siguientes enunciados son equivalentes para una función $f : A \longrightarrow B$ con $A \neq \emptyset$:

1. f es inyectiva (sobreyectiva).
2. f es sección (retracción) en SET.
3. f es monomorfismo (epimorfismo) en SET •

Ejemplo 2.2.13. *Isomorfismos en $Vec\mathbb{F}$.*

Sea $\mathbb{F}$ un campo y sea $T : V \longrightarrow W$ un morfismo de $Vec\mathbb{F}$ (ver Ejemplos 2.1.2). Así, T debe ser una transformación lineal. Supongase que, además, T es una función biyectiva. Entonces por la Proposición 1.4.18 existe una única función $S : W \longrightarrow V$ tal que $T \circ S = id_W$ y $S \circ T = id_V$.

Afirmación: S es una transformación lineal. En efecto, sean $w_1, w_2 \in W$ y $\alpha \in \mathbb{F}$. Como T es sobreyectiva, entonces $w_1 = T(v_1)$ y $w_2 = T(v_2)$ para algunos $v_1, v_2 \in V$. De ahí que $S(w_1) = S(T(v_1)) = id_v(v_1) = v_1 \quad$ y $\quad S(w_2) = S(T(v_2)) = id_v(v_2) = v_2$. Luego,

$$\begin{aligned} S(w_1 + w_2) &= S(T(v_1) + T(v_2)) \\ &= S(T(v_1 + v_2)) \\ &= id_V(v_1 + v_2) \\ &= v_1 + v_2 \\ &= S(w_1) + S(w_2). \end{aligned}$$

y

$$\begin{aligned} S(\alpha w_1) &= S(\alpha T(v_1)) \\ &= S(T(\alpha v_1)) \\ &= id_V(\alpha v_1) \\ &= \alpha v_1 \\ &= \alpha S(w_1). \end{aligned}$$

Por consiguiente S es transformación lineal y por lo tanto, $S \in Hom(W, V)$. Debido a que $T \circ S = id_W$ y $S \circ T = id_V$ se deduce que T es un isomorfismo de $Vec\mathbb{F}$. Supóngase ahora que $T : V \longrightarrow W$ es un isomorfismo de $Vec\mathbb{F}$. Entonces existe $S \in Hom(W, V)$ tal que $T \circ S = id_W$ y $S \circ T = id_V$. Como en particular T y S son funciones, se ve entonces que T debe ser biyectiva. Se concluye de todo esto que en la categoría $Vec\mathbb{F}$, $T \in Hom(V, W)$ es un isomorfismo si y solo si T es una función biyectiva •

Ejemplo 2.2.14. *Monomorfismos en $Vec\mathbb{F}$.*

De nuevo, sea $\mathbb{F}$ un campo y sea $T : V \longrightarrow W$ un morfismo de $Vec\mathbb{F}$. Supóngase que T es un monomorfismo y sea $U := Nu(T)$ donde

$$Nu(T) := \{k \in V \mid T(k) = 0_W\}.$$

Observe que U es un subespacio vectorial de V, en particular, U es un $\mathbb{F}-$espacio vectorial de dimensión finita. Considerar a las funciones $R, S : U \longrightarrow V$ definidas por $R(k) := k$ y $S(k) := 0_V$. Es fácil ver que R y S son transformaciones lineales. Ahora bien, para cada $k \in U$:

$$T(R(k)) = T(k) = 0_W.$$

mientras que

$$T(S(k)) = T(0_V) = 0_W.$$

Se sigue entonces que $T \circ R = T \circ S$, y como T es un monomorfismo entonces $R = S$. De ahí que si $k \in U$, entonces $k = R(k) = S(k) = 0_V$. Se concluye que $U := Nu(T) = \{0_V\}$ y en consecuencia T es una función inyectiva. Supóngase ahora que T es una función inyectiva y sean $U \in Ob(Vec\mathbb{F})$ y $R, S : U \longrightarrow V$ transformaciones lineales tales que $T \circ R = T \circ S$. Como en particular U, V, W son conjuntos y R, S, T son funciones, se sigue de la Proposición 1.4.10 que $R = S$ y por lo tanto T debe ser un monomorfismo. Se concluye de todo esto que en la categoría $Vec\mathbb{F}$, $T \in Hom(V, W)$ es un monomorfismo si y solo si T es una función inyectiva •

El siguiente ejemplo está dedicado a exhibir quiénes son los epimorfismos de la categoría de grupos GRP. Para tal efecto, se necesita hacer uso de los siguientes resultados auxiliares:

Proposición 2.2.15.

Si $f, g : G \longrightarrow H$ son morfismos de grupos, entonces

$$I(f, g) := \{a \in G \mid f(a) = g(a)\}$$

es un subgrupo de G.

Demostración. Notar que $I(f, g) \neq \emptyset$, pues si e_G y e_H son los elementos neutros de G y H respectivamente, entonces $f(e_G) = e_H = g(e_G)$.
Si $a, b \in I(f, g)$ se tiene lo siguiente:

$$\begin{aligned} f(ab^{-1}) &= f(a)f(b^{-1}) \\ &= f(a)f(b)^{-1} \\ &= g(a)g(b)^{-1} \\ &= g(a)g(b^{-1}) \\ &= g(ab^{-1}). \end{aligned}$$

De ahí que $ab^{-1} \in I(f,g)$ y por lo tanto $I(f,g)$ es un subgrupo de G.

□

Proposición 2.2.16.

Sea H un grupo y sea K un subgrupo de H. Entonces, existe un grupo G y un par de morfismos de grupos $f_1, f_2 : H \longrightarrow G$ tales que

$$K = I(f_1, f_2).$$

Demostración. Considerar el conjunto $\frac{H}{K} := \{hK \mid h \in H\}$ de clases laterales izquierdas de K en H y sea $\hat{K}$ un conjunto tal que $\hat{K} \cap H = \emptyset$. Observar que como cada $hK \neq \emptyset$, entonces $\hat{K} \notin \frac{H}{K}$. Así, $\{\hat{K}\}$ y $\frac{H}{K}$ son disjuntos. Sea $X := \{\hat{K}\} \cup \frac{H}{K}$. Para cada $h \in H$ considerar las funciones $\hat{\alpha}_h, \hat{\beta}_h : \frac{H}{K} \longrightarrow X$ definidas por $\hat{\alpha}_h(aK) := haK$ y $\hat{\beta}_h(aK) := h^{-1}aK$. Veamos que $\hat{\beta}_h$ está bien definida:

$$\begin{aligned} aK = bK &\Longrightarrow a^{-1}b \in K \\ &\Longrightarrow a^{-1}e_H b \in K \\ &\Longrightarrow a^{-1}hh^{-1}b \in K \\ &\Longrightarrow (h^{-1}a)^{-1}h^{-1}b \in K \\ &\Longrightarrow h^{-1}aK = h^{-1}bK \\ &\Longrightarrow \hat{\beta}_h(aK) = \hat{\beta}_h(bK). \end{aligned}$$

De manera similar se ve que $\hat{\alpha}_h$ está bien definida. Ahora bien, sea ι la inclusión de $\{\hat{K}\}$ en X. Como $\{\hat{K}\}$ y $\frac{H}{K}$ son disjuntos, se sigue de la Proposición 1.4.23 que $\alpha_h := \hat{\alpha}_h \cup \iota$ y $\beta_h := \hat{\beta}_h \cup \iota$ son funciones de X en X, más aún, se tiene que

$$\alpha_h(S) = \begin{cases} haK & si \quad S = aK. \\ \hat{K} & si \quad S = \hat{K}. \end{cases}$$

y

$$\beta_h(S) = \begin{cases} h^{-1}aK & si \quad S = aK. \\ \hat{K} & si \quad S = \hat{K}. \end{cases}$$

Por otra parte, observe que

$$\alpha_h(\beta_h(S)) = \begin{cases} \alpha_h(\beta_h(aK)) = \alpha_h(h^{-1}aK) = hh^{-1}aK = aK & si \quad S = aK. \\ \alpha_h(\beta_h(\hat{K})) = \alpha_h(\hat{K}) = \hat{K} & si \quad S = \hat{K}. \end{cases}$$

Por lo tanto $\alpha_h \circ \beta_h = id_X$. De manera similar se ve que $\beta_h \circ \alpha_h = id_X$ y en consecuencia, para cada $h \in H$, α_h es una función biyectiva. Las funciones α_h tienen la siguiente propiedad:

$$\text{Para cada } h_1, h_2 \in H, \quad \alpha_{h_1h_2} = \alpha_{h_1} \circ \alpha_{h_2}.$$

En efecto, para $S = aK$:

$$\begin{aligned} \alpha_{h_1h_2}(aK) &:= h_1h_2aK \\ &= \alpha_{h_1}(h_2aK) \\ &= \alpha_{h_1}(\alpha_{h_2}(aK)). \end{aligned}$$

mientras que para $S = \hat{K}$:

$$\begin{aligned} \alpha_{h_1h_2}(\hat{K}) &:= \hat{K} \\ &= \alpha_{h_1}(\hat{K}) \\ &= \alpha_{h_1}(\alpha_{h_2}(\hat{K})). \end{aligned}$$

Por lo tanto $\alpha_{h_1h_2} = \alpha_{h_1} \circ \alpha_{h_2}$. Sea $G := S_X$ el grupo de permutaciones del conjunto X. De todo lo anterior, se deduce que la función $f_1 : H \longrightarrow G$ definida por $f_1(h) := \alpha_h$ es un morfismo de grupos. Considerar ahora a la función $\rho : X \longrightarrow X$ definida por

$$\rho(S) = \begin{cases} K & si \quad S = \hat{K}. \\ \hat{K} & si \quad S = K. \\ S & \text{en otro caso.} \end{cases}$$

Es decir, ρ intercambia a K por $\hat{K}$, intercambia a $\hat{K}$ por K y deja a los demás elementos de X fijos. Es fácil ver que ρ es una función biyectiva. Sea $h \in H$. Como $f_1(h) := \alpha_h$ y ρ son ambas biyectivas, tiene sentido considerar a la función $f_2 : H \longrightarrow G$ definida por $f_2(h) := \rho \circ \alpha_h \circ \rho^{-1}$. Si $h_1, h_2 \in H$ entonces:

$$\begin{aligned} f_2(h_1h_2) &: = \rho \circ \alpha_{h_1h_2} \circ \rho^{-1} \\ &= \rho \circ (\alpha_{h_1} \circ \alpha_{h_2}) \circ \rho^{-1} \\ &= \rho \circ (\alpha_{h_1} \circ id_X \circ \alpha_{h_2}) \circ \rho^{-1} \\ &= \rho \circ (\alpha_{h_1} \circ \rho^{-1} \circ \rho \circ \alpha_{h_2}) \circ \rho^{-1} \\ &= (\rho \circ \alpha_{h_1} \circ \rho^{-1}) \circ (\rho \circ \alpha_{h_2} \circ \rho^{-1}) \\ &= f_2(h_1) \circ f_2(h_2). \end{aligned}$$

De ahí que f_2 es un morfismo de grupos.
Afirmación 1)**:** Para cada $k \in K$, $\quad \rho \circ \alpha_k = \alpha_k \circ \rho$. En efecto, sea $k \in K$.

- Si $S = aK$ donde $a \notin K$, entonces $aK \neq K$ y $kaK \neq K$, pues de otra forma, $kaK = K$, de manera que $ka \in K$ y por tanto $a \in K$ (Contradicción). Así, en este caso, $\rho(\alpha_k(aK)) = \rho(kaK) = kaK$, mientras que $\alpha_k(\rho(aK)) = \alpha_k(aK) = kaK$.

- Si $S = K$, entonces $\rho(\alpha_k(K)) = \rho(kK) = \rho(K) = \hat{K}$, mientras que $\alpha_k(\rho(K)) = \alpha_k(\hat{K}) = \hat{K}$.
- Si $S = \hat{K}$, entonces $\rho(\alpha_k(\hat{k})) = \rho(\hat{K}) = K$, mientras que $\alpha_k(\rho(\hat{K})) = \alpha_k(K) = kK = K$.

Por lo tanto $\rho \circ \alpha_k = \alpha_k \circ \rho$.
Afirmación 2): $K \subseteq I(f_1, f_2)$. En efecto, sea $k \in K$. Por la Afirmación 1) se sigue que $\rho \circ \alpha_k = \alpha_k \circ \rho$, de donde $\rho \circ \alpha_k \circ \rho^{-1} = \alpha_k$, o lo que es lo mismo, $f_1(k) = f_2(k)$. Por lo tanto $k \in I(f_1, f_2)$.
Afirmación 3): $I(f_1, f_2) \subseteq K$. En efecto, sea $h \in I(f_1, f_2)$, entonces $f_1(h) = f_2(h)$, de donde $\rho \circ \alpha_h \circ \rho^{-1} = \alpha_h$ y por tanto $\rho \circ \alpha_h = \alpha_h \circ \rho$. Así,

$$\begin{aligned} & \rho(\alpha_h(\hat{K})) = \alpha_h(\rho(\hat{K})) \\ \Longrightarrow\ & \rho(\hat{K}) = \alpha_h(K) \\ \Longrightarrow\ & K = hK \\ \Longrightarrow\ & h \in K. \end{aligned}$$

Por consiguente $I(f_1, f_2) \subseteq K$ y $K = I(f_1, f_2)$.

□

Ejemplo 2.2.17. *Epimorfismos en GRP.*

Sea $f : G \longrightarrow H$ un morfismo de la categoría GRP (ver Ejemplos 2.1.2). Suponga que f es un epimorfismo en GRP. Como $K := Im(f)$ es un subgrupo de H, de la Proposición 2.2.16 se sigue que existe un grupo G' y un par de morfismos de grupos $f_1, f_2 : H \longrightarrow G'$ tales que $K = I(f_1, f_2)$. Ahora bien, si $a \in G$, entonces $f(a) \in Im(f) = I(f_1, f_2)$, de manera que $f_1(f(a)) = f_2(f(a))$ y por lo tanto $f_1 \circ f = f_2 \circ f$. Así, como f es un epimorfismo se sigue que $f_1 = f_2$ y en consecuencia $Im(f) = I(f_1, f_2) = I(f_1, f_1) = \{h \in H \mid f_1(h) = f_1(h)\} = H$. Se sigue entonces que f debe ser una función sobreyectiva. Suponga ahora que f es una función sobreyectiva y sean $K \in Ob(GRP)$ y $\alpha, \beta : H \longrightarrow K$ morfismos de grupos tales que $\alpha \circ f = \beta \circ f$. Sea $h \in H$. Como f es sobreyectiva, entonces $h = f(a)$ para algún $a \in G$. Así:

$$\alpha(h) = \alpha(f(a)) = \beta(f(a)) = \beta(h).$$

Por lo tanto $\alpha = \beta$ y f es un epimorfismo. Se concluye de todo esto que en la categoría GRP, $f \in Hom(G, H)$ es un epimorfismo si y solo si f es una función sobreyectiva •

2.2.2. Observaciones

Observación 2.2.18.

Según el Ejemplo 2.2.12, los monomorfismos de la categoría SET son las funciones inyectivas y según el Ejemplo 2.2.6, dos objetos de SET son isomorfos si y solo si son equipotentes. De acuerdo con esto, el Teorema 1.4.31 afirma que la categoría SET tiene la siguiente propiedad:
Sean $A, B \in Ob(SET)$. Si existe un monomorfismo de A en B y un monomorfismo de B en A, entonces $A \cong B$ •

Observación 2.2.19.

Sea $\mathbb{F}$ un campo y sean $V, W \in Ob(Vec\mathbb{F})$. Suponga que $T : V \longrightarrow W$ y $R : W \longrightarrow V$ son monomorfismos. De acuerdo con el Ejemplo 2.2.14, T y R deben ser inyectivas, de manera que $\hat{T} : V \longrightarrow Im(T)$ y $\hat{R} : W \longrightarrow Im(R)$ definidas por $\hat{T}(v) := T(v)$ y $\hat{R}(w) := R(w)$ son transformaciones lineales biyectivas. Por lo tanto, del Ejemplo 2.2.13 se sigue que $V \cong Im(T)$ y $W \cong Im(R)$. De esto último y de que $Im(T)$ e $Im(R)$ son subespacios vectoriales de W y V respectivamente, se sigue que $DimV \leq DimW$ y $DimW \leq DimV$. En consecuencia $DimV = DimW$ y $V \cong W$. Se concluye que la categoría $Vec\mathbb{F}$ tiene la siguiente propiedad:
Sean $V, W \in Ob(Vec\mathbb{F})$. Si existe un monomorfismo de V en W y un monomorfismo de W en V, entonces $V \cong W$ •

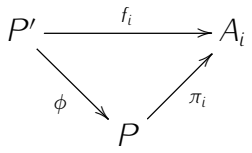
2.3. Productos y Coproductos

Definición 2.3.1.

Sean $\mathcal{A}$ una categoría y $(A_i)_{i\in I} \subseteq Ob(\mathcal{A})$ una familia de objetos indexada por el conjunto I.

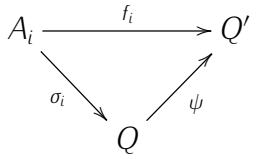
- Un **producto** para la familia $(A_i)_{i\in I}$ es un objeto $P \in Ob(\mathcal{A})$ junto con una familia de morfismos $\{\pi_i : P \longrightarrow A_i\}_{i\in I}$ con la siguiente propiedad:

  Para cada $P' \in Ob(\mathcal{A})$ y cada familia de morfismos $\{f_i : P' \longrightarrow A_i\}_{i\in I}$ existe un único morfismo $\phi : P' \longrightarrow P$ tal que para cada $i \in I$ el siguiente diagrama conmuta:



- Un **coproducto** para la familia $(A_i)_{i\in I}$ es un objeto $Q \in Ob(\mathcal{A})$ junto con una familia de morfismos $\{\sigma_i : A_i \longrightarrow Q\}_{i\in I}$ con la siguiente propiedad:

  Para cada $Q' \in Ob(\mathcal{A})$ y cada familia de morfismos $\{f_i : A_i \longrightarrow Q'\}_{i\in I}$ existe un único morfismo $\psi : Q \longrightarrow Q'$ tal que para cada $i \in I$ el siguiente diagrama conmuta:



•

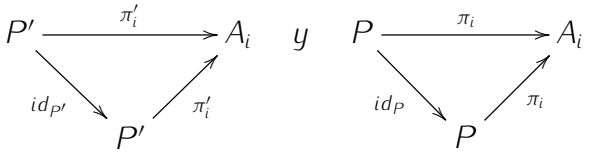
Proposición 2.3.2.

Sean $\mathcal{A}$ una categoría y $(A_i)_{i\in I} \subseteq Ob(\mathcal{A})$ una familia de objetos indexada por el conjunto I.

1. Suponga que $P \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\pi_i : P \longrightarrow A_i\}_{i\in I}$ y $P' \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\pi'_i : P' \longrightarrow A_i\}_{i\in I}$ son ambos productos para $(A_i)_{i\in I}$. Entonces $P \cong P'$.

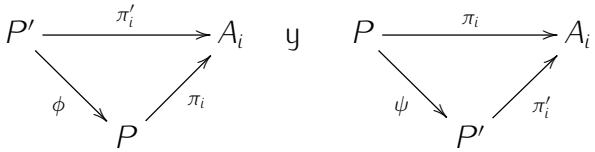
2. Suponga que $Q \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\sigma_i : A_i \longrightarrow Q\}_{i\in I}$ y $Q' \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\sigma'_i : A_i \longrightarrow Q'\}_{i\in I}$ son ambos coproductos para $(A_i)_{i\in I}$. Entonces $Q \cong Q'$.

Demostración. 1) De que P junto con los morfismos π_i , y P' junto con los morfismos π'_i son productos, acompañado de las propiedades de los morfismos identidad, se sigue que id_P e $id_{P'}$ son los únicos morfismos tales que para cada $i \in I$ los siguientes diagramas conmutan:



(2.1)

De nuevo, de que P junto con los morfismos π_i , y P' junto con los morfismos π'_i son productos, se sigue que existen morfismos $\phi : P' \longrightarrow P$ y $\psi : P \longrightarrow P'$ (que además deben ser únicos) tales que para cada $i \in I$ los siguientes triángulos conmutan:



De ahí que para cada $i \in I$:

$$\pi'_i \circ (\psi \circ \phi) = (\pi'_i \circ \psi) \circ \phi = \pi_i \circ \phi = \pi'_i$$

y

$$\pi_i \circ (\phi \circ \psi) = (\pi_i \circ \phi) \circ \psi = \pi'_i \circ \psi = \pi_i$$

Se sigue entonces que los morfismos $\psi \circ \phi$ y $\phi \circ \psi$ hacen conmutar a los diagramas (2. 1) respectivamente, luego $\psi \circ \phi = id_{P'}$ y $\phi \circ \psi = id_P$. De esto último se ve que $\psi : P \longrightarrow P'$ es un isomorfismo, y en consecuencia $P \cong P'$. La prueba de 2) es similar a la anterior y se omite. □

Observación 2.3.3.

- Si $P \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\pi_i : P \longrightarrow A_i\}_{i \in I}$ son un producto para $(A_i)_{i \in I}$, entonces al objeto P se le denota usando el símbolo $\prod_{i \in I} A_i$.
- Si $Q \in Ob(\mathcal{A})$ junto con la familia de morfismos $\{\sigma_i : A_i \longrightarrow Q\}_{i \in I}$ son un coproducto para $(A_i)_{i \in I}$, entonces al objeto Q se le denota usando el símbolo $\bigsqcup_{i \in I} A_i$ •

Ejemplo 2.3.4.

En la categoría SET, el producto y coproducto de una familia $(A_i)_{i \in I}$ está dado en las Definiciones 1.4.21 y 1.4.25 (ver también las Proposiciones 1.4.22 y 1.4.24) •

2.4. Funtores

Definición 2.4.1.

Sean $\mathcal{A}$ y $\mathcal{B}$ categorías. Un **funtor** de $\mathcal{A}$ en $\mathcal{B}$ es una pareja $F = (F_1, F_2)$ de clases-funciones $F_1 : Ob(\mathcal{A}) \longrightarrow Ob(\mathcal{B})$ y $F_2 : Mor(\mathcal{A}) \longrightarrow Mor(\mathcal{B})$ con las siguientes propiedades:

1. $f \in Hom_{\mathcal{A}}(X, Y) \Longrightarrow F_2(f) \in Hom_{\mathcal{B}}(F_1(X), F_1(Y))$.
2. $f \in Hom_{\mathcal{A}}(X, Y) \quad$ y $\quad g \in Hom_{\mathcal{A}}(Y, Z) \Longrightarrow F_2(g \circ f) = F_2(g) \circ F_2(f)$.
3. Para cada $A \in Ob(\mathcal{A}), \quad F_2(id_A) = id_{F_1(A)}$ •

Observación 2.4.2.

- Si $F = (F_1, F_2)$ es un funtor, entonces suele usarse a F para denotar a F_1 y a F_2.
- Se escribe $F : \mathcal{A} \longrightarrow \mathcal{B}$ para indicar que F es un funtor de $\mathcal{A}$ en $\mathcal{B}$ •

Si $F : \mathcal{A} \longrightarrow \mathcal{B}$ es un funtor y $X, Y \in Ob(\mathcal{A})$, entonces $f \in Hom_{\mathcal{A}}(X, Y)$ implica que $F(f) \in Hom_{\mathcal{B}}(F(X), F(Y))$. Por lo tanto, tiene sentido considerar para cada $X, Y \in Ob(\mathcal{A})$ a la función $F_{X,Y} : Hom_{\mathcal{A}}(X, Y) \longrightarrow Hom_{\mathcal{B}}(F(X), F(Y))$ definida por $F_{X,Y}(f) := F(f)$. Pudiera suceder que para cada $X, Y \in Ob(\mathcal{A})$ la función $F_{X,Y}$ sea inyectiva (o sobreyectiva), en cuyo caso al funtor F se le da un nombre especial:

Definición 2.4.3.

Sea $F : \mathcal{A} \longrightarrow \mathcal{B}$ un funtor. Se dice que F es un funtor:

- **fiel**, si para cada $X, Y \in Ob(\mathcal{A})$ la función $F_{X,Y}$ es inyectiva.

- **pleno**, si para cada $X, Y \in Ob(\mathcal{A})$ la función $F_{X,Y}$ es sobreyectiva •

Ejemplos 2.4.4.

1. Sean G y H dos grupos y considere las categorías $C(G)$ y $C(H)$. Suponga que $f : G \longrightarrow H$ es un morfismo de grupos y defínase a $\hat{f} : C(G) \longrightarrow C(H)$ por $\hat{f}(G) := H$ y para cada $x \in Hom(G, G)$ por $\hat{f}(x) := f(x)$. Entonces $\hat{f}$ es un funtor, pues para cada $x, y \in Hom(G, G)$ se tiene que $\hat{f}(x \circ y) = f(xy) = f(x)f(y) = \hat{f}(x) \circ \hat{f}(y)$, además de que $\hat{f}(id_G) = f(e_G) = e_H = id_H = id_{\hat{f}(G)}$.

2. Se define $\mathcal{U} : GRP \longrightarrow SET$ como sigue: Si $(G, \cdot)$ y $(H, *)$ son grupos y $f : G \longrightarrow H$ es un morfismo de grupos, entonces $\mathcal{U}((G, \cdot)) := G$ y $\mathcal{U}(f) := f$. Es fácil ver que $\mathcal{U}$ es un funtor, más aún, $\mathcal{U}$ es un funtor fiel, sin embargo, $\mathcal{U}$ no es un funtor pleno, pues si se toma al grupo $(\mathbb{Z}, +)$, entonces la función $\mathcal{U}_{\mathbb{Z},\mathbb{Z}} : Hom(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathbb{Z}^{\mathbb{Z}}$ no es sobreyectiva, ya que $\alpha : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $\alpha(n) := n + 2$ no es morfismo de grupos. Al funtor $\mathcal{U}$ se le llama **funtor olvidadizo** •

2.5. Categorías concretas

Definición 2.5.1.

Sea $\mathcal{X}$ una categoría. Una **categoría concreta** sobre $\mathcal{X}$ es un par $(\mathcal{A},\mathcal{U})$ donde $\mathcal{A}$ es una categoría y $\mathcal{U} : \mathcal{A} \longrightarrow \mathcal{X}$ es un funtor fiel •

Observación 2.5.2.

Resaltando las hipótesis de la Definición 2.5.1:

- Una categoría concreta sobre SET se denomina **constructo**.

- Si $A \in Ob(\mathcal{A})$ y $f \in Mor(\mathcal{A})$, entonces se escribe $|A|$ en lugar de $\mathcal{U}(A)$ y $|f|$ en lugar de $\mathcal{U}(f)$ •

Ejemplo 2.5.3.

El par $(GRP,\mathcal{U})$ donde $\mathcal{U}$ es el funtor olvidadizo, es una categoría concreta sobre SET, es decir, un constructo •

2.5.1. Objetos Libres

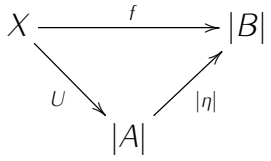
Se cierra este capítulo con los siguientes conceptos:

Definición 2.5.4.

Sea $(\mathcal{A},\mathcal{U})$ una categoría concreta sobre la categoría $\mathcal{X}$ y sea $X \in Ob(\mathcal{X})$:

- Un **morfismo estructurado con dominio** X es un par (f, A), siendo A un objeto de $\mathcal{A}$ y $f : X \longrightarrow |A|$ un morfismo de $\mathcal{X}$.
- Un **morfismo universal sobre** X es un morfismo estructurado (U, A) con dominio X con la siguiente propiedad:

  Para cada morfismo estructurado (f, B) con dominio X, existe un único morfismo de $\mathcal{A}$, digamos $\eta : A \longrightarrow B$, que hace conmutativo al siguiente diagrama:



- Un **objeto libre sobre** X es un objeto $A \in Ob(\mathcal{A})$ para el cuál existe un morfismo universal (U, A) sobre X •

En el siguiente capítulo se verá un ejemplo que ilustre a estos últimos conceptos.

.

Capítulo 3

Semigrupos y Monoides

El presente capítulo da inicio a la parte esencial de este trabajo de tesis. Aquí, el objeto principal de estudio serán dos estructuras algebraicas que llevan por nombre **semigrupo** y **monoide**. Se empieza con algunas definiciones y resultados generales para posteriormente estudiar a ciertos semigrupos y monoides con propiedades particulares.

3.1. Definiciones y resultados generales

A partir de dos objetos de un mismo tipo, ¿cómo podemos obtener un tercero de ese mismo tipo?. En este sentido se establece la siguiente definición.

Definición 3.1.1.

Si $X \neq \emptyset$ es un conjunto, una **operación binaria sobre** X es simplemente una función de $X \times X$ en X •

Observación 3.1.2.

Si $\circ$ es una operación binaria sobre el conjunto $X \neq \emptyset$, para cada $a, b \in X$ al elemento $\circ((a, b)) \in X$ se le denota escribiendo $a \circ b$, y cuando no hay peligro de confusión la notación se simplifica más y se escribe simplemente ab i,e, $\circ((a, b)) := a \circ b := ab$ •

Se distinguen los siguientes tipos de operaciones binarias:

Definición 3.1.3.

Una operación binaria $\circ$ sobre $X \neq \emptyset$ se dice que es:

- **asociativa**, si para cada $a, b, c \in X$ se verifica que $a(bc) = (ab)c$.
- **conmutativa**, si para cada $a, b \in X$ se verifica que $ab = ba$ •

Con estos conceptos en mente, lo que sigue es definir el concepto de semigrupo, que como se dijo antes, será uno de los objetos principales de estudio de este capítulo.

Definición 3.1.4.

- Un **grupoide** es un par ordenado $(X, \circ)$ donde X es un conjunto no vacío y $\circ$ es una operación binaria sobre X.
- Un **semigrupo** es un grupoide $(S, \circ)$ donde $\circ$ es una operación binaria asociativa •

Observación 3.1.5.

- Como se puede apreciar en la definición anterior, un grupoide es un par ordenado cuya primera componente es un conjunto no vacío y cuya segunda componente es una operación binaria sobre el conjunto de la primera componente. Así, de la igualdad entre parejas ordenadas se sigue que dos grupoides $(X, \circ)$ y $(X', \circ')$ serán iguales si y solo si $X = X'$ y $\circ = \circ'$.
- A X se le llama **conjunto subyacente** del grupoide $(X, \circ)$.
- En la práctica, un grupoide es denotado a través de su conjunto subyacente, así, la frase ' 'Sea X un grupoide' ' significa que hay una operación binaria sobre X, digamos $\circ$, de tal manera que $(X, \circ)$ es un grupoide.
- Un **grupoide conmutativo** es un grupoide $(X, \circ)$ en el que $\circ$ es una operación binaria conmutativa •

3.2. Elementos especiales

Si $\cdot$ denota el producto usual de números enteros, entonces $(\mathbb{Z}, \cdot)$ es un grupoide. Más aún, $(\mathbb{Z}, \cdot)$ es un semigrupo. Nuestra experiencia con este semigrupo nos indica que para cada $n \in \mathbb{Z}$, $1 \cdot n = n = n \cdot 1$ i,e, multiplicar por 1 no produce cambios. Este fenómeno motiva la siguiente definición.

Definición 3.2.1.

Sea $(X, \circ)$ un grupoide. Decimos que $e \in X$ es:

1. **neutro izquierdo (o identidad izquierda)** si para cada $x \in X$ ocurre que $e \circ x = x$.
2. **neutro derecho (o identidad derecha)** si para cada $x \in X$ ocurre que $x \circ e = x$.
3. **neutro (o identidad)** si para cada $x \in X$ ocurre que $e \circ x = x = x \circ e$ •

Proposición 3.2.2.

Sea $(X, \circ)$ un grupoide y suponga que $e \in X$ es neutro izquierdo y que $e' \in X$ es neutro derecho. Entonces $e = e'$.

Demostración. Como e es neutro izquierdo, entonces $ee' = e'$. Por otra parte, como e' es neutro derecho, entonces $ee' = e$. De ahí que $e = e'$. □

Corolario 3.2.3.

Si un grupoide tiene elemento neutro, entonces éste debe ser único.

Demostración. Directa de la Proposición 3.2.2. □

En el semigrupo $(\mathbb{Z}, \cdot)$ también ocurre que para cada $n \in \mathbb{Z}$, $n \cdot 0 = 0 = 0 \cdot n$. Esto motiva la siguiente definición.

Definición 3.2.4.

Sea $(X, \circ)$ un grupoide. Decimos que $z \in X$ es:

1. **cero izquierdo** si para cada $x \in X$ ocurre que $z \circ x = z$.
2. **cero derecho** si para cada $x \in X$ ocurre que $x \circ z = z$.
3. **elemento cero** si para cada $x \in X$ ocurre que $z \circ x = z = x \circ z$ •

Proposición 3.2.5.

Sea $(X, \circ)$ un grupoide y suponga que $z \in X$ es cero izquierdo y que $z' \in X$ es cero derecho. Entonces $z = z'$.

Demostración. Como z es cero izquierdo, entonces $zz' = z$. Por otra parte, como z' es cero derecho, entonces $zz' = z'$. De ahí que $z = z'$. □

Corolario 3.2.6.

Si un grupoide tiene elemento cero, entonces éste debe ser único.

Demostración. Directa de la Proposición 3.2.5. □

Definición 3.2.7.

Un **monoide** es un semigrupo $(M, \circ)$ que tiene elemento neutro •

La siguiente proposición no será utilizada posteriormente, sin embargo, su contenido resulta interesante.

Proposición 3.2.8.

Sean $(X, \circ)$ y $(X, \circ')$ grupoides con elementos neutros $e \in X$ y $e' \in X$ respectivamente. Suponga además, que para cada $a, b, c, d \in X$

$$(a \circ b) \circ' (c \circ d) = (a \circ' c) \circ (b \circ' d).$$

Entonces $\circ = \circ'$ y $(X, \circ)$ es un monoide conmutativo.

Demostración. Se empieza exhibiendo que $e = e'$:

$$\begin{aligned} e' &= e' \circ' e' \\ &= (e \circ e') \circ' (e' \circ e) \\ &= (e \circ' e') \circ (e' \circ' e) \\ &= e \circ e \\ &= e \end{aligned}$$

Ahora bien, para cada $a, b \in X$:

$$\begin{aligned} a \circ' b &= (a \circ e) \circ' (e \circ b) \\ &= (a \circ' e) \circ (e \circ' b) \\ &= (a \circ' e') \circ (e' \circ' b) \\ &= a \circ b \end{aligned}$$

De ahí que $\circ = \circ'$. Más aún:

$$\begin{aligned} a \circ b &= (e \circ a) \circ (b \circ e) \\ &= (e \circ b) \circ (a \circ e) \\ &= b \circ a \end{aligned}$$

Así, $\circ$ es una operación binaria conmutativa. Finalmente, observe que para cada $a, b, c \in X$:

$$\begin{aligned} a \circ (b \circ c) &= (a \circ e) \circ (b \circ c) \\ &= (a \circ b) \circ (e \circ c) \\ &= (a \circ b) \circ c \end{aligned}$$

Se concluye que $\circ$ es una operación binaria asociativa. Por consiguiente $(X, \circ)$ es un monoide conmutativo.

□

Cuando un grupoide tiene elemento neutro, tiene sentido preguntarse por aquellos elementos que tienen un *inverso* con respecto del neutro. Más precisamente, se tiene el siguiente par de definiciones:

Definición 3.2.9.

Sea $(X, \circ)$ un grupoide con elemento identidad $e \in X$ y sean $x, t \in X$. Se dice que t es :

1. **inverso izquierdo de** x, si $tx = e$.
2. **inverso derecho de** x, si $xt = e$.

3. **inverso de** x , si $tx = e = xt$ •

Definición 3.2.10.

Sea $(X, \circ)$ un grupoide con elemento identidad $e \in X$. Se dice que $x \in X$ es:

1. **invertible por la izquierda**, si x tiene al menos un inverso izquierdo.
2. **invertible por la derecha**, si x tiene al menos un inverso derecho.
3. **invertible** , si x tiene al menos un inverso •

El Corolario 3.2.3 indica que en caso de que un grupoide tenga elemento neutro entonces este es único i,e, se garantiza la unicidad del neutro. Ahora bien, en caso de que un elemento de un grupoide con identidad tenga inverso ¿puede garantizarse la unicidad de éste?

Ejemplo 3.2.11.

Considerar el conjunto de tres elementos $X = \{e, a, b\}$ y considerar también a la operación binaria $\circ$ definida a través de la siguiente tabla:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	e

De la tabla se aprecia que e es neutro del grupoide $(X, \circ)$. Más aún, también se tiene que $a \circ b = e = b \circ a$ y $b \circ b = e$. De ahí que a y b son ambos inversos de b i,e, b tiene más de un inverso. Observe que $\circ$ no es una operación binaria asociativa, pues $(a \circ a) \circ b = b \circ b = e$ mientras que $a \circ (a \circ b) = a \circ e = a$ •

¿Bajo qué condiciones si puede garantizarse la unicidad de un inverso?

Proposición 3.2.12.

Sea $(X, \circ)$ un grupoide con elemento neutro $e \in X$. Suponga que $\circ$ es una operación binaria asociativa. Entonces todo elemento de X tiene a lo más un inverso.

Demostración. Suponga que $u, v \in X$ son ambos inversos de $x \in X$. Entonces $u = ue = u(xv) = (ux)v = ev = v$. □

Observación 3.2.13.

Si M es un monoide y $a \in M$ es invertible, entonces se denota a su inverso por a^{-1} •

La siguiente estructura algebraica es de suma importancia para las matemáticas, física, química y otras ciencias.

Definición 3.2.14.

Un **grupo** es un monoide $(G, \circ)$ en el que cada elemento es invertible •

Proposición 3.2.15.

Sea $(G, \circ)$ un semigrupo y sea $e \in G$ un neutro izquierdo. Suponga que para cada $g \in G$ existe $x_g \in G$ tal que $x_g g = e$. Entonces $(G, \circ)$ es un grupo.

Demostración. Veamos que para cada $g, x, y \in G$, $gx = gy \Longrightarrow x = y$:

$$\begin{aligned} gx = gy &\Longrightarrow x_g(gx) = x_g(gy) \\ &\Longrightarrow (x_g g)x = (x_g g)y \\ &\Longrightarrow ex = ey \\ &\Longrightarrow x = y. \end{aligned}$$

Si $g \in G$ es arbitrario, entonces ocurre que $x_g(ge) = (x_g g)e = ee = e = x_g g$. Por lo tanto $x_g(ge) = x_g g$ y en consecuencia $ge = g$. De ahí que e es también neutro derecho y por consiguiente elemento neutro. De lo anterior se sigue que $(G, \circ)$ es un monoide con elemento neutro e. De nuevo, si $g \in G$ es arbitrario, entonces se tiene que $x_g(gx_g) = (x_g g)x_g = ex_g = x_g = x_g e$. Por lo tanto $x_g(gx_g) = x_g e$ y por consiguiente $gx_g = e$. Esto último aunado a que $x_g g = e$ permite concluir que x_g es un inverso para g. Por lo tanto todo elemento de $(G, \circ)$ es invertible y por consiguiente $(G, \circ)$ es un grupo. □

Observación 3.2.16.

Grupo $\Longrightarrow$ Monoide $\Longrightarrow$ Semigrupo $\Longrightarrow$ Grupoide. Sin embargo, las flechas no pueden revertirse (ver Ejemplos 3.4) •

3.3. Potencias de un elemento

Definición 3.3.1.

Sea $(S, \circ)$ un semigrupo y $a \in S$. Para cada $n \in \mathbb{N}$ se define

$$a^n := \begin{cases} a & si \quad n = 1. \\ a^{n-1}a & si \quad n > 1. \end{cases}$$

Y si además $(S, \circ)$ es un monoide con neutro $e \in S$, entonces $a^0 := e$ •

Proposición 3.3.2.

Sea $(S, \circ)$ un semigrupo y $a \in S$. Para cada $n, m \in \mathbb{N}$ se cumple lo siguiente:

1. $a^n a^m = a^{n+m}$.

2. $a^n a^m = a^m a^n$. (Cualesquiera dos potencias de a conmutan)

3. $(a^n)^m = a^{nm}$.

Demostración. 1) Sea $n \in \mathbb{N}$ arbitrario pero fijo. Se procederá usando inducción sobre $m \in \mathbb{N}$: para $m = 1$ se tiene que $a^{n+1} := a^n a = a^n a^1$, luego la afirmación es válida para $m = 1$. Suponga ahora que para $m > 1$ se verifica que $a^n a^m = a^{n+m}$. Entonces $a^{n+(m+1)} := a^{n+m} a = (a^n a^m)a = a^n(a^m a) = a^n a^{m+1}$. Así, la afirmación es cierta para $m + 1$. Por consiguiente para cada $m \in \mathbb{N}$ se tiene que $a^n a^m = a^{n+m}$.
2) $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$.
3) Se sigue usando inducción y 1). □

3.4. Algunos ejemplos

A continuación se muestran los primeros ejemplos de grupoides, semigrupos, monoides y grupos.

Ejemplo 3.4.1.

El Ejemplo 3.2.11 muestra un grupoide no asociativo •

Ejemplo 3.4.2.

Sea $X \neq \emptyset$. Para cada $a, b \in X$ defínase $ab := a$. Entonces, para $a, b, c \in X$ se tiene que $a(bc) = a = ab = (ab)c$. Luego, X es un semigrupo con respecto a esta operación binaria. Observe que todo elemento de este semigrupo es un cero izquierdo y un neutro derecho. Además, si X tiene al menos dos elementos, entonces X no puede ser un monoide, pues si fuese un monoide con neutro e, tómese un $x \neq e$, de manera que como e es neutro, entonces $ex = x$ y también $ex = e$ i,e, $x = e$, lo cuál es una contradicción. Así, cuando X tiene al menos dos elementos esta construcción proporciona un ejemplo de un semigrupo que no es un monoide •

Ejemplo 3.4.3.

Sea $X \neq \emptyset$. De la Observación 1.1.9 y de la Proposición 1.1.10 se sigue que $(\mathcal{B}(X), \circ)$ es un monoide con neutro Δ_X (ver Observación 1.1.2) •

Ejemplo 3.4.4.

Sea $X \neq \emptyset$. Defínase $\mathcal{T}_X := X^X$. De las Proposiciones 1.4.5, 1.1.10 y 1.4.6 se sigue que $(\mathcal{T}_X, \circ)$ es un monoide con neutro id_X. En el caso cuando $X = \mathbb{N}$, la función $f : \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(n) := 2n$ es inyectiva pero no sobreyectiva, luego, f no puede tener un inverso derecho con respecto de $\circ$. Por consiguiente $(\mathcal{T}_{\mathbb{N}}, \circ)$ es un monoide que no es un grupo •

Ejemplo 3.4.5.

Sea $X \neq \emptyset$. Defínase $\mathcal{S}_X := \{f : X \longrightarrow X \mid f \text{ es biyectiva.}\}$. De las Proposiciones 1.4.5, 1.1.10, 1.4.6 y el Corolario 1.4.20 se sigue que $(\mathcal{S}_X, \circ)$ es un monoide con neutro id_X. Más aún, de la Definición 1.4.17 (ver también Definición 1.4.15) se deduce que $(\mathcal{S}_X, \circ)$ es un grupo •

Ejemplos más generales que los dos últimos son los siguientes:

Ejemplo 3.4.6.

Sea $\mathcal{A}$ una categoría y $X \in Ob(\mathcal{A})$. Entonces $(Hom(X, X), \circ)$ es un monoide con neutro id_X. Más aún, si $Isom(X) := \{f \in Hom(X, X) \mid f \text{ es isomorfismo}\}$, entonces de las Proposiciones 2.2.4 y 2.2.7 se sigue que $(Isom(X), \circ)$ es un grupo •

Ejemplo 3.4.7.

Sea S un semigrupo y $X \neq \emptyset$ un conjunto. Si $f, g \in S^X$, se define $fg : X \longrightarrow S$ mediante la regla $(fg)(x) := f(x)g(x)$. Si $f, g, h \in S^X$, entonces para cada $x \in X$ se tiene lo siguiente:

$$\begin{aligned}(f(gh))(x) :&= f(x)(gh)(x)\\ &= f(x)(g(x)h(x))\\ &= (f(x)g(x))h(x)\\ &= (fg)(x)h(x)\\ &= ((fg)h)(x)\end{aligned}$$

De ahí que $f(gh) = (fg)h$ y por consiguiente S^X es un semigrupo con esta operación binaria. Más aún, si S es un monoide con neutro e, entonces S^X es un monoide con neutro la función $E : X \longrightarrow S$ definida por $E(x) := e$ •

Ejemplo 3.4.8.

Sea S un semigrupo. Sobre el conjunto S se define la siguiente operación binaria: para cada $x, y \in S$, $x * y := yx$. Entonces $x*(y*z) = x*(zy) = (zy)x = z(yx) = (yx)*z = (x*y)*z$. Por lo tanto $(S, *)$ es un semigrupo llamado **semigrupo opuesto** de S, el cuál es denotado por S^{op} •

Observar que los primeros ejemplos muestran una manera de obtener semigrupos y monoides a partir de un conjunto $X \neq \emptyset$ dado. Los últimos, muestran una forma de obtener nuevos semigrupos a partir de los que ya se tienen.

3.5. Subestructuras

Un semigrupo (monoide) puede contener subconjuntos que a su vez sean también semigrupos (monoides) con respecto de la misma operación binaria. A tales subconjuntos se les da un nombre especial.

Definición 3.5.1.

Sean S un semigrupo y $\emptyset \neq H \subseteq S$. Se dice que H es un **subsemigrupo** de S si para cada $a, b \in H$ se verifica que $ab \in H$ •

Observación 3.5.2.

- Cualquier semigrupo es subsemigrupo de sí mismo.
- Si M es un monoide con neutro e, entonces $\{e\}$ es un subsemigrupo de M.
- Si S es un semigrupo con elemento cero 0_S, entonces $\{0_S\}$ es un subsemigrupo de S •

Proposición 3.5.3.

Sea S un semigrupo y $\mathcal{F} \neq \emptyset$ una familia de subsemigrupos de S. Si $\bigcap \mathcal{F} \neq \emptyset$, entonces $\bigcap \mathcal{F}$ es un subsemigrupo de S.

Demostración. Tómense $a, b \in \bigcap \mathcal{F}$ y sea $H \in \mathcal{F}$ arbitrario. Entonces $a, b \in H$, y como H es subsemigrupo, entonces $ab \in H$. Por tanto $ab \in H$ para cada $H \in \mathcal{F}$. De ahí que $ab \in \bigcap \mathcal{F}$ y por consiguiente $\bigcap \mathcal{F}$ es un subsemigrupo de S. □

Observación 3.5.4.

La intersección de una familia de subsemigrupos puede ser vacía según lo siguiente: Considerar el semigrupo $(\mathbb{N}, +)$. Para cada $n \in \mathbb{N}$ considerar el conjunto $n\mathbb{N} := \{kn | k \in \mathbb{N}\}$. Se tiene que $n\mathbb{N}$ es subsemigrupo de $\mathbb{N}$, pues si $nj, nk \in n\mathbb{N}$, entonces $nj+nk = n(j+k) \in n\mathbb{N}$. **Afirmación:** $\bigcap_{n\in\mathbb{N}} n\mathbb{N} = \emptyset$. En efecto, suponga que $x \in \bigcap_{n\in\mathbb{N}} n\mathbb{N}$ y sea m un entero positivo que no divide a x. Como $x \in \bigcap_{n\in\mathbb{N}} n\mathbb{N}$, se tiene que en particular $x \in m\mathbb{N}$. De ahí que $x = mk$ para algún $k \in \mathbb{N}$ i,e, m divide a x, lo cuál es una contradicción. Por consiguiente $\bigcap_{n\in\mathbb{N}} n\mathbb{N} = \emptyset$ •

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Considérese a la siguiente familia de subsemigrupos de S:

$$\mathcal{F}_X := \{H \subseteq S \mid H \text{ es subsemigrupo de } S \text{ y } X \subseteq H\}$$

Observe que $\mathcal{F}_X \neq \emptyset$, pues $S \in \mathcal{F}_X$. Más aún, como $X \subseteq \bigcap \mathcal{F}_X$ y $\emptyset \neq X$ se sigue que $\bigcap \mathcal{F}_X \neq \emptyset$. Así, de la Proposición 3.5.3 se deduce que $\bigcap \mathcal{F}_X$ es un subsemigrupo de S. Note que si H es un subsemigrupo de S tal que $X \subseteq S$, entonces $H \in \mathcal{F}_X$ y por lo tanto $\bigcap \mathcal{F}_X \subseteq H$. Así, $\bigcap \mathcal{F}_X$ es el más pequeño subsemigrupo de S que contiene a X.

Definición 3.5.5.

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Al subsemigrupo $\langle X \rangle := \bigcap \mathcal{F}_X$ se le llama **subsemigrupo de S generado por X** •

Si S es un semigrupo y $A, B \subseteq S$, entonces $AB := \{ab \mid a \in A \text{ y } b \in B\}$. Más generalmente, si $n \in \mathbb{N}$, entonces $A^n := \{a_1 a_2 \cdots a_n \mid a_i \in A\}$. A partir de este producto de subconjuntos puede caracterizarse al subsemigrupo $\langle X \rangle$.

Proposición 3.5.6.

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Entonces $\langle X \rangle = \bigcup_{n \in \mathbb{N}} X^n$.

Demostración. Se exhibe primero que $\bigcup_{n \in \mathbb{N}} X^n \subseteq \langle X \rangle$: si $x \in \bigcup_{n \in \mathbb{N}} X^n$, entonces puede escribirse $x = x_1 x_2 \cdots x_n$ para algunos $x_i \in X$ y $n \in \mathbb{N}$. Ahora bien, como $X \subseteq \langle X \rangle$ y $\langle X \rangle$ es subsemigrupo, se sigue entonces que $x_1 x_2 \cdots x_n \in \langle X \rangle$. Por lo tanto $\bigcup_{n \in \mathbb{N}} X^n \subseteq \langle X \rangle$. Veamos ahora que $\bigcup_{n \in \mathbb{N}} X^n$ es un subsemigrupo de S: si $x, y \in \bigcup_{n \in \mathbb{N}} X^n$, entonces puede escribirse $x = x_1 x_2 \cdots x_n$ y $y = y_1 y_2 \cdots y_m$ para algunos $x_i, y_j \in X$ y $n, m \in \mathbb{N}$. Así, $xy = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m \in X^{n+m} \subseteq \bigcup_{n \in \mathbb{N}} X^n$. Por consiguiente $\bigcup_{n \in \mathbb{N}} X^n$ es un subsemigrupo de S. Por otra parte, es claro que $X \subseteq \bigcup_{n \in \mathbb{N}} X^n$, luego $\langle X \rangle \subseteq \bigcup_{n \in \mathbb{N}} X^n$. Se concluye así que $\langle X \rangle = \bigcup_{n \in \mathbb{N}} X^n$. □

Para el caso de los monoides, un submonoide será un subsemigrupo que contenga al elemento neutro. Más precisamente:

Definición 3.5.7.

Sea M un monoide con neutro e y $H \subseteq M$. Se dice que H es un **submonoide** de M si H es un subsemigrupo de M y además $e \in H$ •

Proposición 3.5.8.

Sea M un monoide con neutro e y $\mathcal{F} \neq \emptyset$ una familia de submonoides de M. Entonces $\bigcap \mathcal{F}$ es un submonoide de M.

Demostración. Se sigue de la Proposición 3.5.3 y notando que cada elemento de $\mathcal{F}$ contiene a e.

□

Observación 3.5.9.

Sea M un monoide con neutro e_M y H un subsemigrupo de M tal que existe $e_H \in H$ de manera que para cada $h \in H$ se verifica que $e_H h = h = h e_H$. Entonces no necesariamente $e_M = e_H$. En efecto, considere el conjunto de dos elementos $\{a, b\}$ y sobre él considere la operación binaria definida como en el Ejemplo 3.4.2. Como este conjunto tiene al menos dos elementos, entonces $\{a, b\}$ es un semigrupo que no es un monoide (ver de nuevo Ejemplo 3.4.2). Sea e un objeto que no pertenece a $\{a, b\}$. Se define $ea = a = ae$, $eb = b = be$ y $e^2 = e$. Entonces no es difícil ver que $M := \{e, a, b\}$ es un monoide con neutro e cuya tabla de productos es la siguiente:

$\circ$	e	a	b
e	e	a	b
a	a	a	a
b	b	b	b

Observar que lo que se ha hecho es añadirle un neutro al semigrupo $\{a, b\}$. (Más adelante se revisa con detalle esta construcción) Ahora bien, como $a^2 = a$, entonces $\{a\}$ es un subsemigrupo de M tal que $ah = h = ha$ para todo $h \in \{a\}$, y a pesar de ello $a \neq e$ •

3.6. Congruencias y semigrupos cociente

A continuación, se revisan los resultados que permiten construir un grupo cociente. Lo primero que hay que considerar es que todo subgrupo de un grupo genera una relación de equivalencia. Más precisamente se tiene el siguiente resultado.

Proposición 3.6.1.

Sea G un grupo y H un subgrupo de G. Entonces $\rho_H := \{(a, b) \in G \times G \mid ab^{-1} \in H\}$ es una equivalencia sobre G. Más aún, $[a]_{\rho_H} = Ha$.

Demostración. Denotemos por e al neutro de G y sea $a \in G$ arbitrario. Como $aa^{-1} = e$ y $e \in H$, se sigue entonces que $aa^{-1} \in H$. Por lo tanto $(a, a) \in \rho_H$ y por consiguiente ρ_H es reflexiva. Suponga ahora que $a, b \in G$ son tales que $(a, b) \in \rho_H$, entonces $ab^{-1} \in H$, de donde $(ab^{-1})^{-1} \in H$, pero $(ab^{-1})^{-1} = ba^{-1}$. Por tanto $ba^{-1} \in H$ y así $(b, a) \in \rho_H$, de donde se sigue que ρ_H es simétrica. Ahora, suponga que $a, b, c \in G$ son tales que $(a, b) \in \rho_H$ y $(b, c) \in \rho_H$. Entonces $ab^{-1} \in H$ y $bc^{-1} \in H$. De ahí que $ab^{-1}bc^{-1} \in H$, o lo que es lo mismo, $ac^{-1} \in H$. En consecuencia $(a, c) \in H$ y ρ_H es transitiva. Concluimos así que ρ_H es una relación de equivalencia sobre G. Finalmente, observe que

$$\begin{aligned}
[a]_{\rho_H} :&= \{b \in G \mid ba^{-1} \in H\} \\
&= \{b \in G \mid ba^{-1} = h \quad \text{para algún} \quad h \in H\} \\
&= \{b \in G \mid b = ha \quad \text{para algún} \quad h \in H\} \\
&= Ha
\end{aligned}$$

□

Definición 3.6.2.

Si G es un grupo y H es un subgrupo de G, entonce $\frac{G}{H} := \frac{G}{\rho_H}$ •

Dentro de todos los subgrupos de un grupo dado, hay un tipo de ellos que son de particular interés. Estos son los subgrupos normales. La definición es la siguiente:

Definición 3.6.3.

Sea G un grupo y N un subgrupo de G. Se dice que N es un **subgrupo normal** de G si para cada $g \in G$ y para cada $n \in N$ se verifica que $gng^{-1} \in N$.
Se escribe $N \triangleleft G$ para indicar que N es un subgrupo normal del grupo G •

La equivalencia ρ_N tiene las siguientes propiedades cuando N es un subgrupo normal.

Proposición 3.6.4.

Sea G un grupo y $N \triangleleft G$. Entonces se verifica lo siguiente:

1. Para todo $c \in G$, $a\rho_N b \Longrightarrow ca\rho_N cb$.
2. Para todo $c \in G$, $a\rho_N b \Longrightarrow ac\rho_N bc$.
3. $a\rho_N b \quad$ y $\quad c\rho_N d \Longrightarrow ac\rho_N bd$.

Demostración. 1) Sea $c \in G$. Si $a\rho_N b$ entonces $ab^{-1} \in N$. Así, de que $N \triangleleft G$ se sigue que $cab^{-1}c^{-1} \in N$, o lo que es lo mismo $ca(cb)^{-1} \in N$. Por lo tanto $ca\rho_N cb$.
2) Si $a\rho_N b$, entonces $ab^{-1} \in N$, pero $ab^{-1} = acc^{-1}b^{-1} = ac(bc)^{-1}$, luego $ac(bc)^{-1} \in N$ y por consiguiente $ac\rho_N bc$.
3) Si $a\rho_N b$ y $c\rho_N d$ entonces de 1) y 2) se sigue que $ac\rho_N bc$ y $bc\rho_N bd$. Finalmente, de la transitividad de ρ_N se concluye que $ac\rho_N bd$. □

Podemos usar ahora estas propiedades para construir al grupo cociente.

Proposición 3.6.5.

Sea G un grupo y $N \triangleleft G$. Considerar al conjunto cociente $\frac{G}{N} := \{Ng \mid g \in G\}$ y también la siguiente operación entre clases laterales derechas:

$$Na \cdot Nb := Nab$$

Se tiene entonces que dicha operación está bien definida y $\frac{G}{N}$ es un grupo bajo este producto de clases laterales.

Demostración. Solo se probará que este producto de clases laterales es una operación bien definida:

$$\begin{aligned} Na = Nx \quad \text{y} \quad Nb = Ny &\Longrightarrow a\rho_N x \quad \text{y} \quad b\rho_N y \\ &\Longrightarrow ab\rho_N xy \\ &\Longrightarrow Nab = Nxy \\ &\Longrightarrow Na \cdot Nb = Nx \cdot Ny \end{aligned}$$

□

Definición 3.6.6.

Al grupo $\frac{G}{N}$ se le llama **grupo cociente o grupo factor** de G sobre N •

En resumen, un grupo cociente se construye a partir de la equivalencia ρ_N generada por un subgrupo normal. Observar que ρ_N está definida en términos de elementos inversos, lo cuál se puede hacer, ya que en un grupo todo elemento de éste es invertible. Ahora bien, como no todo semigrupo (monoide) es un grupo, para construir un *semigrupo (monoide) cociente* no podremos imitar tal cuál la construcción hecha para los grupos. Sin embargo, observe que la demostración de la Proposición 3.6.5 sólo depende de las propiedades de ρ_N dadas en la Proposición 3.6.4. Así, con base en esto se tiene la siguiente definición:

Definición 3.6.7.

Sea S un semigrupo y sea ρ una equivalencia sobre S. Decimos que ρ es una

- **congruencia izquierda**, si para cada $c \in S$ se verifica lo siguiente:

$$a\rho b \Longrightarrow ca\rho cb.$$

- **congruencia derecha**, si para cada $c \in S$ se verifica lo siguiente:

$$a\rho b \Longrightarrow ac\rho bc.$$

- **congruencia**, si ρ es a la vez una congruencia izquierda y una congruencia derecha •

Proposición 3.6.8.

Sea S un semigrupo y sea ρ una equivalencia sobre S. Entonces ρ es una congruencia si y solo si $a\rho b \quad \text{y} \quad c\rho d \Longrightarrow ac\rho bd$.

Demostración. $\Longrightarrow$) Suponga que ρ es una congruencia y que $a\rho b$ y $c\rho d$. Entonces $ac\rho bc$ y $bc\rho bd$. Luego, de la transitividad de ρ se sigue lo pedido.
$\Longleftarrow$) Sea $c \in S$ y suponga que $a\rho b$. Como $c\rho c$, de la hipótesis se sigue que $ca\rho cb$ y $ac\rho bc$. Así, ρ es a la vez una congruencia izquierda y derecha. □

Observación 3.6.9.

Si G es un grupo y $N \triangleleft G$, entonces según la Proposición 3.6.4 ρ_N es una congruencia •

Para los semigrupos, será a partir de una congruencia como se construirá un semigrupo cociente:

Proposición 3.6.10.

Sea S un semigrupo y sea ρ una congruencia sobre S. Considere el conjunto cociente $\frac{S}{\rho} := \{[a]_\rho \mid a \in S\}$ y también la siguiente operación entre clases de equivalencia:

$$[a]_\rho[b]_\rho := [ab]_\rho$$

Se tiene entonces que dicha operación está bien definida y $\frac{S}{\rho}$ es un semigrupo bajo este producto de clases de equivalencia.

Demostración. Veamos primero que este producto de clases es una operación bien definida:

$$\begin{aligned}
[a]_\rho = [x]_\rho \quad \text{y} \quad [b]_\rho = [y]_\rho &\Longrightarrow a\rho x \quad \text{y} \quad b\rho y \\
&\Longrightarrow ab\rho xy \\
&\Longrightarrow [ab]_\rho = [xy]_\rho \\
&\Longrightarrow [a]_\rho[b]_\rho = [x]_\rho[y]_\rho
\end{aligned}$$

Ahora bien, se tiene que

$$\begin{aligned}
[a]_\rho([b]_\rho[c]_\rho) &= [a]_\rho[bc]_\rho \\
&= [a(bc)]_\rho \\
&= [(ab)c]_\rho \\
&= [ab]_\rho[c]_\rho \\
&= ([a]_\rho[b]_\rho)[c]_\rho
\end{aligned}$$

Por consiguiente, $\frac{S}{\rho}$ es un semigrupo bajo este producto de clases de equivalencia. Más aún, si S es un monoide con neutro e entonces $\frac{S}{\rho}$ es un monoide con neutro $[e]_\rho$ pues, $[a]_\rho[e]_\rho = [ae]_\rho = [a]_\rho = [ea]_\rho = [e]_\rho[a]_\rho$. □

Definición 3.6.11.

Sea S un semigrupo y sea ρ una congruencia sobre S. Al semigrupo $\frac{S}{\rho}$ se le llama **semigrupo cociente o semigrupo factor** de S sobre ρ •

3.7. Morfismos de semigrupos

Un morfismo de semigrupos será una función entre dos semigrupos que respete la estructura de estos.

Definición 3.7.1.

- Sean S y T semigrupos. Un **morfismo de semigrupos** de S en T es una función $f : S \longrightarrow T$ tal que para cada $x, y \in S$, $f(xy) = f(x)f(y)$.
- Si S y T son monoides con neutros e_S y e_T respectivamente, una función $f : S \longrightarrow T$ es un **morfismo de monoides** si f es un morfismo de semigrupos y $f(e_S) = e_T$ •

Observación 3.7.2.

Sea $M_2(\mathbb{Z})$ el conjunto de todas las matrices de tamaño 2×2 con entradas enteras. Entonces $M_2(\mathbb{Z})$ es un monoide con respecto del producto usual de matrices. Además, el neutro de este monoide es la matriz $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Considerar también al monoide $(\mathbb{N}, \cdot)$ donde $\cdot$ denota el producto usual de enteros. Sea $f : \mathbb{N} \longrightarrow M_2(\mathbb{Z})$ definida por $f(n) := \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$. Entonces

$$f(n)f(m) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix} = f(nm)$$

Por consiguiente f es un morfismo de semigrupos. Sin embargo, observe que $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ i,e, f no manda el neutro en el neutro •

Proposición 3.7.3.

Sean M y N monoides con neutros e_M y e_N respectivamente, y sea $f : M \longrightarrow N$ un morfismo sobreyectivo de semigrupos. Entonces $f(e_M) = e_N$.

Demostración. Sea $n \in N$ arbitrario. Como f es sobreyectiva puede escribirse $n = f(m)$ para algún $m \in M$. Así, $nf(e_M) = f(m)f(e_M) = f(me_M) = f(m) = n$, y también $f(e_M)n = f(e_M)f(m) = f(e_Mm) = f(m) = n$. Por lo tanto $f(e_M)$ es neutro de N, de manera que del Corolario 3.2.3 se deduce que $f(e_M) = e_N$. □

La composición de morfismos de semigrupos es de nuevo un morfismo de semigrupos.

Proposición 3.7.4.

Si $f : S \longrightarrow T$ y $g : T \longrightarrow R$ son morfismos de semigrupos (monoides), entonces $g \circ f$ es un morfismo de semigrupos (monoides):

Demostración. Se tiene que $g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y))$. Además, si f y g son morfismos de monoides, entonces $g(f(e_S)) = g(e_T) = e_R$.

□

Definición 3.7.5.

Un **isomorfismo de semigrupos (monoides)** es un morfismo de semigrupos (monoides) $f : S \longrightarrow T$ para el cual existe un morfismo de semigrupos (monoides) $g : T \longrightarrow S$ tal que $g \circ f = id_S$ y $f \circ g = id_T$. Se escribe $S \cong T$ para indicar que existe un isomorfismo de semigrupos (monoides) de S en T, y en ese caso se dice que S es **isomorfo** a T •

De acuerdo con la definición anterior, un isomorfismo de semigrupos debe ser, en particular, una función biyectiva.

Proposición 3.7.6.

Sea $f : S \longrightarrow T$ un morfismo biyectivo de semigrupos y $g : T \longrightarrow S$ su función inversa. Entonces $g : T \longrightarrow S$ es un morfismo de semigrupos, y en consecuencia, f es un isomorfismo de semigrupos.

Demostración. Sean $a, b \in T$. Como f es sobreyectiva, entonces $a = f(x)$ y $b = f(y)$ para algunos $x, y \in S$. Ahora bien, como g es la inversa de f, entonces $g(a) = g(f(x)) = x$ y $g(b) = g(f(y)) = y$. Por otra parte, $g(ab) = g(f(x)f(y)) = g(f(xy)) = xy = g(a)g(b)$. Por consiguiente g es un morfismo de semigrupos.

□

Ejemplo 3.7.7.

Si $(S, \circ)$ es un semigrupo (monoide), entonces $id_S : S \longrightarrow S$ es un isomorfismo de $(S, \circ)$ en sí mismo •

Ejemplo 3.7.8.

Todo grupo es isomorfo a su grupo opuesto. En efecto, sea G un grupo y considere la función $f : G \longrightarrow G^{op}$ definida por $f(g) := g^{-1}$. Como todo elemento de G tiene un único inverso se sigue entonces que f es biyectiva. Aún más, para cada $x, y \in G$, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = f(y)f(x) = f(x) * f(y)$. De ahí que f es un isomorfismo de grupos y $G \cong G^{op}$ •

Ejemplo 3.7.9.

En contraste con el ejemplo anterior, no todo monoide es isomorfo a su opuesto (ver Ejemplo3.4.8). En efecto, considere al monoide M de la Observación 3.5.9 cuya tabla de productos es la siguiente

$\circ$	e	a	b
e	e	a	b
a	a	a	a
b	b	b	b

Sea $f : M \longrightarrow M$ una función biyectiva tal que $f(e) = e$. Entonces se tienen los siguientes casos:

1. $f(a) = a$ y $f(b) = b$
2. $f(a) = b$ y $f(b) = a$

En el primer caso $f = id_M$ y así $id_M(ab) = id_M(a) = a$, mientras que $id_M(a) * id_M(b) = a * b = ba = b$. De ahí que id_M no es un isomorfismo de M en M^{op}. En el segundo caso, $f(ab) = f(a) = b$, mientras que $f(a) * f(b) = b * a = ab = a$. Por lo tanto f no es un isomorfismo de M en M^{op}. Se concluye que no hay isomorfismos de monoides de M en M^{op} •

Todo morfismo de semigrupos induce una congruencia sobre su dominio.

Proposición 3.7.10.

Sea $f : S \longrightarrow T$ un morfismo de semigrupos (monoides). Entonces

- $Im(f) = f(S)$ es un subsemigrupo (submonoide) de T.
- $Ker(f)$ es una congruencia sobre S.

Demostración. Sean $x, y \in Im(f)$. Luego $x = f(a)$ y $y = f(b)$ para algunos $a, b \in S$. Así, $xy = f(a)f(b) = f(ab) \in Im(f)$, y por consiguiente $Im(f)$ es subsemigrupo de T. Si S y T son monoides con neutros e_S y e_T respectivamente y f es un morfismo de monoides, entonces $e_T = f(e_S) \in Im(f)$ y por lo tanto $Im(f)$ es un submonoide de T. Ahora bien, de la Proposición 1.4.32 se sigue que $Ker(f)$ es una equivalencia sobre S. Además, si $aKer(f)b$ y $cKer(f)d$, entonces $f(a) = f(b)$ y $f(c) = f(d)$, de donde $f(a)f(c) = f(b)f(d)$ y por tanto $f(ac) = f(bd)$. Así, $acKer(f)bd$ y por consiguiente $Ker(f)$ es una congruencia sobre S. □

Observación 3.7.11.

- Sea ρ una congruencia sobre el semigrupo S. Entonces la proyección canónica $\pi_\rho : S \longrightarrow \frac{S}{\rho}$ (ver Definición 1.4.33) es un morfismo de semigrupos, pues $\pi_\rho(ab) = [ab]_\rho = [a]_\rho[b]_\rho = \pi_\rho(a)\pi_\rho(b)$. Además

$$\begin{aligned} Ker(\pi_\rho) &:= \{(a, b) \in S \times S \mid \pi_\rho(a) = \pi_\rho(b)\} \\ &= \{(a, b) \in S \times S \mid [a]_\rho = [b]_\rho\} \\ &= \{(a, b) \in S \times S \mid a\rho b\} \\ &= \rho \quad \bullet \end{aligned}$$

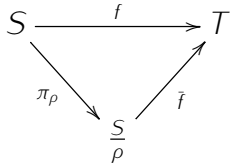
- Sea $f : G \longrightarrow H$ un morfismo de grupos y $Nu(f) := \{g \in G \mid f(g) = e_H\}$. Entonces $Nu(f) \triangleleft G$ y

$$\begin{aligned} \rho_{Nu(f)} &:= \{(a, b) \in G \times G \mid ab^{-1} \in Nu(f)\} \\ &= \{(a, b) \in G \times G \mid f(ab^{-1}) = e_H\} \\ &= \{(a, b) \in G \times G \mid f(a) = f(b)\} \\ &= Ker(f) \quad \bullet \end{aligned}$$

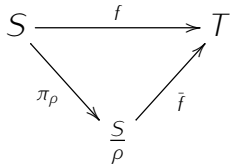
La siguiente proposición es la versión para los semigrupos del teorema de homomorfismo que existe para otras estructuras como los grupos y anillos.

Proposición 3.7.12. *De homomorfismo para semigrupos.*

Sea $f : S \longrightarrow T$ un morfismo de semigrupos y ρ una congruencia sobre S tal que $\rho \subseteq Ker(f)$. Entonces, existe un único morfismo de semigrupos $\bar{f} : \frac{S}{\rho} \longrightarrow T$ tal que el siguiente triángulo conmuta:



Demostración. De acuerdo con el Teorema 1.4.35, existe una única función $\bar{f} : \frac{S}{\rho} \longrightarrow T$ que hace al siguiente triángulo conmutativo:



Tal función está dada por $\bar{f}([a]_\rho) := f(a)$. Más aún, $\bar{f}$ es un morfismo de semigrupos, pues $\bar{f}([a]_\rho[b]_\rho) = \bar{f}([ab]_\rho) = f(ab) = f(a)f(b) = \bar{f}([a]_\rho)\bar{f}([b]_\rho)$.

□

Corolario 3.7.13.

Sea $f : S \longrightarrow T$ un morfismo de semigrupos. Entonces $\frac{S}{Ker(f)} \cong Im(f)$.

Demostración. Sea $f : S \longrightarrow T$ un morfismo de semigrupos y considere a la función $F : S \longrightarrow Im(f)$ definida por $F(x) := f(x)$. Es claro que F es una función sobreyectiva. Además, como F tiene la misma regla de correspondencia de f, se sigue entonces que F es un morfismo de semigrupos. Más aún, observe que

$$\begin{aligned} Ker(F) &= \{(a,b) \in S \times S \mid F(a) = F(b)\} \\ &= \{(a,b) \in S \times S \mid f(a) = f(b)\} \\ &= Ker(f) \end{aligned}$$

La Proposición 3.7.12 garantiza la existencia de un morfismo de semigrupos $\bar{F} : \frac{S}{Ker(F)} \longrightarrow Im(f)$ tal que $F = \bar{F} \circ \pi_{Ker(F)}$. En particular, del Teorema 1.4.35 se deduce que $\bar{F}$ es biyectiva y por lo tanto un isomorfismo de semigrupos. Por consiguiente $\frac{S}{Ker(f)} = \frac{S}{Ker(F)} \cong Im(f)$.

□

Observación 3.7.14.

Sea S un semigrupo. No es difícil ver que Δ_S, la diagonal en S, es una congruencia sobre S. Así, $\frac{S}{\Delta_S}$ es un semigrupo. Más aún, $\frac{S}{\Delta_S} \cong S$. En efecto, considerar el morfismo de semigrupos $id_S : S \longrightarrow S$. En este caso se tiene que

$$\begin{aligned} Ker(id_S) &= \{(a,b) \in S \times S \mid id_S(a) = id_S(b)\} \\ &= \{(a,b) \in S \times S \mid a = b\} \\ &= \Delta_S \end{aligned}$$

Como id_S es sobreyectiva, del Corolario 3.7.13 se concluye que $\frac{S}{\Delta_S} \cong S$ •

No es casualidad que $Ker(id_S) = \Delta_S$. Esto es una consecuencia de lo siguiente.

Proposición 3.7.15.

Sea $f : S \longrightarrow T$ una función. Entonces f es inyectiva si y solo si $Ker(f) = \Delta_S$.

Demostración. $\Longrightarrow$) Suponga que f es inyectiva. Como $Ker(f)$ es una equivalencia, entonces $\Delta_S \subseteq Ker(f)$. Sea $(a,b) \in Ker(f)$, luego $f(a) = f(b)$, así que de la inyectividad de f se sigue que $a = b$ y por consiguiente $(a,b) \in \Delta_S$. De ahí que $Ker(f) \subseteq \Delta_S$ y por lo tanto $Ker(f) = \Delta_S$.
$\Longleftarrow$) Suponga que $Ker(f) = \Delta_S$ y sean $a, b \in S$ tales que $f(a) = f(b)$. Entonces $(a,b) \in Ker(f) = \Delta_S$, de donde $a = b$ y por consiguiente f es inyectiva.

□

Observación 3.7.16.

Sean S, T y R semigrupos. Del Corolario 1.4.20 y la Proposición 3.7.4 se sigue que si $S \cong T$ y $T \cong R$, entonces $S \cong R$ •

Proposición 3.7.17.

Si $f : S \longrightarrow T$ es un morfismo inyectivo de semigrupos, entonces $S \cong Im(f)$ i,e, S es isomorfo a un subsemigrupo de T.

Demostración. Como f es inyectiva, entonces $Ker(f) = \Delta_S$. Así, del Corolario 3.7.13 se sigue que $\frac{S}{\Delta_S} = \frac{S}{Ker(f)} \cong Im(f)$, pero $S \cong \frac{S}{\Delta_S}$, luego $S \cong Im(f)$.

□

Ejemplo 3.7.18.

Sean S un semigrupo, $X \neq \emptyset$ un conjunto , $f : S \longrightarrow X$ una función biyectiva y $g : X \longrightarrow S$ su función inversa. Para cada $x, y \in X$ se define $xy := f(g(x)g(y))$. Si $x, y, z \in X$ entonces

$$\begin{aligned} x(yz) &= xf(g(y)g(z)) \\ &= f(g(x)g(f(g(y)g(z)))) \\ &= f(g(x)(g(y)g(z))) \\ &= f((g(x)g(y))g(z)) \\ &= f(g(f(g(x)g(y)))g(z)) \\ &= f(g(x)g(y))z \\ &= (xy)z \end{aligned}$$

Por consiguiente X es un semigrupo bajo esta operación binaria. Además, si S es un monoide con neutro e y se define $\bar{e} := f(e)$, entonces

$$\begin{aligned} x\bar{e} &= xf(e) \\ &= f(g(x)g(f(e))) \\ &= f(g(x)e) \\ &= f(g(x)) \\ &= x \end{aligned}$$

y también

$$\begin{aligned} \bar{e}x &= f(e)x \\ &= f(g(f(e))g(x)) \\ &= f(eg(x)) \\ &= f(g(x)) \\ &= x \end{aligned}$$

De manera que X es un monoide con neutro $\bar{e}$. Finalmente, observe que si $s, t \in S$

$$f(s)f(t) := f(g(f(s))g(f(t))) = f(st)$$

de donde f es un isomorfismo de semigrupos y por tanto $S \cong X$. Así, si un conjunto X es equipotente a un semigrupo (monoide), entonces a partir de una función biyectiva puede dotarse a X con estructura de semigrupo (monoide) •

3.8. El teorema de Cayley para semigrupos

El teorema de Cayley de la teoría de grupos afirma que todo grupo es isomorfo a algún subgrupo de $\mathcal{S}_X$ para algún conjunto X (ver Ejemplo 3.4.5). La versión para monoides involucra al monoide $\mathcal{T}_X$ (ver Ejemplo 3.4.4) y es la siguiente.

Proposición 3.8.1.

Todo monoide es isomorfo a algún submonoide de $\mathcal{T}_X$ para algún conjunto X.

Demostración. Sea M un monoide con neutro e. Para cada $m \in M$ considere a la función $f_m : M \longrightarrow M$ definida por $f_m(x) := mx$. Observe que

$$\begin{aligned} f_{mn}(x) &= (mn)x \\ &= m(nx) \\ &= f_m(nx) \\ &= f_m(f_n(x)) \end{aligned}$$

Así, para cada $m, n \in M$ se tiene que $f_{mn} = f_m \circ f_n$. Ahora bien, para $m = e$, $f_e(x) := ex = x$, i,e, $f_e = id_M$. Más aún, si $f_m = f_n$, entonces $f_m(e) = f_n(e)$ y por tanto $me = ne$, de donde $m = n$. Por consiguiente $f_m = f_n \Longrightarrow m = n$. Todo lo anterior permite concluir que la función $\phi : M \longrightarrow \mathcal{T}_M$ definida por $\phi(m) := f_m$ es un morfismo inyectivo de monoides. Por consiguiente, de la Proposición 3.7.17 se concluye que $M \cong Im(\phi)$.

□

Observación 3.8.2.

Observe que para mostrar la implicación $f_m = f_n \Longrightarrow m = n$ fue necesaria la existencia del neutro e. Así que como no todo semigrupo es un monoide, entonces la prueba de la Proposición 3.8.1 puede no ser válida para un semigrupo que carece de neutro. Sin embargo, puede llevarse a cabo lo siguiente: Sea S un semigrupo y sea e un objeto tal que $e \notin S$. Entonces, conservando para los elementos de S la misma operación que hay en S y definiendo para cada $x \in S$, $ex := x$, $xe := x$ y $e^2 := e$, se sigue que $S \cup \{e\}$ es un monoide con neutro e. Observar que lo que se ha hecho es añadirle un elemento e al semigrupo S y después extender la operación binaria que tiene S de tal forma que $S \cup \{e\}$ sea un monoide con neutro e. De momento, denótese a este semigrupo por $S(e)$ •

Proposición 3.8.3.

Sea S un semigrupo y a, b objetos tales que $a, b \notin S$. Entonces $S(a) \cong S(b)$.

Demostración. Se sigue de observar que la función $f : S(a) \longrightarrow S(b)$ definida por

$$f(x) := \begin{cases} x & si \quad x \in S. \\ b & si \quad x = a. \end{cases}$$

es un isomorfismo de monoides. □

De acuerdo con esto, puede hacerce la siguiente definición.

Definición 3.8.4.

Sean S un semigrupo y a un objeto tal que $a \notin S$. Se define $S^1 := S(a)$, donde $S(a) := S \cup \{a\}$ es el monoide definido en la Observación 3.8.2 •

Observe que S es siempre un subsemigrupo de S^1. Ahora, con ayuda del monoide S^1 puede establecerse lo siguiente.

Teorema. 3.8.5. *De Cayley para semigrupos.*

Todo semigrupo es isomorfo a algún subsemigrupo de $\mathcal{T}_X$ para algún conjunto X.

Demostración. Sea S un semigrupo. De acuerdo a la Proposición 3.8.1, existe un conjunto X y un submonoide de $\mathcal{T}_X$, digamos T, tal que $S^1 \cong T$. Sea $\phi : S^1 \longrightarrow T$ un isomorfismo de monoides y considere la función $\psi : S \longrightarrow T$ definida por $\psi(x) := \phi(x)$. Es fácil ver que ψ es un morfismo inyectivo de semigrupos. Así, $S \cong Im(\psi)$. Ahora bien, observe que $Im(\psi)$ es un subsemigrupo de T y a su vez T es un subsemigrupo de $\mathcal{T}_X$, por consiguiente $Im(\psi)$ es un subsemigrupo de $\mathcal{T}_X$ y el resultado se sigue.

□

3.9. Ideales

El concepto de ideal es bien conocido en teoría de anillos. Recordar que a partir de un ideal es posible construir un nuevo anillo, más precisamente un anillo cociente. Para el caso de los semigrupos también existe el concepto de ideal y parecido al caso de los anillos, un ideal permitirá construir un semigrupo cociente.

Definición 3.9.1.

Sea S un semigrupo e $\emptyset \neq I \subseteq S$. Se dice que I es un

1. **ideal izquierdo** de S si $SI \subseteq I$, o lo que es lo mismo, si para cada $x \in S$ y cada $a \in I$ ocurre que $xa \in I$.

2. **ideal derecho** de S si $IS \subseteq I$, o lo que es lo mismo, si para cada $x \in S$ y cada $a \in I$ ocurre que $ax \in I$.

3. **ideal bilátero (o simplemente ideal)** de S, si I es un ideal izquierdo y un ideal derecho •

Observación 3.9.2.

- Todo ideal izquierdo, derecho o bilátero es también un subsemigrupo.

- Por el contrario, no todo subsemigrupo es un ideal. Por ejemplo, para el semigrupo $(\mathbb{N}, +)$ se tiene que $2\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$ es un subsemigrupo pero no un ideal, pues la suma de un número natural impar con un natural par da como resultado un número impar.
- Cualquier semigrupo es un ideal de sí mismo. Además, si S es un semigrupo con elemento cero 0_S, entonces $\{0_S\}$ es un ideal.
- Si M es un monoide con neutro e e I es un ideal de M tal que $e \in I$, entonces $I = M$, pues para cada $x \in S$ debe ocurrir que $x = xe \in I$.
- El único ideal de un grupo es él mismo. En efecto, sea G un grupo e I un ideal. Sea $g \in I$. Entonces $e = gg^{-1} \in I$ y por tanto $I = G$ •

Proposición 3.9.3.

Sea S un semigrupo. Si I es un ideal izquierdo (derecho) de S entonces la equivalencia de Rees ρ_I (ver Ejemplo 1.2.3) es una congruencia izquierda (derecha).

Demostración. Sea $c \in S$ y suponga que $a\rho_I b$. Si $a = b$ entonces, $ca = cb$ y $ca\rho_I cb$. Si $a, b \in I$, entonces de que I es un ideal izquierdo se sigue que $ca, cb \in I$, luego $ca\rho_I cb$. Por consiguiente ρ_I es una congruencia izquierda. La demostración para ideales derechos es análoga y se omite. □

De lo anterior, se sigue que si I es un ideal bilátero del semigrupo S, entonces ρ_I es una congruencia y por consiguiente $\frac{S}{\rho_I}$ es un semigrupo. Del Ejemplo 1.2.3 se ve que $\frac{S}{\rho_I} = \{I\} \cup \{\{x\} \mid x \in S - I\}$ y además

$$[x]_{\rho_I}[y]_{\rho_I} := [xy]_{\rho_I} = \begin{cases} I & si \quad xy \in I. \\ \{xy\} & si \quad xy \notin I. \end{cases}$$

Así, si $a \in I$ entonces para cada $[x]_{\rho_I} \in \frac{S}{\rho_I}$ se tiene que $[x]_{\rho_I} I = [x]_{\rho_I}[a]_{\rho_I} = [xa]_{\rho_I} = I$ mientras que $I[x]_{\rho_I} = [a]_{\rho_I}[x]_{\rho_I} = [ax]_{\rho_I} = I$. Por lo tanto $[x]_{\rho_I} I = I = I[x]_{\rho_I}$. Se concluye que $\frac{S}{\rho_I}$ es un semigrupo con elemento cero el ideal I. Por lo tanto, todo ideal bilátero genera un semigrupo con cero.

Observación 3.9.4.

Sea S un semigrupo. De la definición de ideal se sigue que si I es un ideal de S y R es un subsemigrupo de S tales que $I \subseteq R \subseteq S$, entonces I es ideal de R •

De la observación anterior se sigue que todo ideal de un semigrupo es también un ideal de cualquier subsemigrupo que lo contenga. Así que cuando se trabaje con la equivalencia de Rees generada por un ideal será necesario denotar sobre qué semigrupo se define esta.

Definición 3.9.5.

Sea S un semigrupo, I un ideal de S y R un subsemigrupo de S tales que $I \subseteq R \subseteq S$. Se escribe ρ_I^R para denotar a la equivalencia de Rees generada por I sobre el subsemigrupo R y se escribe $\frac{R}{I}$ para denotar al semigrupo cociente $\dfrac{R}{\rho_I^R}$ •

Proposición 3.9.6.

Sea S un semigrupo y sean I, J ideales de S tales que $I \subseteq J \subseteq S$. Entonces

$$\frac{S}{J} \cong \frac{\frac{S}{I}}{\frac{J}{I}}$$

Demostración. Considerar a la función $f : \frac{S}{I} \longrightarrow \frac{S}{J}$ definida por $f([a]_{\rho_I^S}) := [a]_{\rho_J^S}$. Tal función está bien definida pues

$$\begin{aligned} [a]_{\rho_I^S} = [b]_{\rho_I^S} &\Longrightarrow a, b \in I \quad \text{ó} \quad a = b \\ &\Longrightarrow a, b \in J \quad \text{ó} \quad a = b \\ &\Longrightarrow [a]_{\rho_J^S} = [b]_{\rho_J^S} \end{aligned}$$

Es fácil ver que f es sobreyectiva. Además, $f([a]_{\rho_I^S}[b]_{\rho_I^S}) = f([ab]_{\rho_I^S}) = [ab]_{\rho_J^S} = [a]_{\rho_J^S}[b]_{\rho_J^S} = f([a]_{\rho_I^S})f([b]_{\rho_I^S})$, de donde f es un morfismo sobreyectivo de semigrupos y por consiguiente $\frac{S}{J} \cong \frac{\frac{S}{I}}{Ker(f)}$. Ahora bien, obsérvese que

$$\begin{aligned} [a]_{\rho_I^S} \in \frac{J}{I} &\Longleftrightarrow [a]_{\rho_I^S} = I \quad \text{ó} \quad [a]_{\rho_I^S} = \{a\}, a \in J - I \\ &\Longleftrightarrow a \in I \quad \text{ó} \quad a \in J - I \\ &\Longleftrightarrow a \in J \end{aligned}$$

De esto último y de que J es un ideal de S se sigue que $\dfrac{J}{I}$ es un ideal de $\dfrac{S}{I}$. Por otra parte se tiene lo siguiente:

$$\begin{aligned} ([a]_{\rho_I^S}, [b]_{\rho_I^S}) \in Ker(f) &\Longleftrightarrow f([a]_{\rho_I^S}) = f([b]_{\rho_I^S}) \\ &\Longleftrightarrow [a]_{\rho_J^S} = [b]_{\rho_J^S} \\ &\Longleftrightarrow a, b \in J \quad \text{ó} \quad a = b \\ &\Longleftrightarrow [a]_{\rho_I^S}, [b]_{\rho_I^S} \in \frac{J}{I} \quad \text{ó} \quad [a]_{\rho_I^S} = [b]_{\rho_I^S} \\ &\Longleftrightarrow ([a]_{\rho_I^S}, [b]_{\rho_I^S}) \in \rho_{\frac{J}{I}}^{\frac{S}{I}} \end{aligned}$$

De ahí que $Ker(f) = \rho_{\frac{J}{I}}^{\frac{S}{I}}$ y el resultado se sigue.

□

La siguiente proposición muestra cómo se comportan los ideales bajo un morfismo de semigrupos.

Proposición 3.9.7.

Sean $f : S \longrightarrow T$ un morfismo de semigrupos, I un ideal de S y J un ideal de T. Entonces

1. $f(I)$ es ideal de T, si f es sobreyectiva.
2. $f^{-1}(J)$ es un ideal de S.

Demostración. 1) Sean $a \in T$ y $b \in f(I)$ arbitrarios. Entonces puede escribirse $a = f(x)$ y $b = f(y)$ para algunos $x \in S$ y $y \in I$. Así, $ab = f(x)f(y) = f(xy) \in f(I)$ y también $ba = f(y)f(x) = f(yx) \in f(I)$. Por lo tanto $f(I)$ es ideal de T.
2) Sean $x \in f^{-1}(J)$ y $y \in S$ arbitrarios. Entonces $f(x) \in J$, de manera que $f(xy) = f(x)f(y) \in J$, y del mismo modo $f(yx) = f(y)f(x) \in J$. De ahí que $xy, yx \in f^{-1}(J)$ y por consiguiente $f^{-1}(J)$ es ideal de S. □

A pesar de ser sencillo, el siguente resultado será de utilidad en lo posterior.

Proposición 3.9.8.

1. Si S es un semigrupo con cero 0_S e I es un ideal de S, entonces $0_S \in I$.
2. Sea $f : S \longrightarrow T$ un morfismo sobreyectivo de semigrupos. Si S es un semigrupo con elemento cero 0_S, entonces $f(0_S)$ es elemento cero de T. En particular, todo morfismo sobreyectivo de semigrupos con cero manda el cero en el cero.

Demostración. 1) Tómese $a \in I$. Entonces $0_S = a0_S \in I$.
2) Sea $t \in T$ arbitrario. Entonces $t = f(x)$ para algún $x \in S$. Luego, $tf(0_S) = f(x)f(0_S) = f(x0_S) = f(0_S)$ y $f(0_S)t = f(0_s)f(x) = f(0_Sx) = f(0_S)$. En consecuencia, $f(0_S)$ es elemento cero de T. □

Sea S un semigrupo e I un ideal de S. Considerar el morfismo proyección $\pi_{\rho_I^S} : S \longrightarrow \frac{S}{I}$. Entonces, de la Observación 3.7.11 se ve que $ker(\pi_{\rho_I^S}) = \rho_I^S$ i,e, el kernel de $\pi_{\rho_I^S}$ es la congruencia de Rees generada por el ideal I. A los morfismos que tengan esta propiedad se les dará un nombre especial.

Definición 3.9.9.

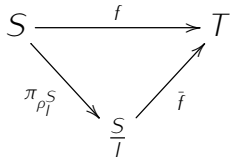
Sea $f : S \longrightarrow T$ un morfismo de semigrupos. Se dice que f es un **morfismo de Rees** si $ker(f) = \rho_I^S$ para algún ideal I de S •

De acuerdo con lo siguiente, el codominio de un morfismo sobreyectivo de Rees debe ser un semigrupo con cero.

Proposición 3.9.10.

Si $f : S \longrightarrow T$ es un morfismo sobreyectivo de Rees, entonces T es un semigrupo con cero. Más aún, si $ker(f) = \rho_I^S$ para algún ideal I y 0_T es el cero de T, entonces $f(I) = \{0_T\}$.

Demostración. De acuerdo con la Proposición 3.7.12 existe un único morfismo de semigrupos $\bar{f} : \frac{S}{I} :\longrightarrow T$ tal que el triángulo siguiente conmuta



Tal morfismo viene dado por $\bar{f}([a]_{\rho_I^S}) := f(a)$, además $\bar{f}$ debe ser biyectiva. Ahora bien, como $\frac{S}{I}$ es un semigrupo con cero el ideal I, de la Proposición 3.9.8 se sigue que $\bar{f}(I)$ es elemento cero de T. Hágase $0_T := \bar{f}(I)$. De que el triángulo de arriba conmute se sigue que para cada $a \in I$ es $f(a) = \bar{f}(\pi_{\rho_I^S}(a)) = \bar{f}([a]_{\rho_I^S}) = \bar{f}(I) = 0_T$. Por lo tanto $f(I) = \{0_T\}$. □

Con la ayuda de estos resultados se puede establecer el siguiente teorema de correspondencia.

Teorema. 3.9.11.

Sea $f : S \longrightarrow T$ un morfismo sobreyectivo de Rees con $ker(f) = \rho_I^S$ para algún ideal I. Entonces los conjuntos que a continuación se definen son equipotentes:

$$\mathbb{X} := \{J \subseteq S \mid J \text{ es ideal de } S \text{ e } I \subseteq J\} \quad \text{y} \quad \mathbb{Y} := \{K \subseteq T \mid K \text{ es ideal de } T\}$$

Demostración. De acuerdo con la Proposición 3.9.7, la imagen directa de un ideal bajo un morfismo sobreyectivo es también un ideal. Puede así considerarse a la función $F : \mathbb{X} \longrightarrow \mathbb{Y}$ definida por $F(J) := f(J)$. Ahora bien, sean $J, J' \in \mathbb{X}$ tales que $F(J) = F(J')$. Luego $f(J) = f(J')$. Si $a \in J$, entonces $f(a) \in f(J) = f(J')$, de manera que $f(a) = f(b)$ para algún $b \in J'$. De ahí que $(a, b) \in ker(f) = \rho_I^S$ y por lo tanto $a, b \in I \subseteq J'$ o bien $a = b$. En cualquier caso se concluye que $a \in J'$. Por consiguiente $J \subseteq J'$. De manera similar se deduce que $J' \subseteq J$. Por lo tanto $J = J'$ y en consecuencia F es inyectiva. Por otro lado sea $K \in \mathbb{Y}$. De la Proposición 3.9.7 se sigue que $f^{-1}(K)$ es ideal de S. Sea 0_T el elemento cero de T. Como K es un ideal de T, entonces $\{0_T\} \subseteq K$. Además de eso, de la Proposición 3.9.10 se ve que $f(I) = \{0_T\}$ y por lo tanto $f(I) \subseteq K$. De esto último y de la Proposición 1.4.27 resulta que $I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(K)$, de donde $f^{-1}(K) \in \mathbb{X}$. Finalmente, como f es sobreyectiva, entonces $K = f(f^{-1}(K)) = F(f^{-1}(K))$ y por tanto F es sobreyectiva. En definitiva F es una función biyectiva y el resultado se sigue. □

Para concluir esta discusión, y como corolario de lo anterior, se caracteriza a los ideales de $\frac{S}{I}$.

Corolario 3.9.12.

Sean S un semigrupo e I un ideal de S. Entonces, $\hat{J}$ es ideal de $\frac{S}{I}$ si y solo si $\hat{J} = \frac{J}{I}$ para algún ideal J de S tal que $I \subseteq J$.

Demostración. $\Longleftarrow$) Sea J un ideal de S tal que $I \subseteq J$. Obsérvese que

$$\begin{aligned}[a]_{\rho_I^S} \in \frac{J}{I} &\Longleftrightarrow [a]_{\rho_I^S} = I \quad \text{ó} \quad [a]_{\rho_I^S} = \{a\}, a \in J - I \\ &\Longleftrightarrow a \in I \quad \text{ó} \quad a \in J - I \\ &\Longleftrightarrow a \in J\end{aligned}$$

De esto último y de que J es un ideal de S se sigue que $\frac{J}{I}$ es un ideal de $\frac{S}{I}$.

$\Longrightarrow$) Como el morfismo proyección $\pi_{\rho_I^S} : S \longrightarrow \frac{S}{I}$ es un morfismo sobreyectivo de Rees, entonces de la prueba del Teorema 3.9.11 resulta que la función $F : \mathbb{X} \longrightarrow \mathbb{Y}$ definida por $F(J) := \pi_{\rho_I^S}(J)$ es una biyección entre los conjuntos

$$\mathbb{X} := \{J \subseteq S \mid J \text{ es ideal de } S \text{ e } I \subseteq J\} \quad \text{y} \quad \mathbb{Y} := \{\hat{J} \subseteq \tfrac{S}{I} \mid \hat{J} \text{ es ideal de } \tfrac{S}{I}\}$$

Sea $\hat{J}$ un ideal de $\frac{S}{I}$. Entonces $\hat{J} = F(J) = \pi_{\rho_I^S}(J)$ para algún ideal J de S tal que $I \subseteq J$. Ahora bien, se tiene que

$$\begin{aligned}\pi_{\rho_I^S}(J) &= \{\pi_{\rho_I^S}(a) \mid a \in J\} \\ &= \{\pi_{\rho_I^S}(a) \mid a \in I\} \cup \{\pi_{\rho_I^S}(a) \mid a \in J - I\} \\ &= \{I\} \cup \{\{a\} \mid a \in J - I\} \\ &= \frac{J}{I}\end{aligned}$$

Por consiguiente $\hat{J} = \frac{J}{I}$ y el resultado queda demostrado.

□

.

Capítulo 4

Semigrupos libres

Tómese un conjunto no vacío y piénsese a éste como un 'alfabeto'. Así, se considerará a todas las 'palabras' que se puedan formar con este alfabeto para entonces definir un 'producto' entre palabras llamado concatenación. Resultará ser que la concatenación entre palabras es una operación binaria asociativa y por consiguiente, se tendrá así un semigrupo. Todas estas ideas se formalizan empezando con el siguiente par de definiciones.

Definición 4.0.1.

Sea $X \neq \emptyset$ un conjunto.

- Una **palabra** sobre el conjunto X es un símbolo de la forma $x_1x_2 \cdots x_n$ donde $n \in \mathbb{N}$ y $x_i \in X$.
- Dos palabras $a_1a_2 \cdots a_n$ y $b_1b_2 \cdots b_m$ **serán iguales** si y solo si $n = m$ y $a_i = b_i$ para cada $i \in \{1, 2, ..., n\}$.
- Se escribe X^+ para denotar a la colección de todas las palabras sobre el conjunto X •

Definición 4.0.2.

Sean $X \neq \emptyset$ y $\hat{x} \in X^+$. De la definición de igualdad entre palabras se sigue que existe un único $n \in \mathbb{N}$ y únicos $x_1, x_2, , , x_n \in X$ tales que $\hat{x} = x_1x_2 \cdots x_n$. Al entero positivo n se le llamará la **longitud** de la palabra $\hat{x}$. Así, observe que las palabras de longitud igual a 1 son simplemente los elementos de X, de manera que $X \subseteq X^+$ •

Observación 4.0.3.

La longitud de una palabra es entonces el número de palabras de longitud 1 de las que ésta se compone •

Sean $X \neq \emptyset$ y $a_1a_2 \cdots a_n, b_1b_2 \cdots b_m \in X^+$. A partir de estas dos palabras puede obtenerse una tercera definiendo

$$a_1a_2\cdots a_n * b_1b_2\cdots b_m := a_1a_2\cdots a_nb_1b_2\cdots b_m$$

A esta nueva palabra se le llamará la **concatenación** de $a_1a_2\cdots a_n$ con $b_1b_2\cdots b_m$. La concatenación de palabras es asociativa, pues

$$\begin{aligned} a_1a_2\cdots a_n * (b_1b_2\cdots b_m * c_1c_2\cdots c_r) &= a_1a_2\cdots a_n * (b_1b_2\cdots b_mc_1c_2\cdots c_r) \\ &= a_1a_2\cdots a_nb_1b_2\cdots b_mc_1c_2\cdots c_r \\ &= (a_1a_2\cdots a_nb_1b_2\cdots b_m) * c_1c_2\cdots c_r \\ &= (a_1a_2\cdots a_n * b_1b_2\cdots b_m) * c_1c_2\cdots c_r \end{aligned}$$

Por consiguiente, X^+ junto con la concatenación de palabras dan lugar a un semigrupo al que se le llama **semigrupo libre de palabras sobre** X.

Observación 4.0.4.

De la definición de concatenación se aprecia que concatenar una palabra de longitud n con una palabra de longitud m produce una palabra de longitud $n+m$ •

A continuación se define lo que se entenderá por una base de un semigrupo.

Definición 4.0.5.

Sea $(S,\odot)$ un semigrupo y $\emptyset \neq X \subseteq S$. Se dice que X es una **base** de S si se verifica que:

1. $S = \langle X\rangle$
2. Para cada $a_1, a_2, ..., a_n, b_1, b_2, ..., b_m \in X$:

$$a_1 \odot a_2 \odot \cdots \odot a_n = b_1 \odot b_2 \odot \cdots \odot b_m \Longrightarrow n = m \text{ y } a_i = b_i \text{ para cada } i \in \{1, 2, ..., n\}$$ •

Con respecto a la definición de base se tiene lo siguiente.

Proposición 4.0.6.

Sea $X \neq \emptyset$. Entonces X es una base de X^+.

Demostración. Ha de verificarse que X satisface las dos condiciones de la Definición 4.0.5. Para ver que 1) se satisface, sea $\hat{x} \in X^+$ arbitraria. Entonces $\hat{x} = x_1x_2\cdots x_n$ para algún $n \in \mathbb{N}$ y algunos $x_i \in X$. De la definición de concatenación entre palabras se sigue que $x_1 * x_2 * \cdots * x_n = x_1x_2\cdots x_n = \hat{x}$, así $\hat{x} \in \langle X\rangle$ y $X^+ = \langle X\rangle$. Para 2), suponga que $a_1, a_2, ..., a_n, b_1, b_2, ..., b_m \in X$ son tales que $a_1 * a_2 * \cdots * a_n = b_1 * b_2 * \cdots * b_m$, luego $a_1a_2\cdots a_n = b_1b_2\cdots b_m$ de manera que de la igualdad entre dos palabras se sigue que $n = m$ y $a_i = b_i$ para cada $i \in \{1, 2, , , n\}$. Por lo tanto X es base de X^+. □

En general, los semigrupos X^+ no son conmutativos.

Proposición 4.0.7.

Suponga que $X \neq \emptyset$ tiene al menos dos elementos. Entonces X^+ no es un semigrupo conmutativo.

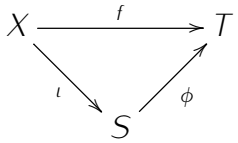
Demostración. Sean $a, b \in X$ con $a \neq b$. Entonces, de la igualdad entre palabras se sigue que $ab \neq ba$ y por consiguiente $a * b \neq b * a$.

□

Lo que sigue es justificar porqué se le llamó libre al semigrupo X^+. Para tal efecto, considere la definición que sigue.

Definición 4.0.8.

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Se dice que S es un **semigrupo libre con base** X si para cada semigrupo T y cada función $f : X \longrightarrow T$ existe un único morfismo de semigrupos $\phi : S \longrightarrow T$ que hace conmutar al diagrama



donde $\iota : X \longrightarrow S$ es la función inclusión •

Como es de esperarse, resulta que el semigrupo X^+ es un semigrupo libre en el sentido de la Definición 4.0.8.

Proposición 4.0.9.

Sea $X \neq \emptyset$. Entonces X^+ es un semigrupo libre con base X.

Demostración. Sean $(T, \odot)$ un semigrupo y $f : X \longrightarrow T$ una función. A partir de f se define a $\phi : X^+ \longrightarrow T$ como $\phi(a_1 a_2 \cdots a_n) := f(a_1) \odot f(a_2) \odot \cdots \odot f(a_n)$. Observe que para cada $a \in X$ se verifica que $\phi(a) = f(a)$ y por consiguiente $f = \phi \circ \iota$. Ahora bien, se tiene que

$$\begin{aligned}
\phi(a_1 a_2 \cdots a_n * b_1 b_2 \cdots b_m) &= \phi(a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m) \\
&= f(a_1) \odot f(a_2) \odot \cdots \odot f(a_n) \odot f(b_1) \odot f(b_2) \odot \cdots \odot f(b_m) \\
&= [f(a_1) \odot f(a_2) \odot \cdots \odot f(a_n)] \odot [(f(b_1) \odot f(b_2) \odot \cdots \odot f(b_m)] \\
&= \phi(a_1 a_2 \cdots a_n) \odot \phi(b_1 b_2 \cdots b_m)
\end{aligned}$$

Por lo tanto ϕ es un morfismo de semigrupos. Suponga ahora que $\psi : X^+ \longrightarrow T$ es un morfismo de semigrupos tal que $f = \psi \circ \iota$. Entonces, si $a_1 a_2 \cdots a_n \in X^+$:

$$\begin{aligned}\psi(a_1a_2\cdots a_n) &= \psi(a_1 * a_2 * \cdots * a_n)\\ &= \psi(a_1)\odot\psi(a_2)\odot\cdots\odot\psi(a_n)\\ &= f(a_1)\odot f(a_2)\odot\cdots\odot f(a_n)\\ &= \phi(a_1a_2\cdots a_n)\end{aligned}$$

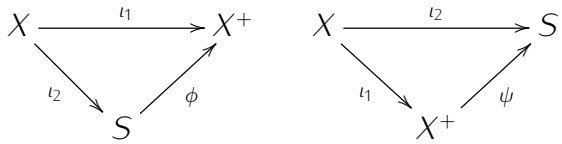
De donde $\phi = \psi$ y el resultado se sigue. □

Resulta que cada semigrupo libre en el sentido de la Definición 4.0.8 es isomorfo a alguno de la forma X^+ como se establece a continuación.

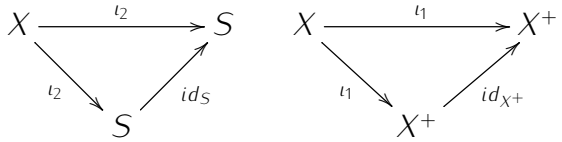
Proposición 4.0.10.

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Si S es libre con base X, entonces $S \cong X^+$.

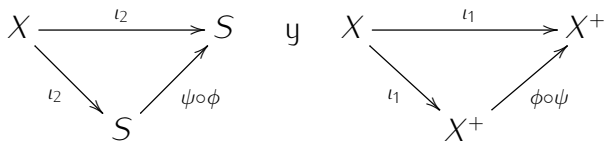
Demostración. Considere las inclusiones $\iota_1 : X \longrightarrow X^+$ y $\iota_2 : X \longrightarrow S$. De que S y X^+ son ambos semigrupos libres con base X se sigue que existen morfismos de semigrupos $\phi : S \longrightarrow X^+$ y $\psi : X^+ \longrightarrow S$ (que además deben ser únicos) que hacen conmutativos a los siguientes diagramas



Por otra parte, es claro que los diagramas



son conmutativos. De nuevo, como S y X^+ son ambos semigrupos libres con base X se sigue que id_S e id_{X^+} son los únicos morfismos de semigrupos que hacen conmutar al último par de diagramas. Ahora bien, de que el primer par de diagramas conmute se deduce que $(\psi \circ \phi) \circ \iota_2 = \psi \circ (\phi \circ \iota_2) = \psi \circ \iota_1 = \iota_2$ y también $(\phi \circ \psi) \circ \iota_1 = \phi \circ (\psi \circ \iota_1) = \phi \circ \iota_2 = \iota_1$. Por consiguiente, $\psi \circ \phi$ y $\phi \circ \psi$ son morfismos de semigrupos tales que



conmutan. De ahí que $\psi \circ \phi = id_S$ y $\phi \circ \psi = id_{X^+}$. En consecuencia $\psi : X^+ \longrightarrow S$ es un isomorfismo de semigrupos y por lo tanto $S \cong X^+$. □

Observación 4.0.11.

Puede determinarse de forma explícita al isomorfismo $\psi : X^+ \longrightarrow S$ que se menciona en la prueba de la Proposición 4.0.10. En efecto, ψ es un morfismo de semigrupos tal que $\psi \circ \iota_1 = \iota_2$. Así que para cada $a \in X$ es $\psi(a) = \psi(\iota_1(a)) = \iota_2(a) = a$. Luego, para cada palabra $a_1a_2 \cdots a_n \in X^+$ se tiene que

$$\begin{aligned}\psi(a_1a_2 \cdots a_n) &= \psi(a_1 * a_2 * \cdots * a_n) \\ &= \psi(a_1) \odot \psi(a_2) \odot \cdots \odot \psi(a_n) \\ &= a_1 \odot a_2 \odot \cdots \odot a_n\end{aligned}$$

donde $\odot$ denota la operación en el semigrupo S •

Corolario 4.0.12.

Sean $(S, \odot)$ un semigrupo y $\emptyset \neq X \subseteq S$. Si S es libre con base X, entonces la función $\psi : X^+ \longrightarrow S$ definida por $\psi(a_1a_2 \cdots a_n) = a_1 \odot a_2 \odot \cdots \odot a_n$ es un isomorfismo de semigrupos.

Demostración. Directa de la Proposición 4.0.10 y la Observación 4.0.11. □

De acuerdo con la Proposición 4.0.6, X es base de X^+ en el sentido de la Definición 4.0.5. También, en virtud de la Proposición 4.0.10 todo semigrupo libre en el sentido de la Definición 4.0.8 es isomorfo a algún semigrupo de la forma X^+. Así, es de esperarse que todo semigrupo libre en el sentido de la Definición 4.0.8 tenga una base en el sentido de la Definición 4.0.5. Para ver que eso sucede se hará uso de lo siguiente.

Proposición 4.0.13.

Sea $f : S \longrightarrow T$ un isomorfismo de semigrupos. Si $\emptyset \neq X \subseteq S$ es una base de S, entonces $f(X)$ es una base de T.

Demostración. Sea $t \in T$ arbitrario. Puesto que f es sobreyectiva puede escribirse $t = f(s)$ para algún $s \in S$. Ahora bien, como $S = \langle X \rangle$, entonces $s = x_1x_2 \cdots x_n$ para algunos $n \in \mathbb{N}$ y $x_i \in X$. De ahí que $t = f(s) = f(x_1x_2 \cdots x_n) = f(x_1)f(x_2) \cdots f(x_n) \in \langle f(X) \rangle$ y por lo tanto $T = \langle f(X) \rangle$. Por otro lado, suponga que $f(a_1)f(a_2) \cdots f(a_n) = f(b_1)f(b_2) \cdots f(b_m)$ donde $n, m \in \mathbb{N}$ y $a_i, b_i \in X$. Entonces $f(a_1a_2 \cdots a_n) = f(b_1b_2 \cdots b_m)$, de manera que al ser f inyectiva se sigue que $a_1a_2 \cdots a_n = b_1b_2 \cdots b_m$. Así que como X es base de S, entonces $n = m$ y $a_i = b_i$ para cada $i \in \{1, 2, , , n\}$. Por consiguiente $f(a_i) = f(b_i)$ y en definitiva $f(X)$ es una base de T. □

Observación 4.0.14.

En la demostración de la Proposición 4.0.13 $x_1x_2 \cdots x_n$ y $f(x_1)f(x_2) \cdots f(x_n)$ no denotan palabras en el sentido de la Definición 4.0.1, si no más bien el producto de los elementos $x_1, x_2, \ldots, x_n$ y $f(x_1), f(x_2), \ldots, f(x_n)$ en el semigrupo S y T respectivamente •

Proposición 4.0.15.

Sean $(S, \odot)$ un semigrupo y $\emptyset \neq X \subseteq S$. Si S es libre con base X, entonces X es una base de S.

Demostración. Del Corolario 4.0.12 se sigue que la función $\psi : X^+ \longrightarrow S$ definida por $\psi(a_1 a_2 \cdots a_n) = a_1 \odot a_2 \odot \cdots \odot a_n$ es un isomorfismo de semigrupos. Obsérvese que $\psi(X) := \{\psi(a) \mid a \in X\} = \{a \mid a \in X\} = X$. Por consiguiente, de la Proposición 4.0.13 se deduce que X es una base de S. □

Se puede decir ahora que todo semigrupo libre tiene una base, pero ¿será cierto el recíproco?

Proposición 4.0.16.

Sea $(S, \odot)$ un semigrupo y $\emptyset \neq X \subseteq S$. Si X es base de S, entonces S es un semigrupo libre con base X.

Demostración. Sea $(T, \otimes)$ un semigrupo y $f : X \longrightarrow T$ una función. De que X es base de S se sigue que $S = \langle X \rangle$. Luego, puede definirse a $\Phi : S \longrightarrow T$ como $\Phi(a_1 \odot a_2 \odot \cdots \odot a_n) := f(a_1) \otimes f(a_2) \otimes \cdots \otimes f(a_n)$. Observese que

$$\begin{aligned}
\Phi([a_1 \odot \cdots \odot a_n] \odot [b_1 \odot \cdots \odot b_m]) &= \Phi(a_1 \odot \cdots \odot a_n \odot b_1 \odot \cdots \odot b_m) \\
&= f(a_1) \otimes \cdots \otimes f(a_n) \otimes f(b_1) \otimes \cdots \otimes f(b_m) \\
&= [f(a_1) \otimes \cdots \otimes f(a_n)] \otimes [f(b_1) \otimes \cdots \otimes f(b_m)] \\
&= \Phi(a_1 \odot \cdots \odot a_n) \otimes \Phi(b_1 \odot b_2 \odot \cdots \odot b_m)
\end{aligned}$$

Por consiguiente Φ es un morfismo de semigrupos. Más aún, para cada $a \in X$ se tiene que $\Phi(a) = f(a)$ y en consecuencia $f = \Phi \circ \iota$ siendo $\iota : X \longrightarrow S$ la función inclusión. Sea $\Psi : S \longrightarrow T$ un morfismo de semigrupos tal que $f = \Psi \circ \iota$. Entonces

$$\begin{aligned}
\Psi(a_1 \odot a_2 \odot \cdots \odot a_n) &= \Psi(a_1) \otimes \Psi(a_2) \otimes \cdots \otimes \Psi(a_n) \\
&= f(a_1) \otimes f(a_2) \otimes \cdots \otimes f(a_n) \\
&= \Phi(a_1 \odot a_2 \odot \cdots \odot a_n)
\end{aligned}$$

De ahí que $\Psi = \Phi$ y el resultado queda demostrado.

□

Observación 4.0.17.

La Proposición 4.0.9 es entonces una consecuencia de las Proposiciones 4.0.6 y 4.0.16 •

Proposición 4.0.18.

Sea S un semigrupo y $\emptyset \neq X \subseteq S$. Los siguientes enunciados son equivalentes

1. S es un semigrupo libre con base X.
2. X es una base de S.

Demostración. $\Longrightarrow$) Es la Proposición 4.0.15.
$\Longleftarrow$) Es la Proposición 4.0.16. □

Por consiguiente, es válido decir que un semigrupo libre es aquel que tiene una base. Ahora bien, ¿cuándo dos semigrupos libres son isomorfos?

Proposición 4.0.19.

Sean X y Y conjuntos no vacíos. Entonces $X^+ \cong Y^+$ si y solo si X y Y son equipotentes.

Demostración. $\Longrightarrow$) Sea $\phi : X^+ \longrightarrow Y^+$ un isomorfismo de semigrupos. **Afirmación:** Si $a \in X$, entonces $\phi(a) \in Y$ i,e, $\phi(a)$ es una palabra de longitud igual a 1. En efecto, supongase que $\phi(a)$ es una palabra de longitud $n > 1$. Entonces $\phi(a) = b_1 b_2 \cdots b_n$ donde cada $b_i \in Y$. Como ϕ es sobreyectiva, para cada $i \in \{1, 2, , , n\}$ puede escribirse $b_i = \phi(\hat{x}_i)$ siendo $\hat{x}_i \in X^+$ una palabra de longitud igual a $m_i \geq 1$. Así

$$\begin{aligned}\phi(a) &= b_1 b_2 \cdots b_n \\ &= b_1 * b_2 * \cdots * b_n \\ &= \phi(\hat{x}_1) * \phi(\hat{x}_2) * \cdots * \phi(\hat{x}_n) \\ &= \phi(\hat{x}_1 * \hat{x}_2 * \cdots * \hat{x}_n)\end{aligned}$$

Al ser ϕ inyectiva se sigue que $a = \hat{x}_1 * \hat{x}_2 * \cdots * \hat{x}_n$ y de la igualdad entre palabras se deduce que la longitud de $\hat{x}_1 * \hat{x}_2 * \cdots * \hat{x}_n$ debe ser igual a 1. Por otra parte, $\hat{x}_1 * \hat{x}_2 * \cdots * \hat{x}_n$ es la concatenación de n palabras de longitud al menos 1, luego, la longitud de $\hat{x}_1 * \hat{x}_2 * \cdots * \hat{x}_n$ debe ser al menos n y por tanto mayor que 1, lo cual es una contradicción. Por consiguiente $\phi(a)$ es una palabra de longitud igual a 1 y la afirmación se sigue. En virtud de lo anterior, tiene sentido considerar a la función $\Phi : X \longrightarrow Y$ definida por $\Phi(a) := \phi(a)$. De la inyectividad de ϕ se sigue que Φ es también inyectiva. En resumen, a partir del isomorfismo $\phi : X^+ \longrightarrow Y^+$ se ha obtenido una función inyectiva de X en Y. Usando ahora al morfismo inverso de ϕ y argumentando de manera similar puede obtenerse una función inyectiva de Y en X. Por lo tanto, el Teorema 1.4.31 permite concluir que X y Y son equipotentes.
$\Longleftarrow$) Sea $f : X \longrightarrow Y$ una función biyectiva. Se define a $\phi : X^+ \longrightarrow Y^+$ como $\phi(a_1 a_2 \cdots a_n) := f(a_1) f(a_2) \cdots f(a_n)$. Este es un morfismo de semigrupos, pues

$$\begin{aligned}\phi(a_1 a_2 \cdots a_n * b_1 b_2 \cdots b_m) &= \phi(a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m) \\ &= f(a_1) f(a_2) \cdots f(a_n) f(b_1) f(b_2) \cdots f(b_m) \\ &= (f(a_1) f(a_2) \cdots f(a_n)) * (f(b_1) f(b_2) \cdots f(b_m)) \\ &= \phi(a_1 a_2 \cdots a_n) * \phi(b_1 b_2 \cdots b_m)\end{aligned}$$

Observar que ϕ manda palabras de longitud n en palabras de longitud n. Además

$$\begin{aligned} & \phi(a_1a_2\cdots a_n) = \phi(b_1b_2\cdots b_m) \\ \Longrightarrow\ & f(a_1)f(a_2)\cdots f(a_n) = f(b_1)f(b_2)\cdots f(b_m) \\ \Longrightarrow\ & n = m \quad \text{y} \quad f(a_i) = f(b_i) \\ \Longrightarrow\ & a_i = b_i \quad \text{para cada} \quad i \in \{1,2,,,n\} \\ \Longrightarrow\ & a_1a_2\cdots a_n = b_1b_2\cdots b_m \end{aligned}$$

Por consiguiente ϕ es inyectiva. Finalmente, sea $y_1y_2\cdots y_n \in Y^+$ arbitraria. Como cada $y_i \in Y$ y f es sobreyectiva, entonces $y_i = f(x_i)$ para algún $x_i \in X$. Así, $y_1y_2\cdots y_n = f(x_1)f(x_2)\cdots f(x_n) = \phi(x_1x_2\cdots x_n)$ y por lo tanto ϕ es sobreyectiva. Se concluye que ϕ es un isomorfismo de semigrupos y $X^+ \cong Y^+$. □

Corolario 4.0.20.

Sea S un semigrupo y $\emptyset \neq X, Y \subseteq S$. Si X y Y son bases de S, entonces X y Y son equipotentes.

Demostración. Si X y Y son bases de S, entonces $X^+ \cong S$ y $S \cong Y^+$, luego $X^+ \cong Y^+$ y en consecuencia X y Y son equipotentes. □

El corolario anterior le da sentido a la definición que a continuación se enuncia.

Definición 4.0.21.

Suponga que S es un semigrupo que posee al menos una base (ver Definición 4.0.5). Se define el **rango** de S, denotado $Rank(S)$, como $Rank(S) := |X|$, siendo $X \subseteq S$ cualquier base de S y $|X|$ el cardinal del conjunto X •

4.1. Observaciones

Se finaliza esta sección con las siguientes 4 observaciones.

1. Para cada conjunto $X \neq \emptyset$ existe un semigrupo para el cual X es base, a saber, el semigrupo X^+.
2. $X = \{1\}$ es base del semigrupo $(\mathbb{N}, +)$. Por consiguiente $(\mathbb{N}, +)$ es un semigrupo libre.
3. Existen semigrupos que no tienen bases.
4. No todo subsemigrupo de un semigrupo libre es libre.

Para establecer la tercera de ellas haremos uso de lo siguiente.

Proposición 4.1.1.

Sean S y T semigrupos. Si $S \cong T$ y S es conmutativo, entonces T es conmutativo.

Demostración. Sean $f : S \longrightarrow T$ un isomorfismo de semigrupos y $x, y \in T$. De la sobreyectividad de f puede escribirse $x = f(a)$ y $y = f(b)$ para algunos $a, b \in S$. Así, $xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$ y T es conmutativo. □

Ahora, se define lo que se entenderá por semigrupo monogénico (o cíclico).

Definición 4.1.2.

Se dice que un semigrupo S es un semigrupo **monogénico** (o **cíclico**) si existe $a \in S$ tal que $S = \langle a \rangle$ •

Proposición 4.1.3.

Si S es un semigrupo conmutativo y no monogénico, entonces S no posee bases.

Demostración. Suponga que $\emptyset \neq X \subseteq S$ es una base de S. Luego, debe suceder que $S \cong X^+$. Por otro lado, como S es conmutativo, entonces X^+ también debe ser conmutativo. Ahora bien, puesto que X es base de S se tiene que $S = \langle X \rangle$, y como S no es monogénico, entonces X debe tener al menos dos elementos. Así, de la Proposición 4.0.7 se deduce que X^+ no es conmutativo, lo cual es una contradicción. Por consiguiente S no posee bases. □

A continuación se muestran ejemplos de semigrupos con las características de la Proposición 4.1.3.

Ejemplo 4.1.4.

El semigrupo $(\mathbb{N}, \cdot)$ es conmutativo y no monogénico. En efecto, supongase que $(\mathbb{N}, \cdot)$ es un semigrupo monogénico. Entonces $\mathbb{N} = \langle a \rangle$ para algún $a \in \mathbb{N}$. Así que $\mathbb{N} = \{a^n \mid n \in \mathbb{N}\}$, y en particular puede escribirse $2 = a^n$ para algún $n \in \mathbb{N}$. De ahí que a sea un divisor de 2, y al ser este último un número primo debe ser entonces que o bien $a = 1$ o bien $a = 2$. En el primer caso resulta que $\mathbb{N} = \{1\}$, lo cual es falso. Luego, $a = 2$ y así $\mathbb{N} = \{2^n \mid n \in \mathbb{N}\}$. Por lo tanto $3 = 2^m$ para algún $m \in \mathbb{N}$ y en consecuencia 2 debe ser un divisor de 3, lo cual es una contradicción. Se concluye que $(\mathbb{N}, \cdot)$ no es un semigrupo monogénico. De la Proposición 4.1.3 se sigue que $(\mathbb{N}, \cdot)$ no posee bases •

Ejemplo 4.1.5.

Considerar al conjunto $2\mathbb{N} + 3\mathbb{N} := \{2n + 3m \mid n, m \in \mathbb{N}\}$. Este es un subsemigrupo de $(\mathbb{N}, +)$ pues, $(2a + 3b) + (2n + 3m) = 2(a + n) + 3(b + m)$. Suponga que $2\mathbb{N} + 3\mathbb{N} = \langle a \rangle = \{na \mid n \in \mathbb{N}\}$ para algún $a \in 2\mathbb{N} + 3\mathbb{N}$. Como $5 \in 2\mathbb{N} + 3\mathbb{N}$, se sigue que $5 = na$ para algún $n \in \mathbb{N}$. Así que como 5 es un número primo debe ser que $a = 1$ o bien $a = 5$. De que $2\mathbb{N} + 3\mathbb{N} \neq \{1\}$ se sigue que $a = 5$. Así, $2\mathbb{N} + 3\mathbb{N} = \{5n \mid n \in \mathbb{N}\}$. Ahora bien, como $8 = 2 + 3(2) \in 2\mathbb{N} + 3\mathbb{N}$, entonces $8 = 5m$ para algún $m \in \mathbb{N}$. De ahí que 5 es un divisor

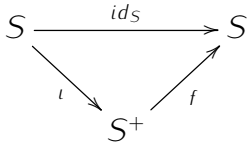
de 8, lo cual es falso. Se concluye que $(2\mathbb{N}+3\mathbb{N},+)$ no es un semigrupo monogénico, y en particular no posee bases •

Para establecer la observación 4 considere a $(2\mathbb{N}+3\mathbb{N},+)$ que es un subsemigrupo del semigrupo libre $(\mathbb{N},+)$. Puesto que $(2\mathbb{N}+3\mathbb{N},+)$ no posee bases se sigue que $(2\mathbb{N}+3\mathbb{N},+)$ no es un semigrupo libre. Los ejemplos anteriores muestran que no todo semigrupo es un semigrupo libre. Sin embargo, se tiene lo siguiente.

Proposición 4.1.6.

Todo semigrupo es isomorfo a un cociente de algún semigrupo libre.

Demostración. Sea S un semigrupo y considere al semigrupo libre S^+. Para la función $id_S : S \longrightarrow S$ existe un único morfismo de semigrupos $f : S^+ \longrightarrow S$ tal que el diagrama



conmuta. De ahí que para cada $s \in S$ se tiene que $s = f(\iota(s))$ y por consiguiente f es sobreyectiva. Por lo tanto $\dfrac{S^+}{Ker(f)} \cong S$ y el resultado se sigue. □

.

Capítulo 5

La categoría de semigrupos

Considere lo siguiente.

- Denótese por $\mathcal{S}$ a la clase de todos los semigrupos.
- Si $S, T \in \mathcal{S}$ sea

$$Hom(S, T) := \{f : S \longrightarrow T \mid f \text{ es morfismo de semigrupos}\}$$

- Para cada $S \in \mathcal{S}$ sea id_S la función identidad.
- Sea $\circ$ la composición entre funciones.

De que la composición entre dos morfismos de semigrupos sea de nuevo un morfismo de semigrupos, de que la función identidad sea un morfismo de semigrupos, de las Proposiciones 1.1.10 y 1.4.6 se deduce que todo lo anterior da lugar a una categoría (véase Definición 2.1.1) cuyos objetos son los semigrupos y cuyos morfismos son los morfismos de semigrupos. Denotamos a ésta por $SGRP$ y la llamamos **categoría de semigrupos**. Se revisan en esta sección algunas propiedades de $SGRP$.
Se da inicio a esta discusión con la definición de subcategoría y enseguida se muestran algunos ejemplos.

Definición 5.0.1.

Sea $\mathcal{A}$ una categoría. Una **subcategoría** $\mathcal{B}$ de $\mathcal{A}$ consiste de

- Una subclase $Ob(\mathcal{B})$ de la clase $Ob(\mathcal{A})$.
- Para cada $X, Y \in Ob(\mathcal{B})$ un conjunto $Hom_{\mathcal{B}}(X, Y)$.

Además, para cada $X, Y, Z \in Ob(\mathcal{B})$ se ha de verificar que

1. $Hom_{\mathcal{B}}(X, Y) \subseteq Hom_{\mathcal{A}}(X, Y)$.

2. $id_X \in Hom_{\mathcal{B}}(X, X)$.

3. Si $f \in Hom_{\mathcal{B}}(X, Y)$ y $g \in Hom_{\mathcal{B}}(Y, Z)$ entonces $g \circ f \in Hom_{\mathcal{B}}(X, Z)$

Si en adición ocurre que $Hom_{\mathcal{B}}(X, Y) = Hom_{\mathcal{A}}(X, Y)$ para cada $X, Y \in Ob(\mathcal{B})$, entonces se dice que $\mathcal{B}$ es una **subcategoría plena** de $\mathcal{A}$ •

Observación 5.0.2.

Se hace evidente de la definición anterior que toda subcategoría de una categoría es por sí misma una categoría bajo la misma ley de composición •

Ejemplos 5.0.3.

1. La categoría de grupos GRP (ver Ejemplos 2.1.2) es una subcategoría plena de $SGRP$.

2. Sea $\mathcal{M}$ la clase de todos los monoides y para cada $M, N \in \mathcal{M}$ sea $Hom_{MON}(M, N) := \{f : M \longrightarrow N \mid f \text{ es morfismo de monoides}\}$. De que la función identidad sea un morfismo de monoides aunado a que la composición entre morfismos de monoides es de nuevo un morfismo de monoides, se sigue que lo anterior forma una subcategoría de $SGRP$. Se denota a esta subcategoría por MON y se le llama la **categoría de monoides**. De acuerdo con la Observación 3.7.2, MON no es una subcategoría plena de $SGRP$.

3. Sea $\mathcal{A}$ la clase de todos los grupos abelianos (conmutativos) y para cada $A, B \in \mathcal{A}$ sea $Hom_{Ab}(A, B) := \{f : A \longrightarrow B \mid f \text{ es morfismo de grupos}\}$. De que la función identidad sea un morfismo de grupos aunado a que la composición entre morfismos de grupos es de nuevo un morfismo de grupos, se sigue que lo anterior forma una subcategoría de GRP. Se denota a esta subcategoría por Ab y se le llama la **categoría de grupos abelianos** •

5.1. Producto y coproducto en SGRP

Definición 5.1.1.

Suponga que $S_1, S_2, ..., S_n$ son n semigrupos. Sobre el conjunto $S_1 \times S_2 \times \cdots \times S_n$ se define la siguiente operación binaria

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) := (a_1 b_1, a_2 b_2, ..., a_n b_n)$$

De la asociatividad de cada S_i se sigue que esta operación entre n-adas es asociativa y por lo tanto $S_1 \times S_2 \times \cdots \times S_n$ es un semigrupo. Cuando cada S_i es un monoide con neutro e_i entonces $S_1 \times S_2 \times \cdots \times S_n$ es un monoide con neutro la n-ada $(e_1, e_2, ..., e_n)$. Llamamos a este semigrupo (monoide) el **producto directo** de los semigrupos (monoides) $S_1, S_2, ..., S_n$ •

Proposición 5.1.2.

Si $f : S \longrightarrow T$ es un morfismo de semigrupos, entonces $Ker(f)$ es un subsemigrupo de $S \times S$.

Demostración. Tómense $(a, b), (c, d) \in Ker(f)$. Entonces

$$\begin{aligned} & f(a) = f(b) \quad \text{y} \quad f(c) = f(d) \\ \Longrightarrow \quad & f(a)f(c) = f(b)f(d) \\ \Longrightarrow \quad & f(ac) = f(bd) \\ \Longrightarrow \quad & (a, b)(c, d) = (ac, bd) \in Ker(f) \end{aligned}$$

□

Observe que se ha definido el producto directo de una colección finita de semigrupos, pero ¿cómo puede extenderse esto a una familia arbitraria?

Sea $(S_i)_{i\in I}$ una familia de objetos de $SGRP$ indexada por el conjunto $I \neq \emptyset$ y sea $\prod_{i\in I} S_i$ el producto cartesiano de la familia $(S_i)_{i\in I}$ (véase Definición 1.4.21). Tómense $f, g \in \prod_{i\in I} S_i$ e $i \in I$ arbitrarios. Entonces debe ocurrir que $f(i), g(i) \in S_i$ y por consiguiente también $f(i)g(i) \in S_i$. Tiene sentido así considerar a la función $fg : I \longrightarrow \bigcup_{i\in I} S_i$ definida por $(fg)(i) := f(i)g(i)$. Observe que $fg \in \prod_{i\in I} S_i$. Más aún, si se toman $f, g, h \in \prod_{i\in I} S_i$, entonces

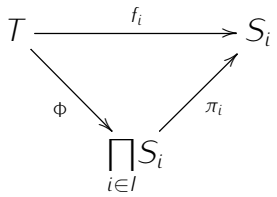
$$\begin{aligned} [(fg)h](i) &= (fg)(i)h(i) \\ &= [f(i)g(i)]h(i) \\ &= f(i)[g(i)h(i)] \\ &= f(i)(gh)(i) \\ &= [f(gh)](i) \end{aligned}$$

Por consiguiente $(fg)h = f(gh)$, de manera que $\prod_{i\in I} S_i$ es un semigrupo bajo esta operación binaria y por lo tanto un objeto de $SGRP$. Si además cada S_i es un monoide con neutro e_i, entonces de la definición de fg se sigue que $\prod_{i\in I} S_i$ es un monoide con neutro la función $\hat{e} : I \longrightarrow \bigcup_{i\in I} S_i$ definida por $\hat{e}(i) := e_i$. Recordar ahora que la $i-$esima función proyección $\pi_i : \prod_{i\in I} S_i \longrightarrow S_i$ está definida por $\pi_i(f) := f(i)$. De acuerdo a esto se tiene que

$$\pi_i(fg) = (fg)(i) = f(i)g(i) = \pi_i(f)\pi_i(g).$$

Por lo tanto cada función proyección π_i es un morfismo de semigrupos y en consecuencia, un morfismo de la categoría $SGRP$. **Afirmación:** El objeto $\prod_{i\in I} S_i$ junto con los morfismos proyección $\{\pi_i : \prod_{i\in I} S_i \longrightarrow S_i\}_{i\in I}$ son un producto en $SGRP$ para la familia $(S_i)_{i\in I}$ (ver

Definición 2.3.1). En efecto, sean T un semigrupo y $\{f_i : T \longrightarrow S_i\}_{i\in I}$ una familia de morfismos de semigrupos. De la Proposición 1.4.22 se sigue que existe una única función $\Phi : T \longrightarrow \prod_{i\in I} S_i$ tal que para cada $i \in I$ el siguiente triángulo conmuta:



Más aún, la función Φ está dada por $\Phi(t) := \phi_t$ donde $\phi_t : I \longrightarrow \bigcup_{i\in I} S_i$ es definida como $\phi_t(i) := f_i(t)$. Por otro lado, si $a, b \in T$, entonces $\Phi(ab) := \phi_{ab}$ y para cada $i \in I$ se tiene que

$$\begin{aligned}\Phi(ab)(i) &= \phi_{ab}(i)\\ &= f_i(ab)\\ &= f_i(a)f_i(b)\\ &= \phi_a(i)\phi_b(i)\\ &= \Phi(a)(i)\Phi(b)(i)\\ &= [\Phi(a)\Phi(b)](i)\end{aligned}$$

Por consiguiente $\Phi(ab) = \Phi(a)\Phi(b)$ y Φ es un morfismo de semigrupos. Suponga que $\Psi : T \longrightarrow \prod_{i\in I} S_i$ es un morfismo de semigrupos tal que para cada $i \in I$ se verifica que $f_i = \pi_i \circ \Psi$. Como todo morfismo de semigrupos es en particular una función, de la unicidad de Φ se concluye que $\Phi = \Psi$ y la afirmación se sigue. Todo lo anterior puede resumirse en la proposición que a continuación se enuncia.

Proposición 5.1.3.

Toda familia no vacía de objetos de $SGRP$ tiene un producto.

Demostración. Se sigue de la discusión anterior. □

Ahora bien, ¿toda familia no vacía de objetos de $SGRP$ tendrá un coproducto?.

Sea $(S_i)_{i\in I}$ una familia de objetos de $SGRP$ indexada por el conjunto $I \neq \emptyset$ y sea Q la colección de todos los símbolos de la forma

$$(a_1, i_1)(a_2, i_2)\cdots(a_n, i_n)$$

donde $n \in \mathbb{N}$, $i_k \in I$, $a_k \in S_{i_k}$ e $i_k \neq i_{k+1}$ para cada $k \in \{1, 2, \ldots, n-1\}$.

Si $\hat{a} := (a_1, i_1)(a_2, i_2)\cdots(a_n, i_n)$ y $\hat{b} := (b_1, j_1)(b_2, j_2)\cdots(b_m, j_m)$ se define

$$\hat{a} * \hat{b} := \begin{cases} (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m) & si \quad i_n \neq j_1. \\ (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m) & si \quad i_n = j_1. \end{cases}$$

Observe que cuando el índice que aparece en el último par ordenado de $\hat{a}$ difiere del índice que aparece en el primer par ordenado de $\hat{b}$, entonces los pares ordenados de $\hat{a}$ y $\hat{b}$ se concatenan. En caso contrario, cuando el índice que aparece en el último par ordenado de $\hat{a}$ coincide con el índice que aparece en el primer par ordenado de $\hat{b}$ entonces los pares ordenados de $\hat{a}$ y $\hat{b}$ se concatenan, y luego se reemplaza a $(a_n, i_n)(b_1, j_1)$ por $(a_n b_1, i_n)$. Esto puede llevarse a cabo, puesto que como $i_n = j_1$ entonces a_n y b_1 son ambos elementos del semigrupo S_{i_n}. **Afirmación:** La operación $*$ es asociativa. En efecto, sean $\hat{a} := (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)$, $\hat{b} := (b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{c} := (c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ elementos de Q. Para establecer la aseveración se ha de verificar que en todos los casos que a continuación se enuncian resulta que $\hat{a} * (\hat{b} * \hat{c}) = (\hat{a} * \hat{b}) * \hat{c}$:

1. Los conjuntos $\{i_n\}$, $\{j_1\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
2. $i_n = j_1$ y los conjuntos $\{j_1\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
3. $i_n = j_m$ y los conjuntos $\{j_1\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
4. $i_n = k_1$ y los conjuntos $\{j_1\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
5. $i_n = k_1$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{j_m\}$ son disjuntos por pares.
6. $j_1 = k_1$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{j_m\}$ son disjuntos por pares.
7. $j_m = k_1$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{j_m\}$ son disjuntos por pares.
8. $j_1 = j_m$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{k_1\}$ son disjuntos por pares.
9. $j_m = k_1$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{k_1\}$ son disjuntos por pares.
10. $j_m = i_n$ y los conjuntos $\{i_n\}$, $\{j_1\}$ y $\{k_1\}$ son disjuntos por pares.
11. $j_1 = i_n$ y los conjuntos $\{i_n\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
12. $j_1 = j_m$ y los conjuntos $\{i_n\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
13. $j_1 = k_1$ y los conjuntos $\{i_n\}$, $\{j_m\}$ y $\{k_1\}$ son disjuntos por pares.
14. $i_n = j_1$, $j_1 \neq j_m$ y $j_m = k_1$.
15. $i_n = j_m$, $j_m \neq j_1$ y $j_1 = k_1$.
16. $i_n = k_1$, $k_1 \neq j_1$ y $j_1 = j_m$.
17. $i_n = j_1 = j_m \neq k_1$

18. $i_n = j_1 = k_1 \neq j_m$

19. $i_n = j_m = k_1 \neq j_1$

20. $j_1 = j_m = k_1 \neq i_n$

21. $i_n = j_i = j_m = k_1$.

Caso 1. Aquí se tiene que $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 2. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 5. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 7. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 11. En este caso $\hat{a} * \hat{b} = (a_1, i_1) \cdots (a_n b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1) \cdots (b_m, j_m)(c_1, k_1) \cdots (c_r, k_r)$. Por lo tanto $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1) \cdots (a_n b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1) \cdots (a_n b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1) \cdots (c_r, k_r)$

Caso 14. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m c_1, j_m)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 17. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$. Por consiguiente $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n b_1, i_n)(b_2, j_2) \cdots (b_m, j_m)(c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$.

Caso 20. En este caso $\hat{a} * \hat{b} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m, j_m)$ y $\hat{b} * \hat{c} = (b_1, j_1)(b_2, j_2) \cdots (b_m c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$. Por lo tanto $(\hat{a} * \hat{b}) * \hat{c} = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$ y $\hat{a} * (\hat{b} * \hat{c}) = (a_1, i_1)(a_2, i_2) \cdots (a_n, i_n)(b_1, j_1)(b_2, j_2) \cdots (b_m c_1, k_1)(c_2, k_2) \cdots (c_r, k_r)$.

Los casos restantes se verifican de manera análoga a los anteriores y por eso se omiten. Se concluye así que $*$ es una operación asociativa y la afirmación se sigue. Por consiguiente $(Q,*)$ es un semigrupo. Ahora bien, para cada $i \in I$ sea $\sigma_i : S_i \longrightarrow Q$ la función definida por $\sigma_i(a) := (a,i)$. Si $a,b \in S_i$ entonces $\sigma_i(ab) := (ab,i) = (a,i) * (b,i) = \sigma_i(a) * \sigma_i(b)$ y por lo tanto cada función σ_i es un morfismo de semigrupos. Sea T un semigrupo arbitrario y $\{f_i : S_i \longrightarrow T\}_{i\in I}$ una familia de morfismos de semigrupos. Considere ahora a la función $\Psi : Q \longrightarrow T$ definida por $\Psi[(a_1,i_1)(a_2,i_2)\cdots(a_n,i_n)] := f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)$. Veamos que Ψ es un morfismo de semigrupos: si $\hat{a} := (a_1,i_1)(a_2,i_2)\cdots(a_n,i_n)$ y $\hat{b} := (b_1,j_1)(b_2,j_2)\cdots(b_m,j_m)$, entonces se tienen los siguientes dos casos

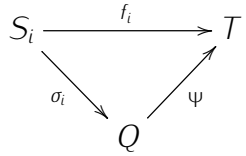
Caso (a) $i_n \neq j_1$. En esta situación se tiene que

$$\begin{aligned}\Psi(\hat{a} * \hat{b}) &= \Psi[(a_1,i_1)(a_2,i_2)\cdots(a_n,i_n)(b_1,j_1)(b_2,j_2)\cdots(b_m,j_m)]\\ &= f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)f_{j_1}(b_1)f_{j_2}(b_2)\cdots f_{j_m}(b_m)\\ &= [f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)][f_{j_1}(b_1)f_{j_2}(b_2)\cdots f_{j_m}(b_m)]\\ &= \Psi(\hat{a})\Psi(\hat{b})\end{aligned}$$

Caso (b) $i_n = j_1$**.** En este caso se tiene que

$$\begin{aligned}\Psi(\hat{a} * \hat{b}) &= \Psi[(a_1,i_1)(a_2,i_2)\cdots(a_nb_1,i_n)(b_2,j_2)\cdots(b_m,j_m)]\\ &= f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_nb_1)f_{j_2}(b_2)\cdots f_{j_m}(b_m)\\ &= f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)f_{j_1}(b_1)f_{j_2}(b_2)\cdots f_{j_m}(b_m)\\ &= [f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)][f_{j_1}(b_1)f_{j_2}(b_2)\cdots f_{j_m}(b_m)]\\ &= \Psi(\hat{a})\Psi(\hat{b})\end{aligned}$$

De lo anterior puede concluirse que Ψ es un morfismo de semigrupos. Más aún, si $i \in I$ y $a \in S_i$, entonces $\Psi(\sigma_i(a)) = \Psi(a,i) = f_i(a)$. Por lo tanto $f_i = \Psi \circ \sigma_i$ y para cada $i \in I$ el siguiente triángulo conmuta:



Suponga ahora que $\Psi' : Q \longrightarrow T$ es un morfismo de semigrupos tal que $f_i = \Psi' \circ \sigma_i$ para cada $i \in I$. Si $\hat{a} := (a_1,i_1)(a_2,i_2)\cdots(a_n,i_n) \in Q$ entonces

$$\begin{aligned}\Psi'(\hat{a}) &= \Psi'[(a_1, i_1)(a_2, i_2)\cdots(a_n, i_n)]\\ &= \Psi'[(a_1, i_1) * (a_2, i_2) * \cdots * (a_n, i_n)]\\ &= \Psi'(a_1, i_1)\Psi'(a_2, i_2)\cdots\Psi'(a_n, i_n)\\ &= \Psi'(\sigma_{i_1}(a_1))\Psi'(\sigma_{i_2}(a_2))\cdots\Psi'(\sigma_{i_n}(a_n))\\ &= f_{i_1}(a_1)f_{i_2}(a_2)\cdots f_{i_n}(a_n)\\ &= \Psi[(a_1, i_1)(a_2, i_2)\cdots(a_n, i_n)]\\ &= \Psi(\hat{a})\end{aligned}$$

De donde $\Psi' = \Psi$. Así, de acuerdo con la Definición 2.3.1 se sigue que $\bigsqcup_{i\in I} S_i := Q$ junto con la familia de morfismos de semigrupos $\{\sigma_i : S_i \longrightarrow Q\}_{i\in I}$ son un coproducto en $SGRP$ para la familia $(S_i)_{i\in I}$.

Proposición 5.1.4.

Toda familia no vacía de objetos de $SGRP$ tiene un coproducto.

Demostración. Se sigue de la discusión anterior. □

5.2. Monomorfismos, epimorfismos e isomorfismos en SGRP

Recuérdese que el Ejemplo 2.2.14 afirma que los monomorfismos en la categoría $Vec\mathbb{F}$ son precisamente las transformaciones lineales inyectivas. En la categoría de semigrupos $SGRP$ ocurre algo similar.

Proposición 5.2.1. *Monomorfismos en SGRP.*

El morfismo de semigrupos $f : S \longrightarrow T$ es un monomorfismo en $SGRP$ si y solo si f es una función inyectiva.

Demostración. $\Longrightarrow$) Suponga que $f : S \longrightarrow T$ es un monomorfismo en $SGRP$. De acuerdo con la Proposición 5.1.2 $Ker(f)$ es subsemigrupo de $S \times S$ y por lo tanto $Ker(f)$ es un semigrupo. Considere a las funciones $\alpha, \beta : Ker(f) \longrightarrow S$ definidas por $\alpha(x, y) := x$ y $\beta(x, y) := y$. Observe que para cada $(x, y), (w, z) \in Ker(f)$ se tiene lo siguiente:

$$\begin{aligned}\alpha[(x, y)(w, z)] &= \alpha(xw, yz)\\ &= xw\\ &= \alpha(x, y)\alpha(w, z)\end{aligned}$$

De ahí que α es un morfismo de semigrupos. De manera análoga se encuentra que β es un morfismo de semigrupos. Más aún, para cada $(x, y) \in Ker(f)$ se tiene que $f[\alpha(x, y)] = f(x) = f(y) = f[\beta(x, y)]$ y por consiguiente $f\circ\alpha = f\circ\beta$. Ahora bien, como f es, por hipótesis,

monomorfismo en $SGRP$ se sigue entonces que $\alpha = \beta$. Así, para cada $(x, y) \in Ker(f)$ se verifica que $\alpha(x, y) = \beta(x, y)$, de donde $x = y$ y por tanto $(x, y) \in \Delta_S$. De ahí que $Ker(f) \subseteq \Delta_S$ y por consiguiente $Ker(f) = \Delta_S$. De la Proposición 3.7.15 se concluye que f debe ser inyectiva.
$\Longleftarrow$) Suponga que f es inyectiva y sean R un semigrupo y $\alpha, \beta : R \longrightarrow S$ morfismos de semigrupos tales que $f \circ \alpha = f \circ \beta$. Como en particular R, S y T son conjuntos y α, β y f son funciones, entonces de la Proposición 1.4.10 se sigue que $\alpha = \beta$ y por consiguiente f debe ser un monomorfismo en $SGRP$. □

Por otro lado, el Ejemplo 2.2.17 afirma que los epimorfismos de la categoría de grupos GRP son precisamente los morfismos sobreyectivos de grupos. Sin embargo, en la categoría de semigrupos no todo epimorfismo es un morfismo sobreyectivo.

Ejemplo 5.2.2.

Defínase $\mathbb{N}^* := \mathbb{N} \cup \{0\}$ y considere a los semigrupos $(\mathbb{N}^*, +)$ y $(\mathbb{Z}, +)$. Sea $\iota : \mathbb{N}^* \longrightarrow \mathbb{Z}$ la función inclusión. Es claro que ι es un morfismo de semigrupos. Además, observe que ι no es una función sobreyectiva. Ahora bien, sean S un semigrupo y $\alpha, \beta : \mathbb{Z} \longrightarrow S$ morfismos de semigrupos tales que $\alpha \circ \iota = \beta \circ \iota$. **Afirmación 1):** $\alpha(\mathbb{Z})$ es un monoide con neutro $\alpha(0)$. En efecto, puesto que α es un morfismo de semigrupos, de la Proposición 3.7.10 se deduce que $\alpha(\mathbb{Z})$ es un subsemigrupo de S. Ahora bien, para cada $n \in \mathbb{Z}$ se tiene que $\alpha(n)\alpha(0) = \alpha(n + 0) = \alpha(n)$ y también $\alpha(0)\alpha(n) = \alpha(0 + n) = \alpha(n)$. Por consiguiente $\alpha(n)\alpha(0) = \alpha(n) = \alpha(0)\alpha(n)$ y $\alpha(\mathbb{Z})$ es un monoide con neutro $\alpha(0)$. De manera análoga se deduce que $\beta(\mathbb{Z})$ es un monoide con neutro $\beta(0)$. **Observación:** Como $\alpha \circ \iota = \beta \circ \iota$, entonces para cada $n \in \mathbb{N}^*$

$$\begin{aligned} \alpha(n) &= \alpha(\iota(n)) \\ &= \beta(\iota(n)) \\ &= \beta(n) \end{aligned}$$

En particular ha de ser que $\alpha(0) = \beta(0)$. **Afirmación 2):** $\alpha = \beta$. En efecto, en virtud de la observación anterior, para hacer ver que $\alpha = \beta$ solo resta mostrar que para cada $n \in \mathbb{Z}$ con $n < 0$ se tiene que $\alpha(n) = \beta(n)$. Sea $n \in \mathbb{N}$. Entonces $-n < 0$ y se tiene lo siguiente

$$\begin{aligned} \alpha(-n) &= \alpha(-n)\alpha(0) \\ &= \alpha(-n)\beta(0) \\ &= \alpha(-n)\beta(n + (-n)) \\ &= \alpha(-n)[\beta(n)\beta(-n)] \\ &= \alpha(-n)[\alpha(n)\beta(-n)] \\ &= [\alpha(-n)\alpha(n)]\beta(-n) \\ &= \alpha(-n + n)\beta(-n) \\ &= \alpha(0)\beta(-n) \\ &= \beta(0)\beta(-n) \\ &= \beta(-n) \end{aligned}$$

De lo anterior se sigue que, en definitiva, $\alpha = \beta$. Esto último permite concluir que $\iota : \mathbb{N}^* \longrightarrow \mathbb{Z}$ es un epimorfismo en $SGRP$ que no es sobreyectivo •

A pesar de lo anterior, si se verifica lo siguiente.

Proposición 5.2.3.

Todo morfismo sobreyectivo de semigrupos es un epimorfismo en la categoría $SGRP$.

Demostración. Sea $f : S \longrightarrow T$ un morfismo sobreyectivo de semigrupos. Tómense un semigrupo arbitrario, digamos R, y un par de morfismos de semigrupos $\alpha, \beta : T \longrightarrow R$ tales que $\alpha \circ f = \beta \circ f$. Si $t \in T$, de la sobreyectividad de f puede escribirse $t = f(s)$ para algún $s \in S$. Así, $\alpha(t) = \alpha(f(s)) = \beta(f(s)) = \beta(t)$ y por consiguiente $\alpha = \beta$. En consecuencia, f es un epimorfismo en $SGRP$. □

Después de todo lo anterior, se puede decir que en $SGRP$ todo morfismo sobreyectivo es un epimorfismo, pero no todo epimorfismo es un morfismo sobreyectivo. Por lo tanto, a diferencia de la categoría GRP, en la categoría $SGRP$ no pueden caracterizarse a los epimorfismos de ésta. Sin embargo, una caracterización para los epimorfismos de cierta subcategoría de $SGRP$ si puede llevarse a cabo. Las siguientes líneas tienen por objetivo mostrar tal caracterización. Para tal fin se introducen las siguientes definiciones.

Definición 5.2.4.

Sea S un semigrupo. Se dice que $a \in S$ es

1. **cancelable a la izquierda** si para cada $x, y \in S$ se verifica que

$$ax = ay \Longrightarrow x = y$$

2. **cancelable a la derecha** si para cada $x, y \in S$ se verifica que

$$xa = ya \Longrightarrow x = y$$

3. **cancelable** si a es a la vez cancelable a la izquierda y a la derecha •

Definición 5.2.5.

Se dice que el semigrupo S es

1. **cancelable a la izquierda** si todo elemento de S es cancelable a la izquierda.

2. **cancelable a la derecha** si todo elemento de S es cancelable a la derecha.

3. **cancelable** si todo elemento de S es cancelable •

Ejemplos 5.2.6.

- Todo grupo es cancelable.
- El monoide $(\mathbb{N}^*, +)$ es cancelable •

En lo que sigue, $\mathcal{O}$ denotará a la clase de todos los monoides conmutativos y cancelables. Para cada $M, N \in \mathcal{O}$ se define

$$Hom_{MCC}(M, N) := \{f : M \longrightarrow N \mid f \text{ es morfismo de monoides}\}$$

No es difícil ver que lo anterior forma una subcategoría de $SGRP$ a la que se denotará por MCC. Tómese $M \in \mathcal{O}$. Sobre el monoide producto $M \times M$ se define la siguiente relación:

$$(a, b)\rho(c, d) \Longleftrightarrow ad = bc$$

Afirmación (1): ρ es una equivalencia sobre $M \times M$. En efecto, como M es conmutativo, entonces para cada $(a, b) \in M \times M$ se tiene que $ab = ba$. Luego $(a, b)\rho(a, b)$ y ρ es reflexiva. Suponga ahora que $(a, b)\rho(c, d)$. Entonces $ad = bc$, o lo que es lo mismo $cb = da$. De ahí que $(c, d)\rho(a, b)$ y por consiguiente ρ es simétrica. Finalmente, suponga que $(a, b)\rho(c, d)$ y $(c, d)\rho(e, f)$. Entonces $ad = bc$ y $cf = de$, o lo que es lo mismo $ad = bc$ y $de = fc$. De la igualdad $ad = bc$ se obtiene que $ade = bce$, y puesto que $de = fc$ se obtiene así que $afc = bce = bec$. De esta última igualdad y de que M es cancelable se sigue que $af = be$. Por lo tanto $(a, b)\rho(e, f)$ y ρ es transitiva. Por consiguiente ρ es una equivalencia sobre $M \times M$. **Afirmación (2):** ρ es una congruencia sobre $M \times M$. En primer lugar, observar que de la conmutatividad de M y de que la operación en el monoide producto se lleva a cabo entrada a entrada se sigue que $M \times M$ es también conmutativo. Debido a esto, solo bastará mostrar que ρ es una congruencia izquierda. Suponga que $(a, b)\rho(c, d)$ y sea $(x, y) \in M \times M$ arbitrario. Entonces $ad = bc$, de donde $xyad = xybc$. Así, asociando y conmutando convenientemente se llega a que $xayd = ybxc$. De ahí que $(x, y)(a, b)\rho(x, y)(c, d)$ y por consiguiente ρ es una congruencia. Una vez que se han establecido estas afirmaciones se puede concluir que si e_M es el elemento neutro de M, entonces $\frac{M\times M}{\rho}$ es un monoide con neutro $[(e_M, e_M)]_\rho$ (ver Proposición 3.6.10). **Observaciones:**

1. $\frac{M\times M}{\rho}$ es un monoide conmutativo.
2. Para cada $a \in M$ se verifica que $(a, a)\rho(e_M, e_M)$ y por tanto $[(a, a)]_\rho = [(e_M, e_M)]_\rho$.
3. $[(a, b)]_\rho[(b, a)]_\rho = [(e_M, e_M)]_\rho$

La primera observación se deduce de la conmutatividad de $M \times M$. La segunda, se sigue de notar que siempre se verifica la identidad $ae_M = ae_M$. Ahora bien, para cada $(a, b) \in M \times M$ se tiene que:

$$[(a,b)]_\rho[(b,a)]_\rho = [(a,b)(b,a)]_\rho = [(ab,ba)]_\rho = [(ab,ab)]_\rho = [(e_M,e_M)]_\rho$$

De donde la última observación se sigue. ¿Qué se puede concluir de esto?. Note que de las observaciones 1 y 3 se concluye que $\frac{M\times M}{\rho}$ es entonces un grupo conmutativo. Se denotará a este grupo por $\mathcal{G}(M)$ y se le llamará **grupo de Grothendieck** del monoide M. Considere ahora a la función $\eta : M \longrightarrow \mathcal{G}(\mathcal{M})$ definida por $\eta(a) := [(a,e_M)]_\rho$. Si $a,b \in M$ son tales que $\eta(a) = \eta(b)$ entonces $[(a,e_M)]_\rho = [(b,e_M)]_\rho$ de donde $(a,e_M)\rho(b,e_M)$. Luego $ae_M = e_Mb$ y así $a = b$. Por consiguiente η es una función inyectiva. Más aún, observe que

$$\begin{aligned}\eta(ab) :&= [(ab,e_M)]_\rho \\ &= [(a,e_M)(b,e_M)]_\rho \\ &= [(a,e_M)]_\rho[(b,e_M)]_\rho \\ &= \eta(a)\eta(b)\end{aligned}$$

De donde η es un morfismo inyectivo de monoides. Así, de la Proposición 3.7.17 se sigue que M es isomorfo a un submonoide de $\mathcal{G}(M)$. Llamaremos al morfismo η la **inmersión de M en $\mathcal{G}(M)$**. A modo de síntesis y de conclusión se tiene la siguiente proposición.

Proposición 5.2.7.

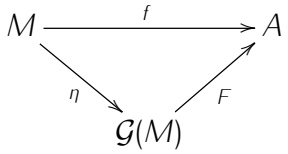
Todo monoide conmutativo y cancelable se *sumerge* en un grupo conmutativo.

Demostración. Directa de la discusión anterior. □

El grupo de Grothendieck de M y el morfismo $\eta : M \longrightarrow \mathcal{G}(\mathcal{M})$ tienen la siguiente propiedad.

Proposición 5.2.8.

Para cada grupo conmutativo A y cada morfismo de monoides $f : M \longrightarrow A$ con $M \in \mathcal{O}$ existe un único morfismo de grupos $F : \mathcal{G}(M) \longrightarrow A$ que hace conmutar al siguiente triángulo



Demostración. Sean A un grupo conmutativo y $f : M \longrightarrow A$ un morfismo de monoides. Se

define a $F : \mathcal{G}(M) \longrightarrow A$ como $F([(a,b)]_\rho) := f(a)f(b)^{-1}$. Veamos que F está bien definida:

$$\begin{aligned} & [(a,b)]_\rho = [(c,d)]_\rho \\ \Longrightarrow \quad & (a,b)\rho(c,d) \\ \Longrightarrow \quad & ad = bc \\ \Longrightarrow \quad & f(ad) = f(bc) \\ \Longrightarrow \quad & f(a)f(d) = f(b)f(c) \\ \Longrightarrow \quad & f(a)f(b)^{-1} = f(c)f(d)^{-1} \\ \Longrightarrow \quad & F([(a,b)]_\rho) = F([(c,d)]_\rho) \end{aligned}$$

Ahora, veamos que F es un morfismo de grupos:

$$\begin{aligned} F([(a,b)]_\rho[(c,d)]_\rho) &= F([(ac,bd)]_\rho) \\ &= f(ac)f(bd)^{-1} \\ &= f(a)f(c)f(b)^{-1}f(d)^{-1} \\ &= (f(a)f(b)^{-1})(f(c)f(d)^{-1}) \\ &= F([(a,b)]_\rho)F([(c,d)]_\rho) \end{aligned}$$

Más aún, para cada $a \in M$ se tiene que

$$F(\eta(a)) = F([(a,e_M)]_\rho) = f(a)f(e_M)^{-1} = f(a)e_A = f(a).$$

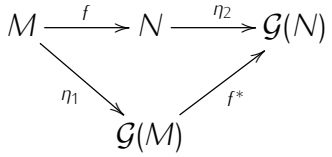
Por consiguiente $f = F \circ \eta$. Suponga ahora que $F' : \mathcal{G}(M) \longrightarrow A$ es un morfismo de grupos para el cual $f = F' \circ \eta$. Entonces

$$\begin{aligned} F'([(a,b)]_\rho) &= F'([(a,e_M)(e_M,b)]_\rho) \\ &= F'([(a,e_M)]_\rho[(e_M,b)]_\rho) \\ &= F'([(a,e_M)]_\rho)F'([(e_M,b)]_\rho) \\ &= F'([(a,e_M)]_\rho)F'([(b,e_M)]_\rho^{-1}) \\ &= F'([(a,e_M)]_\rho)F'([(b,e_M)]_\rho)^{-1} \\ &= F'(\eta(a))F'(\eta(b))^{-1} \\ &= f(a)f(b)^{-1} \\ &= F([(a,b)]_\rho) \end{aligned}$$

Se concluye de esto último que $F' = F$ y el resultado se sigue. □

Nota: En lo posterior, se denorará a la clase de equivalencia de (a,b) por $[(a,b)]$ en lugar de $[(a,b)]_\rho$ i,e, prescindiremos del subíndice ρ (Véase la definición de ρ en la página 100).

Tómense $M, N \in \mathcal{O}$ y sean $\eta_1 : M \longrightarrow \mathcal{G}(M)$ y $\eta_2 : N \longrightarrow \mathcal{G}(N)$ las inmersiones de cada monoide en su respectivo grupo de Grothendieck. Supóngase ahora que $f : M \longrightarrow N$ es un morfismo de monoides. De la Proposición 5.2.8 se deduce que existe un único morfismo de grupos $f^* : \mathcal{G}(M) \longrightarrow \mathcal{G}(N)$ que hace conmutar al siguiente triángulo



O lo que es lo mismo, tal que $f^* \circ \eta_1 = \eta_2 \circ f$. Más aún, para cada $[(a,b)] \in \mathcal{G}(M)$ de la prueba de la Proposición 5.2.8 se tiene que

$$\begin{aligned} f^*([(a,b)]) &:= (\eta_2 \circ f)(a)(\eta_2 \circ f)(b)^{-1} \\ &= \eta_2(f(a))\eta_2(f(b))^{-1} \\ &= [(f(a), e_N)][(f(b), e_N)]^{-1} \\ &= [(f(a), e_N)][(e_N, f(b))] \\ &= [(f(a), f(b))] \end{aligned}$$

Con esto, se tiene una manera de asignarle a cada morfismo de MCC, digamos f, un morfismo de Ab, a saber, el morfismo f^*.

Proposición 5.2.9.

1. Si $M \xrightarrow{f} N \xrightarrow{g} T$ son morfismos de MCC, entonces $(g \circ f)^* = g^* \circ f^*$.
2. Para cada $M \in \mathcal{O}$ se tiene que $id_M^* = id_{\mathcal{G}(M)}$.
3. Si $f : M \longrightarrow N$ es un epimorfismo en MCC, entonces f^* es un epimorfismo en Ab.

Demostración. 1) Si $[(a,b)] \in \mathcal{G}(M)$, entonces

$$\begin{aligned} (g \circ f)^*([(a,b)]) &= [((g \circ f)(a), (g \circ f)(b))] \\ &= [(g(f(a)), g(f(b)))] \\ &= g^*([(f(a), f(b))]) \\ &= g^*(f^*([(a,b)])) \\ &= (g^* \circ f^*)([(a,b)]) \end{aligned}$$

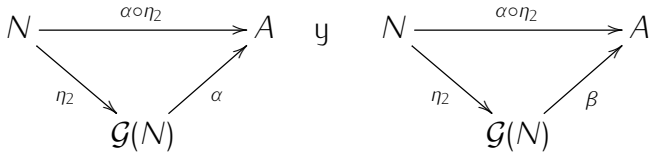
Por consiguiente $(g \circ f)^* = g^* \circ f^*$.

2) Sea $M \in \mathcal{O}$ y $[(a,b)] \in \mathcal{G}(M)$. Entonces $id_M^*([(a,b)]) = [(id_M(a), id_M(b))] = [(a,b)] = id_{\mathcal{G}(M)}([(a,b)])$. Por lo tanto $id_M^* = id_{\mathcal{G}(M)}$.

3) Suponga que $f : M \longrightarrow N$ es un epimorfismo de la categoría MCC. Sean A un grupo conmutativo y $\alpha, \beta : \mathcal{G}(N) \longrightarrow A$ un par de morfismos de grupos tales que $\alpha \circ f^* = \beta \circ f^*$. Como $f^* \circ \eta_1 = \eta_2 \circ f$, entonces

$$\begin{aligned} (\alpha \circ f^*) \circ \eta_1 &= (\beta \circ f^*) \circ \eta_1 \\ \Longrightarrow \alpha \circ (f^* \circ \eta_1) &= \beta \circ (f^* \circ \eta_1) \\ \Longrightarrow \alpha \circ (\eta_2 \circ f) &= \beta \circ (\eta_2 \circ f) \\ \Longrightarrow (\alpha \circ \eta_2) \circ f &= (\beta \circ \eta_2) \circ f \end{aligned}$$

Ahora bien, observe que como todo grupo es cancelable y todo morfismo de grupos es, en particular, un morfismo de monoides, se deduce entonces que $\alpha \circ \eta_2$ y $\beta \circ \eta_2$ son ambos morfismos de MCC. Así, de la igualdad $(\alpha \circ \eta_2) \circ f = (\beta \circ \eta_2) \circ f$ y de que f es, por hipótesis, un epimorfismo en MCC, se sigue que $\alpha \circ \eta_2 = \beta \circ \eta_2$. De esto último se concluye que los siguientes triángulos son conmutativos



La Proposición 5.2.8 permite concluir que $\alpha = \beta$. Así, $f^* : \mathcal{G}(M) \longrightarrow \mathcal{G}(N)$ es un epimorfismo en Ab.

□

Corolario 5.2.10.

Se define $\mathcal{T} : MCC \longrightarrow Ab$ como sigue:

- Si M es un objeto de MCC, $\mathcal{T}(M) := \mathcal{G}(M)$.
- Si $f : M \longrightarrow N$ es un morfismo de MCC, $\mathcal{T}(f) := f^*$.

Entonces $\mathcal{T} : MCC \longrightarrow Ab$ es un funtor que transforma epimorfismos en epimorfismos.

Demostración. Directa de la Proposición 5.2.9. □

Recordar que anteriormente se mencionó que se llevaría a cabo una caracterización para los epimorfismos de cierta subcategoría de $SGRP$. Tal subcategoría resulta ser MCC. Hasta este punto se tiene casi todo listo para realizar dicha tarea. Solo falta establecer lo siguiente.

Proposición 5.2.11. *Epimorfismos en Ab.*

Sea $f : A \longrightarrow B$ un morfismo de grupos abelianos. Entonces, f es un epimorfismo en Ab si y solo si f es una función sobreyectiva.

Demostración. $\Longrightarrow$) Suponga que $f : A \longrightarrow B$ es un epimorfismo de Ab. Puesto que todos los grupos involucrados son conmutativos, se sigue que $Im(f) \triangleleft B$. Así, puede considerarse al grupo cociente $\frac{B}{Im(f)}$ el cual también es conmutativo. Sea $\pi : B \longrightarrow \frac{B}{Im(f)}$ el morfismo proyección canónica y sea $\alpha : B \longrightarrow \frac{B}{Im(f)}$ dada por $\alpha(b) := Im(f)$. No es difícil ver que α es un morfismo de grupos. Por otra parte, observar que para cada $x \in A$ se tiene que $\pi(f(x)) = (Im(f))f(x) = Im(f) = \alpha(f(x))$ y por consiguiente $\pi \circ f = \alpha \circ f$. Así que como f es epimorfismo en Ab debe ser que $\pi = \alpha$. Sea $b \in B$. Entonces $\pi(b) = \alpha(b)$, o lo que es lo mismo $(Im(f))b = Im(f)$. De ahí que $b \in Im(f)$. Por consiguiente $B = Im(f)$ y f es sobreyectiva.
$\Longleftarrow$) Es similar a la prueba de la Proposición 5.2.3 y por eso se omite. □

Observación 5.2.12.

En comparación con el Ejemplo 2.2.17, la prueba para los epimorfismos en Ab es mucho más sencilla •

A continuación, se caracterizan a los epimorfismos de MCC.

Proposición 5.2.13. *Epimorfismos en MCC.*

Sea $f : M \longrightarrow N$ un morfismo de MCC. Entonces, f es un epimorfismo en MCC si y solo si para cada $n \in N$ existen $a, b \in M$ tales que $nf(b) = f(a)$.

Demostración. $\Longrightarrow$) Suponga que $f : M \longrightarrow N$ es un epimorfismo de MCC. Entonces, $f^* : \mathcal{G}(M) \longrightarrow \mathcal{G}(N)$ es un epimorfismo en Ab. De la Proposición 5.2.11 se deduce que f^* debe ser una función sobreyectiva. Así, para $n \in N$ y $[(n, e_N)] \in \mathcal{G}(N)$ existe $[(a, b)] \in \mathcal{G}(M)$ tal que $[(n, e_N)] = f^*([(a, b)]) = [(f(a), f(b))]$. De ahí que $(n, e_N)\rho(f(a), f(b))$ y por consiguiente $nf(b) = e_N f(a) = f(a)$.
$\Longleftarrow$) Suponga que para cada $n \in N$ existen $a, b \in M$ tales que $nf(b) = f(a)$ y sean $\alpha, \beta : N \longrightarrow T$ un par de morfismos de MCC tales que $\alpha \circ f = \beta \circ f$. Tómese $n \in N$. Entonces, existen $a, b \in M$ para los cuales $nf(b) = f(a)$.
De esta igualdad se desprende que $\alpha(n)\alpha(f(b)) = \alpha(nf(b)) = \alpha(f(a))$. De ahí que

$$\begin{aligned}\alpha(n)\alpha(f(b)) &= \alpha(f(a)) \\ &= \beta(f(a)) \\ &= \beta(nf(b)) \\ &= \beta(n)\beta(f(b)) \\ &= \beta(n)\alpha(f(b))\end{aligned}$$

Ahora bien, puesto que T es un monoide cancelable se sigue entonces que $\alpha(n) = \beta(n)$ y por consiguiente $\alpha = \beta$. En consecuencia, f es un epimorfismo en MCC.

□

Se finaliza esta subsección determinando a los isomorfismos de $SGRP$.

Proposición 5.2.14. *Isomorfismos en SGRP.*

El morfismo de semigrupos $f : S \longrightarrow T$ es un isomorfismo en $SGRP$ si y solo si f es una función biyectiva.

Demostración. $\Longrightarrow$) Suponga que f es un isomorfismo en $SGRP$. Luego, debe existir un morfismo en $SGRP$, digamos $g : T \longrightarrow S$, tal que $g \circ f = id_S$ y $f \circ g = id_T$. De esto último y debido a que f y g son en particular funciones, se puede concluir que f debe ser biyectiva.

$\Longleftarrow$) Suponga que $f : S \longrightarrow T$ es un morfismo biyectivo de semigrupos. De la Proposición 1.4.18 se sigue que f tiene una única función inversa, digamos $g : T \longrightarrow S$, y de la Proposición 3.7.6 se deduce que g es un morfismo de semigrupos i,e, un morfismo de $SGRP$. Así, como $g \circ f = id_S$ y $f \circ g = id_T$ se puede concluir que f es un isomorfismo en $SGRP$. □

5.3. Objetos libres

Sea $\mathcal{U} : SGRP \longrightarrow SET$ el funtor olvidadizo (ver Ejemplos 2.4.4). Como tal funtor es un funtor fiel, se sigue entonces que el par $(SGRP, \mathcal{U})$ es una categoría concreta sobre SET (ver Definición 2.5.1). Además, en este caso, para cada semigrupo S y cada morfismo de semigrupos f se tiene que $|S| = S$ y $|f| = f$ (véase Observación 2.5.2). Se aprovecha la información obtenida sobre semigrupos libres para establecer lo siguiente.

Proposición 5.3.1.

Para cada conjunto $X \neq \emptyset$, el par (ι, X^+) donde $\iota : X \longrightarrow X^+$ es la inclusión, es un morfismo universal sobre X (ver Definición 2.5.4).

Demostración. Primero, ver la Definición 4.0.8 y luego la Proposición 4.0.9. □

Corolario 5.3.2.

Si $X \neq \emptyset$ es un conjunto, entonces el semigrupo libre X^+ es un objeto libre sobre X •

En conclusión, en la categoría concreta $(SGRP, \mathcal{U})$, todo semigrupo libre es un objeto libre sobre su base.

5.4. Observación final

Recordar que las Observaciones 2.2.18 y 2.2.19 afirman que las categorías SET y $Vec\mathbb{F}$ tienen la propiedad de que si A y B son dos objetos tales que existe un monomorfismo de A en B y un monomorfismo de B en A entonces $A \cong B$. ¿Será cierto que la categoría de semigrupos $SGRP$ también cuenta con tal atributo?. La respuesta a esta interrogante es negativa y para establecerla haremos uso de los semigrupos libres.

Proposición 5.4.1.

Sean $X, Y \neq \emptyset$ dos conjuntos y considere a los semigrupos libres X^+ y Y^+. Suponga que $f : X \longrightarrow Y^+$ es una función inyectiva tal que para cada $x \in X$ se verifica que $f(x) \in Y^+$ es una palabra de longitud k i,e, f transforma palabras de longitud 1 en palabras de longitud k. Entonces, el morfismo de semigrupos $\phi : X^+ \longrightarrow Y^+$ que garantiza la Proposición 4.0.9 debe ser una función inyectiva.

Demostración. Recordar que el morfismo $\phi : X^+ \longrightarrow Y^+$ que garantiza la Proposición 4.0.9 está dado por $\phi(x_1x_2 \cdots x_n) := f(x_1)f(x_2) \cdots f(x_n)$. Sean $a_1a_2 \cdots a_n$ y $b_1b_2 \cdots b_m$ dos palabras de longitud n y m en X^+ tales que

$$\phi(a_1a_2 \cdots a_n) = \phi(b_1b_2 \cdots b_m)$$

Luego,

$$f(a_1)f(a_2) \cdots f(a_n) = f(b_1)f(b_2) \cdots f(b_m) \tag{5.1}$$

Puesto que f transforma palabras de longitud 1 en palabras de longitud k entonces el primer miembro de la igualdad (5.1) es la concatenación de n palabras de longitud k y el segundo miembro de (5.1) es la concatenación de m palabras de longitud k. De esto último y de la igualdad entre palabras se sigue que $kn = km$ y por consiguiente $n = m$. Ahora bien, para cada $i \in \{1, 2, ..., n\}$ puede escribirse

$$f(a_i) = u_{i1}u_{i2} \cdots u_{ik} \quad \text{y} \quad f(b_i) = v_{i1}v_{i2} \cdots v_{ik}$$

Donde $u_{ij}, v_{ij} \in Y$. Así, la igualdad (5.1) toma la forma

$$u_{11}u_{12} \cdots u_{1k} \cdots u_{n1}u_{n2} \cdots u_{nk} = v_{11}v_{12} \cdots v_{1k} \cdots v_{n1}v_{n2} \cdots v_{nk}$$

De manera que de la igualdad entre palabras se deduce que $u_{ij} = v_{ij}$ para cada $i \in \{1, 2, ..., n\}$ y cada $j \in \{1, 2, ..., k\}$. Por consiguiente, para cada $i \in \{1, 2, ..., n\}$ se tiene que $f(a_i) = f(b_i)$, y dado que f es inyectiva, entonces $a_i = b_i$ para cada $i \in \{1, 2, ..., n\}$ y en consecuencia $a_1a_2 \cdots a_n = b_1b_2 \cdots b_m$. Por consiguiente ϕ debe ser inyectiva.

□

Proposición 5.4.2.

Existe un par de semigrupos no isomorfos A y B para los cuales hay un monomorfismo de A en B y un monomorfismo de B en A.

Demostración. Considere a los conjuntos $X := \{a, b\}$ y $Y := \{a, b, c\}$ de dos y tres elementos respectivamente y también a las funciones $f : X \longrightarrow Y^+$ y $g : Y \longrightarrow X^+$ definidas por

$$f(x) := \begin{cases} a & si \quad x = a. \\ b & si \quad x = b. \end{cases}$$

y

$$g(y) := \begin{cases} aa & si \quad y = a. \\ bb & si \quad y = b. \\ ab & si \quad y = c. \end{cases}$$

No es difícil ver que ambas funciones son inyectivas, y además, de su definición se aprecia que f transforma palabras de longitud 1 en palabras de longitud 1 y g transforma palabras de longitud 1 en palabras de longitud 2. Por lo tanto, de la Proposición 5.4.1 se sigue que existen morfismos inyectivos de semigrupos $\phi : X^+ \longrightarrow Y^+$ y $\psi : Y^+ \longrightarrow X^+$. Ahora bien, como en la categoría $SGRP$ monomorfismo equivale a morfismo inyectivo (ver Proposición 5.2.1) se sigue entonces que ϕ y ψ son ambos monomorfismos. Finalmente, observe que X^+ y Y^+ no son isomorfos, pues X y Y no son equipotentes (véase Proposición 4.0.19). □

.

Capítulo 6

Bandas rectangulares

En este capítulo se introduce a un tipo especial de semigrupos a los que se les dará el nombre de bandas rectangulares. Se empieza dando una definición general de ellos para, posteriormente, ofrecer otras definiciones equivalentes.

Definición 6.0.1.

Se dice que el semigrupo S es una **banda rectangular** si para cada $a, b \in S$ se verifica que $aba = a$ •

Ejemplos 6.0.2.

- Tómense dos conjuntos no vacíos A y B y sobre el producto cartesiano $A \times B$ defínase la siguiente operación entre pares ordenados:

  $$(a, b)(c, d) := (a, d)$$

  Observe que

  $$\begin{aligned}(a, b)[(c, d)(e, f)] &= (a, b)(c, f)\\ &= (a, f)\\ &= (a, d)(c, f)\\ &= [(a, b)(c, d)](e, f)\end{aligned}$$

  Por lo tanto, esta operación es asociativa y $A \times B$ es entonces un semigrupo bajo tal operación. Más aún, $(a, b)(c, d)(a, b) = (a, b)(c, b) = (a, b)$. Por consiguiente $A \times B$ es una banda rectangular.

- Sea $X \neq \emptyset$ un conjunto y para cada $a, b \in X$ sea $ab := a$. Según el Ejemplo 3.4.2, X es un semigrupo bajo esta operación, y además, $aba = a(ba) = ab = a$. En consecuencia X es una banda rectangular •

Observación 6.0.3.

Los dos ejemplos anteriores proporcionan una forma de obtener bandas rectangulares a partir de conjuntos no vacíos dados •

Proposición 6.0.4.

Si S es una banda rectangular, entonces para cada $a \in S$, $a^2 = a$.

Demostración. Se tiene que $a = aa^3a = a^5$ y también $a^2 = a^2aa^2 = a^5$, luego $a^2 = a$. □

Una forma equivalente de definir a una banda rectangular viene dada en la siguiente proposición.

Proposición 6.0.5.

Los siguientes enunciados son equivalentes para un semigrupo S.

1. S es una banda rectangular.
2. Para cada $a, b \in S$, $ab = ba \Longrightarrow a = b$.

Demostración. 1) $\Longrightarrow$ 2) Suponga que $ab = ba$. De esta igualdad se desprende que $aba = ba^2$ y $bab = b^2a$. Ahora bien, de que S es una banda rectangular junto con la Proposición 6.0.4, permite concluir que el último par de igualdades toma la forma $a = ba$ y $b = ba$. Por consiguiente $a = b$.

2) $\Longrightarrow$ 1) Observe que $a^2a = aa^2$. Por lo tanto $a^2 = a$ para cada $a \in S$. De ahí que $(aba)a = aba^2 = aba = a^2ba = a(aba)$. Por consiguiente $aba = a$ y S es una banda rectangular.

□

Observación 6.0.6.

La segunda parte de este resultado será de utilidad cuando se pretenda exhibir que dos elementos de una banda rectangular son iguales, pues solo bastará con mostrar que dichos elementos conmutan •

Recuerde que el centro de un grupo (o un anillo) es definido como la colección de todos aquellos elementos del grupo (o anillo) que conmutan con cualquier elemento del grupo (o anillo). Siguiendo esta idea, también puede definirse al centro de un semigrupo.

Definición 6.0.7.

Se define el **centro** de un semigrupo S como sigue:

$$Z(S) := \{a \in S \mid ab = ba \text{ para cada } b \in S\}$$

Además, para cada $a \in S$ al conjunto

$$C(a) := \{b \in S \mid ab = ba\}$$

se le llama **centralizador** de a •

Observe que con estas definiciones la Proposición 6.0.5 puede ser enunciada como sigue:

Proposición 6.0.8.

Los siguientes enunciados son equivalentes para un semigrupo S.

1. S es una banda rectangular.
2. Para cada $a \in S$, $C(a) = \{a\}$ •

Corolario 6.0.9.

Sea S una banda rectangular. Si $Z(S) \neq \emptyset$, entonces S tiene exactamente un elemento.

Demostración. Tómese $k \in Z(S)$ y sea $a \in S$ arbitrario. Como $ka = ak$, entonces $a \in C(k) = \{k\}$. Así $a = k$. De ahí que $S = \{k\}$. □

Del Corolario anterior se ve que cualquier banda rectangular con más de un elemento debe tener centro vacío. Así, a diferencia de los grupos, un semigrupo puede tener centro vacío. Sin embargo, cuando el centro de un semigrupo tiene al menos un elemento sucede lo siguiente.

Proposición 6.0.10.

Sea S un semigrupo.

- Si $Z(S) \neq \emptyset$, entonces $Z(S)$ es un subsemigrupo de S.
- Para cada $a \in S$, $C(a)$ es un subsemigrupo de S.

Demostración. Tómense $z_1, z_2 \in Z(S)$. Entonces, para cada $a \in S$ se tiene que $a(z_1z_2) = (az_1)z_2 = (z_1a)z_2 = z_1(az_2) = z_1(z_2a) = (z_1z_2)a$. De ahí que $z_1z_2 \in Z(S)$ y por consiguiente $Z(S)$ es subsemigrupo de S. El argumento para ver que $C(a)$ es siempre subsemigrupo de S es similar al anterior y se omite. □

Ahora bien, regresando al tema de las bandas rectangulares, resulta que todo semigrupo isomorfo a una banda rectangular debe ser también una banda rectangular.

Proposición 6.0.11.

Suponga que S y T son dos semigrupos tales que $S \cong T$. Si S es una banda rectangular, entonces T es una banda rectangular.

Demostración. Sea $f : S \longrightarrow T$ un isomorfismo de semigrupos y $x, y \in T$. Puede escribirse $x = f(a)$ y $y = f(b)$ para algunos $a, b \in S$. Así que $xyx = f(a)f(b)f(a) = f(aba) = f(a) = x$. Por consiguiente T es una banda rectangular. □

A continuación se enuncian algunas propiedades adicionales de las bandas rectangulares.

Proposición 6.0.12.

Sea S una banda rectangular y $a \in S$ fijo. Entonces para cualesquiera $x, y \in S$ se verifican las siguientes igualdades

1. $xaya = xa$
2. $axay = ay$
3. $xya = xa$
4. $axy = ay$

Demostración. 1) Puesto que $a = aya$, se tiene entonces que $xa = xaya$.
4) Bastará con mostrar que axy conmuta con ay: observe que $(axy)(ay) = ax(yay) = axy$ mientras que $(ay)(axy) = (aya)xy = axy$. Por consiguiente $(axy)(ay) = (ay)(axy)$. Las dos identidades restantes se exhiben de manera similar. □

El primero de los Ejemplos 6.0.2 afirma que el producto cartesiano de dos conjuntos no vacíos junto con la operación que ahí se define da lugar a una banda rectangular. Resulta interesante el hecho de que toda banda rectangular es isomorfa a algún semigrupo construido de esta forma.

Proposición 6.0.13.

Si S es una banda rectangular, entonces existen conjuntos no vacíos A y B tales que $S \cong A \times B$, donde $A \times B$ es un semigrupo construido como aparece en el primero de los Ejemplos 6.0.2.

Demostración. Tómese $a \in S$ y fíjelo. Considere ahora al conjunto $S_a := \{(xa, ax) \mid x \in S\}$. Sobre este conjunto se define la siguiente operación binaria:

$$(xa, ax)(ya, ay) := (xya, axy)$$

Se tiene entonces que

$$\begin{aligned}(xa, ax)[(ya, ay)(za, az)] &= (xa, ax)(yza, ayz)\\ &= (xyza, axyz)\\ &= (xya, axy)(za, az)\\ &= [(xa, ax)(ya, ay)](za, az)\end{aligned}$$

Por lo tanto S_a es un semigrupo bajo esta operación. Ahora, sea $f : S \longrightarrow S_a$ la función definida por $f(x) := (xa, ax)$. Observe que

$$\begin{aligned} f(xy) &= (xya, axy) \\ &= (xa, ax)(ya, ay) \\ &= f(x)f(y) \end{aligned}$$

Así, f es un morfismo de semigrupos. De la definición de f queda claro que f es sobreyectiva. Más aún, si $f(x) = f(y)$, entonces $(xa, ax) = (ya, ay)$, de donde $xa = ya$ y $ax = ay$. Luego $x = xax = yax$ y $y = yay = yax$. De ahí que $x = y$ y por lo tanto f es inyectiva. Se sigue entonces que f es un isomorfismo y por consiguiente $S \cong S_a$. Considere a los conjuntos $A := \{xa \mid x \in S\}$ y $B := \{ay \mid y \in S\}$. **Afirmación:** $S_a = A \times B$. En efecto, es claro que $S_a \subseteq A \times B$. Sea $(xa, ay) \in A \times B$ y considere al elemento $z := xay$. De las igualdades 1) y 2) que aparecen en la Proposición 6.0.12 se sigue que $xa = za$ y $ay = az$. Así, $(xa, ay) = (za, az) \in S_a$ y por consiguiente $A \times B \subseteq S_a$. En definitiva $S_a = A \times B$. Finalmente, de las igualdades 3) y 4) que aparecen en la Proposición 6.0.12, se deduce que $(xa, ax)(ya, ay) := (xya, axy) = (xa, ay)$. Por consiguiente S_a es un semigrupo construido como en el primero de los Ejemplos 6.0.2.

□

Proposición 6.0.14.

Los siguientes enunciados son equivalentes.

1. S es una banda rectangular.
2. S es isomorfo a algún semigrupo de la forma $A \times B$ con operación binaria dada por $(a, b)(c, d) := (a, d)$.

Demostración. 1) $\Longrightarrow$ 2) Es la Proposición 6.0.13.
2) $\Longrightarrow$ 1) Puesto que todo semigrupo de la forma $A \times B$ con operación binaria dada por $(a, b)(c, d) := (a, d)$ es una banda rectangular, se sigue de la Proposición 6.0.11 que cualquier semigrupo isomorfo a alguno de este tipo es también una banda rectangular. □

.

Capítulo 7

Semigrupos regulares

En este capítulo se introduce a los semigrupos regulares, que incluyen a las bandas rectangulares del capítulo anterior y a otro tipo de semigrupos más generales que estos últimos. Cabe mencionar que gran parte de este trabajo de tesis se enfoca en estudiar propiedades de algunos tipos de semigrupos que resultan ser semigrupos regulares, de manera que comprender el contenido del presente capítulo resulta ser de suma importancia.

7.1. Idempotentes

Considere al monoide $M_2(\mathbb{Z})$ de la Observación 3.7.2. Note que las siguientes matrices verifican que $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$; $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ i,e, cada una de estas matrices es igual a su cuadrado. En general, a cada elemento de un semigrupo que cumpla con esta propiedad se le dará el nombre de idempotente. Los idempotentes de un semigrupo jugarán un papel importante dentro de la teoría de semigrupos regulares.

Definición 7.1.1.

Sea S un semigrupo. Decimos que $\alpha \in S$ es **idempotente** si $\alpha^2 = \alpha$. Además, denotamos por $E(S)$ a la colección de todos los idempotentes de S •

Ejemplos 7.1.2.

1. Si M es un monoide con neutro e, entonces e es un idempotente.
2. Para cualquier grupo G con neutro e se tiene que $E(G) = \{e\}$. En efecto, si $g \in E(G)$ entonces $g^2 = g$, de ahí que $g^{-1}g^2 = g^{-1}g$, o lo que es lo mismo $g = e$. Por consiguiente $E(G) = \{e\}$.
3. El semigrupo $(\mathbb{N}, +)$ carece de idempotentes. Así, $E(\mathbb{N}) = \emptyset$.
4. De acuerdo con la Proposición 6.0.4, todo elemento de una banda rectangular es idempotente i,e, si S es una banda rectangular, entonces $E(S) = S$ •

Se deduce del tercero de los Ejemplos 7.1.2 que un semigrupo puede no tener idempotentes. Por otro lado, el último de estos ejemplos motiva a la siguiente definición.

Definición 7.1.3.

Una **banda** es un semigrupo S para el cual se verifica que $E(S) = S$ •

Ahora bien, sea S un semigrupo para el cual $E(S) \neq \emptyset$. Sobre el conjunto $E(S)$ se define la siguiente relación:

$$\alpha \leq \beta \iff \alpha\beta = \alpha = \beta\alpha$$

Afirmación: $\leq$ es una relación de orden parcial. En efecto, es claro que para cada $\alpha \in E(S)$ $\alpha \leq \alpha$, pues $\alpha^2 = \alpha$. Por lo tanto $\leq$ es reflexiva. Por otro lado, si $\alpha \leq \beta$ y $\beta \leq \alpha$, entonces $\alpha\beta = \alpha = \beta\alpha$ y $\beta\alpha = \beta = \alpha\beta$. De ahí que $\alpha = \beta$ y por consiguiente $\leq$ es antisimétrica. Finalmente, si $\alpha \leq \beta$ y $\beta \leq \gamma$, entonces $\alpha\beta = \alpha = \beta\alpha$ y $\beta\gamma = \beta = \gamma\beta$. De este par de igualdades se desprende que

$$\begin{aligned} \alpha\gamma &= (\alpha\beta)\gamma \\ &= \alpha(\beta\gamma) \\ &= \alpha\beta \\ &= \alpha \end{aligned}$$

y

$$\begin{aligned} \gamma\alpha &= \gamma(\beta\alpha) \\ &= (\gamma\beta)\alpha \\ &= \beta\alpha \\ &= \alpha \end{aligned}$$

Por consiguiente $\alpha \leq \gamma$ y así $\leq$ es transitiva. En definitiva $\leq$ es una relación de orden parcial. Se tiene entonces lo siguiente.

Proposición 7.1.4.

Sea S un semigrupo para el cual $E(S) \neq \emptyset$. Sobre el conjunto $E(S)$ se define la relación

$$\alpha \leq \beta \iff \alpha\beta = \alpha = \beta\alpha$$

Entonces $(E(S), \leq)$ es un copo.

Demostración. Se sigue de la discusión anterior. □

Ahora que se puede ver al conjunto de idempotentes de un semigrupo como un copo, tiene sentido entonces considerar a los elementos minimales de éste. Así, se tiene la siguiente definición.

Definición 7.1.5.

Sea S un semigrupo para el cual $E(S) \neq \emptyset$. Se dice que el idempotente α es un **idempotente minimal** si α es elemento minimal del copo $(E(S), \leq)$ (ver Definición 1.3.6) i,e, α es un idempotente minimal si para cada $\beta \in E(S)$ se verifica lo siguiente

$$\beta \leq \alpha \Longrightarrow \alpha = \beta \bullet$$

Antes de continuar con los idempotentes será conveniente revisar el próximo resultado.

Proposición 7.1.6.

Si M es un monoide con neutro e, entonces $Inv(M) := \{x \in M \mid x \text{ es invertible}\}$ es un grupo.

Demostración. Es claro que e es invertible, luego $e \in Inv(M)$. Si $x, y \in Inv(M)$, entonces $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$ y a la vez $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$. Por consiguiente xy es invertible y $xy \in Inv(M)$. Se deduce que $Inv(M)$ es submonoide de M. Finalmente, de que el inverso de un elemento invertible es también invertible se concluye que $Inv(M)$ es un grupo. □

Ahora, suponga que α es un idempotente del semigrupo S. A partir de α se puede definir al conjunto

$$M_\alpha := \{\alpha x \alpha \mid x \in S\}$$

Afirmación: M_α es un monoide con neutro α. En efecto, para cada $x, y \in S$ se tiene que $(\alpha x\alpha)(\alpha y\alpha) = \alpha(x\alpha y)\alpha \in M_\alpha$. Por lo tanto M_α es un subsemigrupo de S. Más aún, puesto que $\alpha = \alpha\alpha\alpha$, se sigue entonces que $\alpha \in M_\alpha$. Además, para cada $x \in S$, $\alpha(\alpha x\alpha) = \alpha^2 x\alpha = \alpha x\alpha$ y $(\alpha x\alpha)\alpha = \alpha x\alpha^2 = \alpha x\alpha$. Por consiguiente M_α es un monoide con neutro el idempotente α. Esto junto con la proposición anterior permite establecer la siguiente definición.

Definición 7.1.7.

Sean S un semigrupo y $\alpha \in E(S)$. Al grupo $\bar{H}_\alpha := Inv(M_\alpha)$ se le llamará **grupo del idempotente** α •

Proposición 7.1.8.

Si $\alpha \in E(S)$, entonces $\bar{H}_\alpha = \{x \in M_\alpha \mid xx' = \alpha = x'x \text{ para algún } x' \in S\}$

Demostración. Por definición

$$\begin{aligned} \bar{H}_\alpha :&= Inv(M_\alpha) \\ &= \{x \in M_\alpha \mid xz = \alpha = zx \text{ para algún } z \in M_\alpha\} \end{aligned}$$

Considere al conjunto $A := \{x \in M_\alpha | xx' = \alpha = x'x \text{ para algún } x' \in S\}$. Es claro que $\bar{H}_\alpha \subseteq A$. Ahora bien, si $x \in A$, entonces $xx' = \alpha = x'x$ para algún $x' \in S$. Así, para $z := \alpha x'\alpha \in M_\alpha$ se tiene que $zx = (\alpha x'\alpha)x = \alpha x'(\alpha x) = \alpha x'x = \alpha^2 = \alpha$ y a la vez $xz = x(\alpha x'\alpha) = (x\alpha)x'\alpha = xx'\alpha = \alpha^2 = \alpha$. Por lo tanto $xz = \alpha = zx$ y con ello $x \in \bar{H}_\alpha$. De esto último se sigue que $\bar{H}_\alpha = A$. □

Con ayuda de estos resultados se puede ver que a partir de un elemento idempotente se puede definir a un grupo, a saber, el grupo del idempotente. Ahora bien, apoyándonos del monoide M_α puede caracterizarse a los idempotentes minimales.

Proposición 7.1.9.

Sea α un idempotente del semigrupo S. Entonces α es un idempotente minimal si y solo si $M_\alpha \cap E(S) = \{\alpha\}$.

Demostración. $\Longrightarrow$) Suponga que α es idempotente minimal y sea $\beta \in M_\alpha \cap E(S)$. Puesto que M_α es un monoide con neutro α se sigue entonces que $\beta\alpha = \beta = \alpha\beta$. De ahí que $\beta \leq \alpha$ y por lo tanto $\alpha = \beta$. Se concluye que $M_\alpha \cap E(S) = \{\alpha\}$.
$\Longleftarrow$) Suponga ahora que $M_\alpha \cap E(S) = \{\alpha\}$ y sea $\beta \in E(S)$ tal que $\beta \leq \alpha$. Entonces $\beta\alpha = \beta = \alpha\beta$, de donde se sigue que $\beta = \alpha\beta\alpha$ y por lo tanto $\beta \in M_\alpha \cap E(S) = \{\alpha\}$. Por consiguiente $\alpha = \beta$ y α es idempotente minimal. □

Para cada $a \in S$ considere a los conjuntos

$$Sa := \{xa \,|\, x \in S\} \text{ y } aS := \{ax \,|\, x \in S\}$$

Observación 7.1.10.

Sea $\alpha \in E(S)$. Es claro que $M_\alpha \subseteq S\alpha \cap \alpha S$. Ahora, si $x \in S\alpha \cap \alpha S$ entonces $x = \alpha u$ y $x = v\alpha$ para algunos $u, v \in S$. Así, $\alpha u = v\alpha$ y por lo tanto $\alpha v\alpha = \alpha\alpha u = \alpha^2 u = \alpha u = x$. De ahí que $x \in M_\alpha$ y así $M_\alpha = S\alpha \cap \alpha S$ •

Proposición 7.1.11.

Sean $\alpha, \beta \in E(S)$. Entonces $\alpha \leq \beta$ si y solo si $S\alpha \subseteq S\beta$ y $\alpha S \subseteq \beta S$.

Demostración. $\Longrightarrow$) Si $\alpha \leq \beta$, entonces $\alpha\beta = \alpha = \beta\alpha$. Por lo tanto para cada $x \in S$, $x\alpha = x\alpha\beta \in S\beta$ y así $S\alpha \subseteq S\beta$. De manera análoga se ve que $\alpha S \subseteq \beta S$.
$\Longleftarrow$) Suponga que $S\alpha \subseteq S\beta$ y $\alpha S \subseteq \beta S$. Puesto que $\alpha = \alpha\alpha$ entonces $\alpha \in S\alpha$ y $\alpha \in \alpha S$, de manera que puede escribirse $\alpha = x\beta$ y $\alpha = \beta y$ para algunos $x, y \in S$. Así que $\alpha\beta = (x\beta)\beta = x\beta^2 = x\beta = \alpha$, y también $\beta\alpha = \beta(\beta y) = \beta^2 y = \beta y = \alpha$. Por consiguiente $\alpha \leq \beta$. □

7.2. Las equivalencias de Green

Recordar de la sección de ideales que a partir de un ideal bilátero de un semigrupo puede obtenerse una relación de equivalencia, a saber, la equivalencia de Rees (ver Ejemplo 1.2.3 y Proposición 3.9.3). Esta no es la única forma de obtener relaciones de equivalencia a partir de ideales. Resulta que a partir de *ideales principales* es posible definir a ciertas relaciones de equivalencia llamadas equivalencias de Green.

Definición 7.2.1.

Sean S un semigrupo y $a \in S$. Se definen a los siguientes conjuntos

- $Sa := \{xa \mid x \in S\}$
- $aS := \{ax \mid x \in S\}$
- $SaS := \{xay \mid x, y \in S\}$ •

Proposición 7.2.2.

Sa, aS y SaS son ideales: izquierdo, derecho y bilátero respectivamente.

Demostración. Veamos que Sa es un ideal izquierdo: para cada $x, y \in S$ se tiene que $x(ya) = (xy)a \in Sa$. Por consiguiente Sa es un ideal izquierdo. Ahora bien, para ver que SaS es un ideal bilátero solo basta con observar que para cada $x, y, z \in S$, $z(xay) = (zx)ay \in SaS$ y $(xay)z = xa(yz) \in SaS$. El argumento para verificar que aS es un ideal derecho es similar a los anteriores y se omite. □

A pesar de que los ideales Sa, aS y SaS fueron definidos a partir de un elemento a, puede suceder que $a \notin Sa$ ó $a \notin aS$ ó $a \notin SaS$. En efecto, considerar al conjunto de un solo elemento $X = \{a\}$ y sea $S = X^+$. Observe que todas las palabras de Sa, aS y SaS son de longitud mayor a uno. Por consiguiente a no es elemento de ninguno de estos ideales. Sin embargo, se tiene lo siguiente.

Proposición 7.2.3.

Sea S un semigrupo y $a \in S$. Entonces los conjuntos

1. $S^1a := Sa \cup \{a\}$
2. $aS^1 := aS \cup \{a\}$
3. $S^1aS^1 := Sa \cup aS \cup SaS \cup \{a\}$

son ideales: izquierdo, derecho y bilátero respectivamente.

Demostración. Sea $b \in S^1aS^1$ y $x \in S$. Se exhibirá que $xb, bx \in S^1aS^1$. Si $b \in Sa$, entonces debido a que Sa es un ideal izquierdo se sigue que $xb \in Sa \subseteq S^1aS^1$. Por otra parte, puede escribirse $b = ya$ para algún $y \in S$. Así $bx = yax \in SaS \subseteq S^1aS^1$. Por consiguiente $xb, bx \in S^1aS^1$. Si $b \in aS$ se verifica de manera similar a la anterior que $xb, bx \in S^1aS^1$. Si $b \in SaS$, entonces debido a que SaS es un ideal bilátero se sigue que $xb, bx \in SaS \subseteq S^1aS^1$. Si $b = a$, entonces $xb = xa \in Sa \subseteq S^1aS^1$ y $bx = ax \in aS \subseteq S^1aS^1$. Por consiguiente S^1aS^1 es un ideal bilátero. Los argumentos para establecer que S^1a y aS^1 son ideales izquierdo y derecho respectivamente, son similares al anterior y se omiten. □

Observar que cada uno de los ideales: S^1a, aS^1 y S^1aS^1 contiene al elemento a. Más aún, sea I un ideal bilátero de S tal que $a \in I$. Entonces para cada $x, y \in S$ se tiene que $xa, ax, xay \in I$. De ahí que cada uno de los ideales Sa, aS y SaS están contenidos en I, de donde $S^1aS^1 := Sa \cup aS \cup SaS \cup \{a\} \subseteq I$. Por consiguiente S^1aS^1 es el menor ideal bilátero que contiene a a en el sentido de que cualquier otro ideal bilátero que tenga a a como uno de sus elementos debe contener a S^1aS^1. Afirmaciones análogas se verifican con los ideales S^1a y aS^1. A continuación se define lo que se entenderá por un ideal principal.

Definición 7.2.4.

Sean S un semigrupo y $a \in S$. Se dice que

- S^1a es el **ideal principal izquierdo generado por** a.
- aS^1 es el **ideal principal derecho generado por** a.
- S^1aS^1 es el **ideal principal generado por** a •

Definición 7.2.5.

Se dice que el semigrupo S es

- de **ideales principales izquierdos** si todo ideal izquierdo de S es de la forma S^1a.
- de **ideales principales derechos** si todo ideal derecho de S es de la forma aS^1.
- de **ideales principales** si todo ideal de S es de la forma S^1aS^1 •

Observación 7.2.6.

Suponga que $a \in S$ pertenece a cada uno de los ideales Sa, aS y SaS. De que S^1a, aS^1 y S^1aS^1 son los menores ideales: izquierdo, derecho y bilátero que contienen a a aunado a que por definición $Sa \subseteq S^1a$, $aS \subseteq aS^1$ y $SaS \subseteq S^1aS^1$ se concluye que, en este caso, $Sa = S^1a$, $aS = aS^1$ y $SaS = S^1aS^1$ •

Proposición 7.2.7.

Sean S un semigrupo y $a, b \in S$. Entonces

1. $S^1a = S^1b$ si y solo si $a = b$ ó $a = xb$ y $b = ya$ para algunos $x, y \in S$.
2. $aS^1 = bS^1$ si y solo si $a = b$ ó $a = bx$ y $b = ay$ para algunos $x, y \in S$.

Demostración. 1) $\Longrightarrow$) Suponga que $S^1a = S^1b$. Entonces $a \in S^1b$ y $b \in S^1a$. De ahí que $a \in Sb \cup \{b\}$ y $b \in Sa \cup \{a\}$. Por lo tanto $a \in Sb$ o $a = b$ y $b \in Sa$ o $b = a$, lo cual equivale a que $a = b$ o $a \in Sb$ y $b \in Sa$, lo que a su vez es equivalente a que $a = b$ ó $a = xb$ y $b = ya$ para algunos $x, y \in S$.

$\Longleftarrow$) Suponga aquí que $a = b$ ó $a = xb$ y $b = ya$ para algunos $x, y \in S$. Si $a = b$, entonces es inmediato que $S^1a = S^1b$. Por otro lado, si $a = xb$ y $b = ya$ para algunos $x, y \in S$, entonces $a \in Sb$ y $b \in Sa$, y puesto que Sa y Sb son ideales izquierdos se sigue que para cada $u \in S$, $ua \in Sb$ y $ub \in Sa$. Por consiguiente $Sa \subseteq Sb$ y $Sb \subseteq Sa$ y en consecuencia $Sa = Sb$. De esto último y de que $a \in Sb$ y $b \in Sa$ se sigue que $a \in Sa$ y $b \in Sb$, de manera que de la Observación 7.2.6 se concluye que $Sa = S^1a$ y $Sb = S^1b$ y por consiguiente $S^1a = S^1b$. La prueba para el inciso 2) es análoga y por eso se omite. □

A partir de ideales principales se pueden definir ciertas relaciones sobre un semigrupo dado.

Definición 7.2.8.

Sobre el semigrupo S se definen las siguientes relaciones

- $a\mathcal{L}b \iff S^1a = S^1b$
- $a\mathcal{R}b \iff aS^1 = bS^1$
- $a\mathcal{H}b \iff a\mathcal{L}b \quad$ y $\quad a\mathcal{R}b$
- $a\mathcal{J}b \iff S^1aS^1 = S^1bS^1$
- $a\mathcal{D}b \iff a\mathcal{R}u \quad$ y $\quad u\mathcal{L}b \quad$ para algún $u \in S$ •

Proposición 7.2.9.

$\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$, $\mathcal{J}$ y $\mathcal{D}$ son todas relaciones de equivalencia.

Demostración. Debido a que la igualdad entre conjuntos es reflexiva, simétrica y transitiva y puesto que $\mathcal{L}$, $\mathcal{R}$ y $\mathcal{J}$ se definen en términos de igualdades entre ciertos conjuntos entonces no resulta difícil ver que estas tres relaciones son reflexivas, simétricas, transitivas y por lo tanto de equivalencia. Ahora bien, que $\mathcal{H}$ sea una equivalencia se sigue de que $\mathcal{L}$ y $\mathcal{R}$ lo son. El argumento para establecer que $\mathcal{D}$ es una equivalencia es más complicado que los anteriores y es el siguiente: que $\mathcal{D}$ sea reflexiva se sigue de observar que para cada $a \in S$, $a\mathcal{R}a$ y $a\mathcal{L}a$. En cuanto a la simetría, suponga que $a\mathcal{D}b$. Entonces $a\mathcal{R}u$ y $u\mathcal{L}b$ para algún $u \in S$. Para a, b y u se tienen los siguientes casos:

1. $a = u = b$
2. $u = a \neq b$
3. $u = b \neq a$
4. a, b y u son distintos entre si.

En el primer caso se sigue de inmediato que $b\mathcal{D}a$. En el segundo caso, reemplazando u por a se tiene que $a\mathcal{L}b$, de donde $b\mathcal{L}a$ y por consiguiente $b\mathcal{R}b$ y $b\mathcal{L}a$. De ahí que $b\mathcal{D}a$. Para el tercer caso se deduce de manera análoga al caso dos que $b\mathcal{D}a$. En el cuarto y último caso, como $aS^1 = uS^1$ y $S^1u = S^1b$ de la Proposición 7.2.7 se infiere que existen $x, y, p, q \in S$ para los cuales $a = ux$, $u = ay$, $u = pb$ y $b = qu$. Hágase $v := qux$. De estas igualdades se desprende que $v = qux = (qu)x = bx$ y $v = qux = q(ux) = qa$. Por consiguiente $v = bx$ y $v = qa$. Más aún, $b = qu = q(ay) = (qa)y = vy$ y $a = ux = (pb)x = p(bx) = pv$. Por lo tanto $b = vy$ y $a = pv$. Tenemos entonces que $b = vy$ y $v = bx$ y $a = pv$ y $v = qa$. De las dos primeras igualdades se sigue, con ayuda de la Proposición 7.2.7, que $bS^1 = vS^1$, y de las últimas dos que $S^1v = S^1a$. De ahí que $b\mathcal{R}v$ y $v\mathcal{L}a$. Por lo tanto $b\mathcal{D}a$ y $\mathcal{D}$ es simétrica. Finalmente, suponga que $a\mathcal{D}b$ y $b\mathcal{D}c$. Entonces, existen $u, v \in S$ tales que $a\mathcal{R}u$ y $u\mathcal{L}b$ y $b\mathcal{R}v$ y $v\mathcal{L}c$. De que $u\mathcal{L}b$ y $b\mathcal{R}v$ se desprende que $v\mathcal{R}b$ y $b\mathcal{L}u$. Por lo tanto $v\mathcal{D}u$, y al ser $\mathcal{D}$ simétrica se sigue entonces que $u\mathcal{D}v$. Así, existe $w \in S$ para el cual $u\mathcal{R}w$ y $w\mathcal{L}v$. Por lo tanto tenemos lo siguiente: $a\mathcal{R}u$ y $u\mathcal{R}w$ y $w\mathcal{L}v$ y $v\mathcal{L}c$. De ahí que $a\mathcal{R}w$ y $w\mathcal{L}c$ y por consiguiente $a\mathcal{D}c$. Se concluye que $\mathcal{D}$ es transitiva y por lo tanto una equivalencia. □

Definición 7.2.10.

$\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$, $\mathcal{J}$ y $\mathcal{D}$ son llamadas las **equivalencias (o relaciones) de Green** •

Las equivalencias de Green se relacionan entre sí de la siguiente manera.

Proposición 7.2.11.

1. $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$
2. $\mathcal{R} \circ \mathcal{L} = \mathcal{D} = \mathcal{L} \circ \mathcal{R}$

Demostración. 2) Si $(x, y) \in \mathcal{R} \circ \mathcal{L}$, entonces existe $u \in S$ tal que $(x, u) \in \mathcal{L}$ y $(u, y) \in \mathcal{R}$. De ahí que $(y, u) \in \mathcal{R}$ y $(u, x) \in \mathcal{L}$ y por lo tanto $(y, x) \in \mathcal{D}$. De esto último se sigue que $(x, y) \in \mathcal{D}$ y por consiguiente $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{D}$. Si ahora $(x, y) \in \mathcal{D}$, entonces $(x, u) \in \mathcal{R}$ y $(u, y) \in \mathcal{L}$ para algún $u \in S$, lo cual significa que $(x, y) \in \mathcal{L} \circ \mathcal{R}$. Por consiguiente $\mathcal{D} \subseteq \mathcal{L} \circ \mathcal{R}$. Finalmente, si $(x, y) \in \mathcal{L} \circ \mathcal{R}$, entonces existe $u \in S$ para el cual $(x, u) \in \mathcal{R}$ y $(u, y) \in \mathcal{L}$. De ahí que $(x, y) \in \mathcal{D}$ y por lo tanto $(y, x) \in \mathcal{D}$. Así, debe existir un $v \in S$ tal que $(y, v) \in \mathcal{R}$ y $(v, x) \in \mathcal{L}$. De esto se deduce que $(x, v) \in \mathcal{L}$ y $(v, y) \in \mathcal{R}$ y en consecuencia $(x, y) \in \mathcal{R} \circ \mathcal{L}$. Por consiguiente $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$. En definitiva $\mathcal{R} \circ \mathcal{L} = \mathcal{D} = \mathcal{L} \circ \mathcal{R}$. El inciso 1) se sigue directamente de la definición de $\mathcal{H}$. □

Una vez que se ha establecido que las relaciones de Green son equivalencias, podemos considerar entonces a la clase de equivalencia de un elemento con respecto de estas relaciones. Si S es un semigrupo y $a \in S$, denotamos por L_a, R_a, H_a, J_a y D_a a la clase de equivalencia de a con respecto de $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$, $\mathcal{J}$ y $\mathcal{D}$ respectivamente. Llamamos a L_a la **$\mathcal{L}$-clase** de a, a R_a la **$\mathcal{R}$-clase** de a y así respectivamente con las demás relaciones.

Proposición 7.2.12.

Sean S un semigrupo y $\alpha \in E(S)$. Entonces, el grupo del idempotente α coincide con la $\mathcal{H}$-clase de α i,e, $\bar{H}_\alpha = H_\alpha$. (ver Definición 7.1.7)

Demostración. Sea $x \in \bar{H}_\alpha$. Entonces debe suceder que $x\alpha = x = \alpha x$ y $xx' = \alpha = x'x$ para algún $x' \in S$. De acuerdo a la Proposición 7.2.7 las identidades $x = x\alpha$ y $\alpha = x'x$ implican que $S^1x = S^1\alpha$, y las identidades $x = \alpha x$ y $\alpha = xx'$ implican que $xS^1 = \alpha S^1$. Por consiguiente $x\mathcal{R}\alpha$ y $x\mathcal{L}\alpha$, de donde $x\mathcal{H}\alpha$. Se concluye que $x \in H_\alpha$ y por lo tanto $\bar{H}_\alpha \subseteq H_\alpha$. Ahora bien, sea $x \in H_\alpha$. Si $x = \alpha$, entonces es inmediato que $x \in \bar{H}_\alpha$. Si $x \neq \alpha$, entonces debido a que $x\mathcal{H}\alpha$, de la Proposición 7.2.7 se sigue que existen $a, b, c, d \in S$ tales que

$$x = a\alpha \tag{7.1}$$
$$\alpha = bx \tag{7.2}$$
$$x = \alpha c \tag{7.3}$$
$$\alpha = xd \tag{7.4}$$

De las identidades (7.1) y (7.3) se deduce que $\alpha x = \alpha^2 c = \alpha c = x$ y $x\alpha = a\alpha^2 = a\alpha = x$. Así $x\alpha = x = \alpha x$, de donde $x = \alpha x\alpha$ y en consecuencia $x \in M_\alpha$. Ahora bien, puesto que $x\alpha = x = \alpha x$, de (7.2) y (7.4) se sigue que $x = x\alpha = xbx$ y $x = \alpha x = xdx$. Por consiguiente $x = xbx$ y $x = xdx$. Defínase $x' := bxd$. Entonces

$$\begin{aligned} xx' &= x(bxd) \\ &= (xbx)d \\ &= xd \\ &= \alpha \end{aligned}$$

mientras que

$$\begin{aligned} x'x &= (bxd)x \\ &= b(xdx) \\ &= bx \\ &= \alpha \end{aligned}$$

Por consiguiente $xx' = \alpha = x'x$, de manera que de la Proposición 7.1.8 se concluye que $x \in \bar{H}_\alpha$ y por lo tanto $H_\alpha \subseteq \bar{H}_\alpha$. En definitiva $\bar{H}_\alpha = H_\alpha$.

□

De acuerdo a la proposición anterior, el grupo de un idempotente puede verse como la colección de los elementos inversos de un monoide o bien como una clase de equivalencia.

7.3. Definición de semigrupo regular y completamente regular

A continuación se introduce a una clase particular de semigrupos llamados *semigrupos regulares*.

Definición 7.3.1.

Sea S un semigrupo y $a, x \in S$. Se dice que x es

- **pseudoinverso** de a si ocurre que $a = axa$.
- **inverso** de a si ocurre que $a = axa$ y $x = xax$

  Adicionalmente, se denota a la colección de todos los inversos de a por $V(a)$ i,e,

$$V(a) := \{x \in S \mid x \text{ es inverso de } a\} \bullet$$

Observación 7.3.2.

Sea M un monoide con neutro e y suponga que t es el inverso de x en el sentido de la Definición 3.2.9. Entonces $xtx = x(tx) = xe = x$ y $txt = t(xt) = te = t$ i,e, $xtx = x$ y $txt = t$. Por consiguiente t es un inverso de x en el sentido de la Definición 7.3.1. Puede concluirse así que en un monoide, todo inverso en el sentido de la Definición 3.2.9 es también un inverso en el sentido de la Definición 7.3.1. Sin embargo, el recíproco no se verifica. En efecto, la matriz $X := \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ es un idempotente del monoide $M_2(\mathbb{Z})$. Por lo tanto $XXX = X$ y así X es inversa de sí misma en el sentido de la Definición 7.3.1. A pesar de ello la matriz X no es inversa de sí misma en el sentido de la Definición 3.2.9 $\bullet$

Proposición 7.3.3.

Sea S un semigrupo y suponga que $a \in S$ posee al menos un pseudoinverso. Entonces

1. $E(S) \neq \emptyset$.
2. $V(a) \neq \emptyset$.

Demostración. Suponga que $x \in S$ es pseudoinverso de a. Luego $axa = a$, de manera que $xaxa = xa$ y $axax = ax$. Por consiguiente $xa, ax \in E(S)$ y con ello $E(S) \neq \emptyset$. Ahora bien, hágase $b := xax$. Entonces

$$\begin{aligned} aba &= a(xax)a \\ &= (axa)xa \\ &= axa \\ &= a \end{aligned}$$

mientras que

$$\begin{aligned} bab &= (xax)a(xax) \\ &= x(axa)xax \\ &= x(axa)x \\ &= xax \\ &= b \end{aligned}$$

Por consiguiente $b \in V(a)$ y así $V(a) \neq \emptyset$. □

A aquellos elementos de un semigrupo que posean al menos un pseudoinverso se les concederá un nombre especial.

Definición 7.3.4.

Sea S un semigrupo. Decimos que

- $a \in S$ es **regular**, si a posee al menos un pseudoinverso.
- S es un **semigrupo regular** si todo elemento de S es regular •

Ejemplo 7.3.5.

De la Definición 6.0.1 se aprecia que toda banda rectangular es un semigrupo regular. Además, de la Observación 7.3.2 se sigue que todo grupo es un semigrupo regular •

Observación 7.3.6.

Si S es un semigrupo regular y $a \in S$, entonces $a = axa$ para algún $x \in S$. De ahí que $a \in Sa$ y $a \in aS$. Además observe que $a = axa = (axa)xa = (ax)a(xa)$ y por consiguiente $a \in SaS$. Así, de la Observación 7.2.6 se concluye que en un semigrupo regular

$$S^1a = Sa \text{ y } aS^1 = aS \text{ y } S^1aS^1 = SaS \bullet$$

Una vez que se ha establecido la definición de semigrupo regular, puede verse entonces que de acuerdo con la Proposición 7.3.3 todo semigrupo regular posee idempotentes. A continuación, se muestra que cualesquiera dos idempotentes de un semigrupo regular generan una banda rectangular.

Proposición 7.3.7.

Sea S un semigrupo regular y $\alpha, \beta \in E(S)$. Considere al conjunto

$$\mathcal{S}(\alpha,\beta) := \{g \in E(S) \mid g\alpha = g = \beta g \quad \text{y} \quad \alpha g\beta = \alpha\beta\}$$

Entonces

- $\mathcal{S}(\alpha,\beta) \neq \emptyset$
- $\mathcal{S}(\alpha,\beta)$ es subsemigrupo de S.
- $\mathcal{S}(\alpha,\beta)$ es una banda rectangular.

Demostración. Puesto que S es regular, para el elemento $\alpha\beta$ existe $x \in S$ tal que $\alpha\beta = \alpha\beta x\alpha\beta$. Defínase $g := \beta x\alpha\beta x\alpha$. Entonces

$$\begin{aligned} g^2 &= (\beta x\alpha\beta x\alpha)(\beta x\alpha\beta x\alpha) \\ &= \beta x(\alpha\beta x\alpha\beta)x\alpha\beta x\alpha \\ &= \beta x(\alpha\beta)x\alpha\beta x\alpha \\ &= \beta x(\alpha\beta x\alpha\beta)x\alpha \\ &= \beta x\alpha\beta x\alpha \\ &= g \end{aligned}$$

Por consiguiente $g \in E(S)$. Ahora bien, observe que $g\alpha = (\beta x\alpha\beta x\alpha)\alpha = \beta x\alpha\beta x\alpha^2 = \beta x\alpha\beta x\alpha = g$ y $\beta g = \beta(\beta x\alpha\beta x\alpha) = \beta^2 x\alpha\beta x\alpha = \beta x\alpha\beta x\alpha = g$. Más aún, $\alpha g\beta = \alpha(\beta x\alpha\beta x\alpha)\beta = (\alpha\beta x\alpha\beta)x\alpha\beta = \alpha\beta x\alpha\beta = \alpha\beta$. Por lo tanto $g \in \mathcal{S}(\alpha,\beta)$ y puede concluirse así que $\mathcal{S}(\alpha,\beta) \neq \emptyset$. **Afirmación 1):** Todo elemento $g \in \mathcal{S}(\alpha,\beta)$ satisface que $g = \beta g\alpha$. En efecto, puesto que todo elemento de $\mathcal{S}(\alpha,\beta)$ es por definición un idempotente, entonces $g = g^2 = \beta gg\alpha = \beta g^2\alpha = \beta g\alpha$. **Afirmación 2):** Para cada $g \in \mathcal{S}(\alpha,\beta)$ se verifica que $\alpha\beta = \alpha\beta g\alpha\beta$. En efecto, si $g \in \mathcal{S}(\alpha,\beta)$, entonces $\alpha\beta = \alpha g\beta$, lo que combinado con la Afirmación 1) resulta en que $\alpha\beta = \alpha\beta g\alpha\beta$ como se requería. Para mostrar que $\mathcal{S}(\alpha,\beta)$ es un subsemigrupo tómense $g, h \in \mathcal{S}(\alpha,\beta)$. De las observaciones anteriores se sigue que

$$\begin{aligned} (gh)^2 &= (\beta g\alpha)(\beta h\alpha)(\beta g\alpha)(\beta h\alpha) \\ &= \beta g(\alpha\beta h\alpha\beta)g\alpha\beta h\alpha \\ &= \beta g\alpha\beta g\alpha\beta h\alpha \\ &= \beta g(\alpha\beta g\alpha\beta)h\alpha \\ &= \beta g\alpha\beta h\alpha \\ &= gh \end{aligned}$$

Por consiguiente $gh \in E(S)$. Por otra parte, $(gh)\alpha = g(h\alpha) = gh$ a la vez que $\beta(gh) = (\beta g)h = gh$. Además

$$\begin{aligned} \alpha gh\beta &= \alpha(\beta g\alpha)(\beta h\alpha)\beta \\ &= (\alpha\beta g\alpha\beta)h\alpha\beta \\ &= \alpha\beta h\alpha\beta \\ &= \alpha\beta \end{aligned}$$

De todo lo anterior se deduce que $gh \in \mathcal{S}(\alpha, \beta)$ y por consiguiente $\mathcal{S}(\alpha, \beta)$ es un subsemigrupo de S. Finalmente, para cualesquiera $g, h \in \mathcal{S}(\alpha, \beta)$

$$\begin{aligned} ghg &= (\beta g\alpha)(\beta h\alpha)(\beta g\alpha) \\ &= \beta g(\alpha\beta h\alpha\beta)g\alpha \\ &= \beta g\alpha\beta g\alpha \\ &= g^2 \\ &= g \end{aligned}$$

Se concluye de esto que $\mathcal{S}(\alpha, \beta)$ es una banda rectangular.

□

Algo notable de la demostración anterior es que proporciona una técnica para obtener un nuevo idempotente a partir de dos ya dados: si $\alpha, \beta \in E(S)$ y x es un pseudoinverso de $\alpha\beta$, entonces $g := \beta x\alpha\beta x\alpha$ es un idempotente. Usaremos este método para establecer el siguiente resultado.

Proposición 7.3.8.

Sea S un semigrupo regular y sea ρ una congruencia sobre S. Si $[a]_\rho \in E(\frac{S}{\rho})$, entonces $[a]_\rho = [g]_\rho$ para algún $g \in E(S)$.

Demostración. Si $[a]_\rho$ es un idempotente del semigrupo $\frac{S}{\rho}$, entonces $[a]_\rho^2 = [a]_\rho$ de donde $[a^2]_\rho = [a]_\rho$ y por consiguiente $a^2 \rho a$. Debido a que S es regular se sigue de la Proposición 7.3.3 que $V(a) \neq \emptyset$. Sea $x \in V(a)$. Entonces debe suceder que

$$axa = a \tag{7.5}$$

$$xax = x \tag{7.6}$$

Ahora bien, tómese $y \in V(xaax) = V(xa^2x)$. Entonces se verifican las igualdades

$$xa^2xyxa^2x = xa^2x \tag{7.7}$$

$$yxa^2xy = y \tag{7.8}$$

Por otro lado, debido a que xa y ax son idempotentes se concluye que $g := axyxa^2xyxa$ es un idempotente. Observe que de la igualdad (7.8) se sigue que $g := axyxa^2xyxa = ax(yxa^2xy)xa = axyxa$. **Afirmación:** $a\rho g$. En efecto, primero observe que

$$a^2\rho a \tag{7.9}$$
$$\Longrightarrow xa^2 \quad \rho \quad xa \tag{7.10}$$
$$\Longrightarrow xa^2x \quad \rho \quad xax \tag{7.11}$$

y también

$$a^2\rho a \tag{7.12}$$
$$\Longrightarrow yxa^2 \quad \rho \quad yxa \tag{7.13}$$
$$\Longrightarrow yxa^2x \quad \rho \quad yxax \tag{7.14}$$

De (7.11) y (7.14) se desprende que $xa^2xyxa^2x \quad \rho \quad xaxyxax$. Ahora bien, de esto último y de las igualdades (7.6) y (7.7) se sigue que $xa^2x \quad \rho \quad xyx$, lo cual en combinación con (7.6) y (7.11) permite concluir que $x \quad \rho \quad xyx$. En consecuencia $axa \quad \rho \quad axyxa$, o lo que es lo mismo $a\rho g$. De ahí que $[a]_\rho = [g]_\rho$ lo cual concluye la prueba.

□

A continuación, haciendo uso de las equivalencias de Green se caracteriza a los semigrupos regulares.

Proposición 7.3.9.

Los siguientes enunciados son equivalentes para un semigrupo S.

1. S es un semigrupo regular.
2. Para cada $x \in S$ existe $\alpha \in E(S)$ tal que $x\mathcal{L}\alpha$
3. Para cada $x \in S$ existe $\beta \in E(S)$ tal que $x\mathcal{R}\beta$

Demostración. 1) $\Longrightarrow$ 2) Si S es regular y $x \in S$, entonces existe $b \in S$ para el cual $x = xbx$. De ahí que $bx = bxbx$ y por lo tanto $bx \in E(S)$. Sea $\alpha := bx$. Entonces puede escribirse $x = x\alpha$ de manera que de la Proposición 7.2.7 se deduce que $S^1x = S^1\alpha$, y por consiguiente $x\mathcal{L}\alpha$.

2) $\Longrightarrow$ 3) Sea $x \in S$. Por hipótesis, existe $\alpha \in E(S)$ tal que $x\mathcal{L}\alpha$. Si $x = \alpha$ entonces para $\beta = \alpha$ se verifica de inmediato que $x\mathcal{R}\beta$. En otro caso, de la Proposición 7.2.7 se sigue que existen $p, q \in S$ tales que $x = p\alpha$ y $\alpha = qx$. De la primera igualdad se sigue que $x\alpha = p\alpha^2 = p\alpha = x$, lo que combinado con la segunda igualdad resulta en que $x = xqx$. Por consiguiente $xq = xqxq$ y $xq \in E(S)$. Hágase $\beta := xq$. Entonces puede escribirse $x = \beta x$ y por lo tanto, de la Proposición 7.2.7 y de la definición de $\mathcal{R}$ puede concluirse

que $x\mathcal{R}\beta$.

3) $\Longrightarrow$ 1) Veamos que todo elemento de S es regular: si $x \in S$ entonces por hipótesis, existe $\beta \in E(S)$ para el cual $x\mathcal{R}\beta$. Si $x = \beta$ entonces x es idempotente y por lo tanto regular. En otro caso, de la Proposición 7.2.7 se sigue que existen $p, q \in S$ tales que $x = \beta p$ y $\beta = xq$. De la primera igualdad se sigue que $\beta x = \beta^2 p = \beta p = x$, lo que combinado con la segunda igualdad resulta en que $x = xqx$. Por consiguiente x es regular. □

Proposición 7.3.10.

Sea S un semigrupo y sea $x \in S$. Entonces x pertenece a la $\mathcal{H}$-clase de algún idempotente si y solo si existe $b \in S$ tal que $x = xbx$ y $xb = bx$.

Demostración. Sea S un semigrupo. Si $x = xbx$, entonces xb y bx son ambos idempotentes, y además, de la primera parte de la prueba de la Proposición 7.3.9 se ve que $x\mathcal{L}bx$. Usando un argumento similar se deduce también que $x\mathcal{R}xb$, de tal manera que si $bx = xb$, entonces $x\mathcal{L}bx$ y $x\mathcal{R}bx$, de donde $x\mathcal{H}bx$. De esto se sigue que si un elemento regular tiene un pseudoinverso conmutativo, entonces tal elemento pertenece a la $\mathcal{H}$-clase de algún idempotente. E inversamente, suponga que $x\mathcal{H}\alpha$ para algún idempotente α. Así, x pertenece a la clase de equivalencia H_α que, según la Proposición 7.2.12, debe ser el grupo del idempotente α. Por lo tanto, debe existir $b \in S$ tal que $xb = \alpha = bx$, de tal manera que $xbx = (xb)x = \alpha x = x$. Por consiguiente b es un pseudoinverso de x que conmuta con x.

□

Lo anterior suscita la siguiente definición.

Definición 7.3.11.

Se dice que el semigrupo S es **completamente regular** si para cada $x \in S$ existe $b \in S$ tal que $x = xbx$ y $xb = bx$. A uno de tales $b \in S$ se le llamará **pseudoinverso conmutativo** de x •

Proposición 7.3.12.

Los siguientes enunciados son equivalentes para un semigrupo S.

1. S es completamente regular.
2. $S = \bigcup_{\alpha \in E(S)} H_\alpha$

Demostración. Directa de la definición de semigrupo completamente regular y de la Proposición 7.3.10 • □

De este resultado se puede apreciar que un semigrupo completamente regular es una unión ajena de grupos.

Observación 7.3.13.

Suponga que S es un semigrupo completamente regular y considere a la familia

$$\mathcal{F} := \{H_\alpha \mid \alpha \in E(S)\}$$

Debido a que cada H_α es una clase de equivalencia, se sigue entonces que los miembros de $\mathcal{F}$ son no vacíos y disjuntos por pares. Por consiguiente, de la proposición anterior puede concluirse que $\mathcal{F}$ es una partición de S •

Observe que por definición, todo semigrupo completamente regular es también un semigrupo regular. Sin embargo, el recíproco no se verifica.

Ejemplo 7.3.14.

Hay un semigrupo regular que no es completamente regular. En efecto, considerar al monoide $M_2(\mathbb{R})$ con el producto usual de matrices. Si A es una matriz invertible con inversa X, entonces es claro que $AXA = A$ y por consiguiente A es regular. Si A es la matriz cero, entonces es claro que $AAA = A$ y así A es regular. Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ es una matriz no invertible y diferente de la matriz cero, entonces $Det(A) = ad - bc = 0$ y además, sin perder generalidad, puede suponerse que $a \neq 0$. Sea $X := \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{pmatrix}$. Se tiene entonces que

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & \frac{bc}{a} \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

Por consiguiente $A = AXA$ y así A es regular. Se concluye de esto que $M_2(\mathbb{R})$ es un semigrupo regular. Ahora bien, considere a la matriz $A := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. **Afirmación 1):** Toda matriz de la forma $\begin{pmatrix} x & 0 \\ z & x \end{pmatrix}$ conmuta con A. En efecto, $\begin{pmatrix} x & 0 \\ z & x \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}$ y a la vez $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ z & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}$. **Afirmación 2):** Si la matriz $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ conmuta con la matriz A entonces $y = 0$ y $x = w$. En efecto, si $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ entonces $\begin{pmatrix} y & 0 \\ w & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix}$ de donde $y = 0$ y $x = w$. De este par de afirmaciones se

deduce que todas aquellas matrices que conmutan con la matriz A son las de la forma $\begin{pmatrix} x & 0 \\ z & x \end{pmatrix}$. Para una cualquiera de tales matrices se tiene que

$$\begin{aligned} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ z & x \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ &\neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Por lo tanto ninguna matriz que conmute con A puede ser pseudoinverso de A, de tal manera que la matriz A carece de pseudoinversos conmutativos. Por consiguiente $M_2(\mathbb{R})$ no es completamente regular •

A partir de un semigrupo completamente regular se puede obtener una banda conmutativa. Sin embargo, para establecer tal aseveración se necesita saber cuando dos ideales de la forma SaS y SbS son iguales. Esto no resulta complicado de averiguar y es el contenido de la siguiente proposición.

Proposición 7.3.15.

Si S es un semigrupo regular, entonces $SaS = SbS$ si y solo si $a = xby$ y $b = paq$ para algunos $x, y, p, q \in S$.

Demostración. En la Observación 7.3.6 se ve que para cada elemento $a \in S$ se verifica que $a \in SaS$, de manera que si $SaS = SbS$ entonces $a \in SbS$ y $b \in SaS$. Por consiguiente $a = xby$ y $b = paq$ para algunos $x, y, p, q \in S$. Y viceversa, suponga que $a = xby$ y $b = paq$ para algunos $x, y, p, q \in S$. Luego $a \in SbS$ y $b \in SaS$, y puesto que SaS y SbS son ideales biláteros se tiene entonces que para cada $s, t, u, v \in S$, $sat \in SbS$ y $ubv \in SaS$. De ahí que $SaS \subseteq SbS$ y $SbS \subseteq SaS$. Por consiguiente $SaS = SbS$. □

Proposición 7.3.16.

Si S es un semigrupo completamente regular, entonces $\mathcal{J}$ (ver Definición 7.2.8) es una congruencia. Más aún, el semigrupo cociente $\dfrac{S}{\mathcal{J}}$ resulta ser una banda conmutativa (ver Definición 7.1.3).

Demostración. Recordar que $a\mathcal{J}b \iff S^1aS^1 = S^1bS^1$. Ahora bien, como en este caso S es un semigrupo regular, entonces para cada $a \in S$ se tiene que $S^1aS^1 = SaS$ (ver Observación 7.3.6). Por lo tanto $a\mathcal{J}b \iff SaS = SbS$. Veamos que para cada $a \in S$, $a\mathcal{J}a^2$: si $a \in S$ entonces existe $x \in S$ tal que $a = axa$ y $xa = ax$. Luego $a = axa = (axa)xa = (axa)ax = (ax)a^2x$ mientras que $a^2 = (axa)a = (ax)aa$. Por consiguiente,

de la Proposición 7.3.15 se deduce que $a\mathcal{J}a^2$. Veamos ahora que para cada $a, b \in S$, $ab\mathcal{J}ba$: para el elemento $ab \in S$ existe $x \in S$ tal que $ab = abxab$ y $xab = abx$. Así que $ab = abxab = ababx = a(ba)(bx)$. Por otra parte, para el elemento $ba \in S$ existe $y \in S$ tal que $ba = bayba$ y $yba = bay$. Así que $ba = bayba = babay = b(ab)(ay)$. Por lo tanto, de la Proposición 7.3.15 se infiere que $ab\mathcal{J}ba$. A continuación se exhibe que $\mathcal{J}$ es una congruencia izquierda: suponga que $a\mathcal{J}b$ y sea $x \in S$. Puede escribirse $a = pbq$ y $b = uav$ para algunos $p, q, u, v \in S$. De la primera de estas igualdades se sigue que $xa = xpbq$. Ahora bien, como S es regular, entonces $x = xtx$ para algún $t \in S$. Así que $xpbq = xtxpbq = (xt)x(pb)q \in Sx(pb)S = S(pb)xS \subseteq SbxS = SxbS$. Por consiguiente $xa = xpbq \in SxbS$, y así $SxaS \subseteq SxbS$. De la igualdad $b = uav$ se sigue que $xb = xtxuav$, pero $xtxuav \in Sx(ua)S = S(ua)xS \subseteq SaxS = SxaS$. Por lo tanto $xb = xtxuav \in SxaS$ y así $SxbS \subseteq SxaS$. En definitiva $SxaS = SxbS$ y por consiguiente $xa\mathcal{J}xb$. Concluimos de ello que $\mathcal{J}$ es una congruencia izquierda. Observe que para probar esto último se usó reiteradamente el hecho de que $ab\mathcal{J}ba$, o lo que es lo mismo, $SabS = SbaS$. Probar que $\mathcal{J}$ es una congruencia derecha será sencillo usando la información anterior: suponga que $a\mathcal{J}b$ y sea $x \in S$. Puesto que $\mathcal{J}$ es una congruencia izquierda, entonces $xa\mathcal{J}xb$, pero $ax\mathcal{J}xa$ y $xb\mathcal{J}bx$, de manera que de la transitividad de $\mathcal{J}$ se sigue que $ax\mathcal{J}bx$ y por consiguiente $\mathcal{J}$ es una congruencia derecha. Concluimos de todo lo anterior que $\mathcal{J}$ es una congruencia sobre S y que $\frac{S}{\mathcal{J}}$ es un semigrupo conmutativo en el que todo elemento es un idempotente i,e, $\frac{S}{\mathcal{J}}$ es una banda conmutativa. □

Corolario 7.3.17.

Si S es un semigrupo completamente regular, entonces para cada $x \in S$ existe $\alpha \in E(S)$ tal que $SxS = S\alpha S$.

Demostración. Directa de las Proposiciones 7.3.8 y 7.3.16. □

.

Capítulo 8

Semigrupos completamente simples y el Teorema de Rees

8.1. Semigrupos matriz de Rees

A continuación se introduce a los llamados *semigrupos matriz de Rees*. Para constriur a uno de tales semigrupos serán necesarios algunos ingredientes, a saber, dos conjuntos no vacíos, un semigrupo y una función que relacione a estos.

Sean A y B conjuntos no vacíos, S un semigrupo y $\mathcal{P} : B \times A \longrightarrow S$ una función. Denotamos al conjunto $A \times S \times B$ por $\mathcal{M}(S, A, B, \mathcal{P})$. Sobre $\mathcal{M}(S, A, B, \mathcal{P})$ se define la siguiente operación binaria:

$$(a, g, b)(c, h, d) := (a, g\mathcal{P}(b, c)h, d) \tag{8.1}$$

Observe que la segunda coordenada de la terna que aparece a la derecha de la igualdad (8.1) es en efecto un elemento del semigrupo S, pues el codominio de la función $\mathcal{P}$ es el semigrupo S. Además,

$$\begin{aligned}(a, g, b)[(c, h, d)(e, i, f)] &= (a, g, b)(c, h\mathcal{P}(d, e)i, f)\\ &= (a, g\mathcal{P}(b, c)[h\mathcal{P}(d, e)i], f)\\ &= (a, [g\mathcal{P}(b, c)h]\mathcal{P}(d, e)i, f)\\ &= (a, g\mathcal{P}(b, c)h, d)(e, i, f)\\ &= [(a, g, b)(c, h, d)](e, i, f)\end{aligned}$$

Por consiguiente $\mathcal{M}(S, A, B, \mathcal{P})$ es un semigrupo bajo esta operación entre ternas. A $\mathcal{M}(S, A, B, \mathcal{P})$ se le llama **semigrupo matriz de Rees** con matriz sandwich $\mathcal{P}$.[1] Será de interés el caso cuando $S = G$ sea un grupo, pues en esta situación los semigrupos matriz

[1] El nombre *semigrupo matriz de Rees con matriz sandwich* $\mathcal{P}$ fue tomado de [1]. Véase capítulo 1, página 18, Ejemplo 2.15 (j) de la referencia citada.

de Rees tendrán propiedades interesantes. Así, y a menos que se indique otra cosa, en lo posterior G denotará un grupo. Observe también que los semigrupos matriz de Rees proporcionan una técnica para obtener nuevos semigrupos a partir de los ya conocidos. Una primera propiedad de este tipo de semigrupos es la siguiente.

Proposición 8.1.1.

Toda banda rectangular es isomorfa a un semigrupo de la forma $\mathcal{M}(G, A, B, \mathcal{P})$.

Demostración. Suponga que S es una banda rectangular. De acuerdo a la Proposición 6.0.13 existen un par de conjuntos, digamos A y B, tales que $S \cong A \times B$ donde la operación en $A \times B$ está dada por $(a, b)(c, d) := (a, d)$. Sea $G = \{e\}$ el grupo con un solo elemento y considere a la función $\mathcal{P} : B \times A \longrightarrow G$ dada por $\mathcal{P}(b, a) := e$. Veamos que $A \times B \cong \mathcal{M}(G, A, B, \mathcal{P})$: sea $f : A \times B \longrightarrow \mathcal{M}(G, A, B, \mathcal{P})$ la función definida por $f(a, b) := (a, e, b)$. Es claro que f es biyectiva y además

$$\begin{aligned} f(a, b)f(c, d) &= (a, e, b)(c, e, d) \\ &= (a, e\mathcal{P}(b, c)e, d) \\ &= (a, e^3, d) \\ &= (a, e, d) \\ &= f(a, d) \\ &= f[(a, b)(c, d)] \end{aligned}$$

Así f es un isomorfismo de semigrupos y por lo tanto $A \times B \cong \mathcal{M}(G, A, B, \mathcal{P})$. De esto último y de que $S \cong A \times B$ se sigue que $S \cong \mathcal{M}(G, A, B, \mathcal{P})$.

□

Otras propiedades adicionales de los semigrupos matriz de Rees sobre un grupo son dadas a continuación.

Proposición 8.1.2.

Sea $S = \mathcal{M}(G, A, B, \mathcal{P})$. Entonces

1. $E(S) \neq \emptyset$
2. Todo idempotente de S es minimal.
3. S es completamente regular.

Demostración. Denotemos por e_G al neutro de G. En primer lugar, observe que debido a que $\mathcal{P}$ toma valores en el grupo G, entonces tiene sentido considerar al inverso de $\mathcal{P}(b, a)$. Así, para cada $a \in A$ y $b \in B$ se tiene que $(a, \mathcal{P}(b, a)^{-1}, b)$ es un idempotente. En efecto

$$\begin{aligned} (a, \mathcal{P}(b, a)^{-1}, b)(a, \mathcal{P}(b, a)^{-1}, b) &= (a, \mathcal{P}(b, a)^{-1}\mathcal{P}(b, a)\mathcal{P}(b, a)^{-1}, b) \\ &= (a, e_G\mathcal{P}(b, a)^{-1}, b) \\ &= (a, \mathcal{P}(b, a)^{-1}, b) \end{aligned}$$

Más aún, todo idempotente es de esa forma, pues si (a, g, b) es idempotente, entonces

$$(a, g, b) = (a, g, b)(a, g, b) = (a, g\mathcal{P}(b, a)g, b)$$

De donde $g\mathcal{P}(b, a)g = g$ y por consiguiente $g = \mathcal{P}(b, a)^{-1}$. Se puede concluir así que

$$E(S) = \{(a, g, b) \mid g = \mathcal{P}(b, a)^{-1}\}$$

(Será conveniente aquí ver la Proposición 7.1.4). Ahora bien, sean (a, g, b) y (x, h, y) dos idempotentes para los cuales $(x, h, y) \leq (a, g, b)$. Entonces $(x, h, y)(a, g, b) = (x, h, y) = (a, g, b)(x, h, y)$, de lo cual se desprende que $(x, h\mathcal{P}(y, a)g, b) = (x, h, y)$ y al mismo tiempo $(a, g\mathcal{P}(b, x)h, y) = (x, h, y)$. De este par de igualdades se sigue que $a = x$ y $b = y$. Por consiguiente $(x, h, y) = (a, g, b)$ y en consecuencia todo idempotente de S es minimal (véase Proposición 7.1.4 y Definición 7.1.5). Finalmente, veamos que todo elemento de S tiene un pseudoinverso conmutativo. Sea (a, g, b) un elemento arbitrario de S y considere a la terna (a, h, b) donde $h := \mathcal{P}(b, a)^{-1}g^{-1}\mathcal{P}(b, a)^{-1}$. Entonces

$$\begin{aligned}(a, g, b)(a, h, b) &= (a, g, b)(a, \mathcal{P}(b, a)^{-1}g^{-1}\mathcal{P}(b, a)^{-1}, b)\\ &= (a, g\mathcal{P}(b, a)\mathcal{P}(b, a)^{-1}g^{-1}\mathcal{P}(b, a)^{-1}, b)\\ &= (a, \mathcal{P}(b, a)^{-1}, b)\end{aligned}$$

y a la vez

$$\begin{aligned}(a, h, b)(a, g, b) &= (a, \mathcal{P}(b, a)^{-1}g^{-1}\mathcal{P}(b, a)^{-1}, b)(a, g, b)\\ &= (a, \mathcal{P}(b, a)^{-1}g^{-1}\mathcal{P}(b, a)^{-1}\mathcal{P}(b, a)g, b)\\ &= (a, \mathcal{P}(b, a)^{-1}, b)\end{aligned}$$

Por lo tanto (a, g, b) conmuta con (a, h, b). Además

$$\begin{aligned}(a, g, b)(a, h, b)(a, g, b) &= (a, \mathcal{P}(b, a)^{-1}, b)(a, g, b)\\ &= (a, \mathcal{P}(b, a)^{-1}\mathcal{P}(b, a)g, b)\\ &= (a, g, b)\end{aligned}$$

Así (a, h, b) es un pseudoinverso conmutativo de (a, g, b) y por consiguiente S es completamente regular. □

8.2. Semigrupos completamente simples

En esta parte se introduce a los llamados semigrupos completamente simples que son semigrupos que contienen ideales con ciertas propiedades. Iniciamos la discusión con el concepto de semigrupo simple.

Definición 8.2.1.

Decimos que el semigrupo S es

- **simple izquierdo** si el único ideal izquierdo de S es S.
- **simple derecho** si el único ideal derecho de S es S.
- **simple** si el único ideal bilátero de S es S •

Ejemplos 8.2.2.

- Sobre el conjunto $X \neq \emptyset$ se define para cada $a, b \in X$, $ab := a$ Según el Ejemplo 3.4.2, X es un semigrupo. Sea I un ideal izquierdo de X y tómense $x \in X$ y $a \in I$ arbitrarios. Entonces $x = xa \in I$ y por consiguiente $I = X$. Así X es un semigrupo simple izquierdo.
- Sea G un grupo y suponga que I es in ideal izquierdo de G. Si $a \in I$, entonces $e = a^{-1}a \in I$. De ahí que para cada $g \in G$, $g = ge \in I$ y por consiguiente $I = G$. Así G es un semigrupo simple izquierdo. De manera similar se exhibe que G es simple derecho y por consiguiente también simple •

A continuación se revisa un resultado que relaciona los nuevos conceptos definidos con las relaciones de Green.

Proposición 8.2.3.

Sea S un semigrupo. Entonces

1. S es simple izquierdo si y solo si $S \times S = \mathcal{L}$
2. S es simple derecho si y solo si $S \times S = \mathcal{R}$
3. S es simple si y solo si $S \times S = \mathcal{J}$

Demostración. 3) Suponga que S es un semigrupo simple y sean $a, b \in S$ arbitrarios. Entonces, puesto que S es simple, $S^1aS^1 = S = S^1bS^1$ y por lo tanto $a\mathcal{J}b$. Así $S \times S = \mathcal{J}$. Ahora bien, suponga que $S \times S = \mathcal{J}$ y sea I un ideal bilátero de S. Tómese $a \in I$ arbitrario. Entonces $S^1aS^1 \subseteq I$, y puesto que $S \times S = \mathcal{J}$, para cada $x \in S$ debe suceder que $x\mathcal{J}a$, o lo que es lo mismo $S^1xS^1 = S^1aS^1 \subseteq I$. De ahí que $x \in I$ y por consiguiente $I = S$. Se concluye así que S es simple. Las pruebas de 1) y 2) son similares que la ya hecha y por eso se omiten. □

El siguiente tipo de ideales será fundamental en toda esta exposición, y de hecho, nos permitirá definir a los ya mencionados semigrupos completamente simples.

Definición 8.2.4.

Sean S un semigrupo e $I \subseteq S$. Se dice que I es un **ideal izquierdo (derecho) minimal** de S si se verifican las siguientes condiciones:

- I es ideal izquierdo (derecho) de S.
- Para cada ideal izquierdo (derecho) I' de S

$$I' \subseteq I \Longrightarrow I' = I \bullet$$

Definición 8.2.5.

Decimos que el semigrupo S es **completamente simple** si S es simple y si contiene al menos un ideal izquierdo minimal y un ideal derecho minimal $\bullet$

Antes de dar un ejemplo se establece que ser completamente simple es un invariante bajo isomorfismo.

Proposición 8.2.6.

Si $S \cong T$ y T es completamente simple, entonces S es completamente simple.

Demostración. Sean $f : S \longrightarrow T$ un isomorfismo de semigrupos e I un ideal bilátero de S. De la sobreyectividad de f y de acuerdo con la Proposición 3.9.7 $f(I)$ debe ser un ideal bilátero del semigrupo simple T. Por lo tanto $f(I) = T$ y en consecuencia $f^{-1}(f(I)) = f^{-1}(T) = f^{-1}(f(S))$. De la Proposición 1.4.27 se sigue que $I = S$ y por consiguiente S es simple. Ahora bien, sean I y J ideales izquierdo y derecho minimales, respectivamente, de T. Según la Proposición 3.9.7 $f^{-1}(I)$ debe ser un ideal izquierdo de S. Más aún, si I' es cualquier ideal izquierdo de S para el cual $I' \subseteq f^{-1}(I)$, entonces $f(I') \subseteq f(f^{-1}(I)) \subseteq I$. De esto último y de que $f(I')$ sea un ideal izquierdo de T se sigue que $f(I') = I$ y por lo tanto $I' = f^{-1}(I)$. Podemos concluir que $f^{-1}(I)$ es un ideal izquierdo minimal de S. De forma análoga se exhibe que $f^{-1}(J)$ es un ideal derecho minimal de S y por consiguiente S es completamente simple.

□

La siguiente proposición proporciona el primer ejemplo de semigrupos completamente simples.

Proposición 8.2.7.

Todo semigrupo de la forma $\mathcal{M}(G, A, B, \mathcal{P})$ es completamente simple.

Demostración. En esta demostración escribiremos $\mathcal{M}$ en lugar de $\mathcal{M}(G, A, B, \mathcal{P})$. **Afirmación 1):** Si I es ideal izquierdo de $\mathcal{M}$ y $(a, g, b) \in I$, entonces para cada $x \in A$ y cada $h \in G$ se tiene que $(x, h, b) \in I$. En efecto, de que I sea un ideal izquierdo se sigue que $(x, hg^{-1}\mathcal{P}(b, a)^{-1}, b)(a, g, b) \in I$, pero $(x, hg^{-1}\mathcal{P}(b, a)^{-1}, b)(a, g, b) = (x, hg^{-1}\mathcal{P}(b, a)^{-1}\mathcal{P}(b, a)g, b) = (x, h, b)$. Por consiguiente $(x, h, b) \in I$. **Afirmación 2):** Si J es ideal derecho de $\mathcal{M}$ y $(a, g, b) \in J$, entonces para cada $y \in B$ y cada $h \in G$ se tiene que $(a, h, y) \in J$. En efecto, como J es un ideal derecho, entonces $(a, g, b)(a, \mathcal{P}(b, a)^{-1}g^{-1}h, y) \in J$, pero $(a, g, b)(a, \mathcal{P}(b, a)^{-1}g^{-1}h, y) = (a, g\mathcal{P}(b, a)\mathcal{P}(b, a)^{-1}g^{-1}h, y) = (a, h, y)$. Por consiguiente $(a, h, y) \in J$. **Afirmación 3):** $\mathcal{M}$ es simple. En efecto, sea I un ideal bilátero de $\mathcal{M}$ y tómese $(a, g, b) \in I$. De las afirmaciones anteriores se deduce que si $(x, h, y) \in \mathcal{M}$ es arbitrario, entonces $(x, \mathcal{P}(b, a)^{-1}, b) \in I$ y $(a, h, y) \in I$. En consecuencia $(x, h, y) = (x, \mathcal{P}(b, a)^{-1}, b)(a, h, y) \in I$ y por lo tanto $I = \mathcal{M}$. De ahí que $\mathcal{M}$ es simple. **Afirmación 4):** Todo ideal principal izquierdo es un ideal izquierdo minimal. En efecto, sea $\bar{u} := (x, h, y) \in \mathcal{M}$ arbitrario. Es preciso mostrar que $\mathcal{M}\bar{u}$ es un ideal izquierdo minimal. Para ello, suponga que I es un ideal izquierdo tal que $I \subseteq \mathcal{M}\bar{u}$. Tómese $(a, g, b) \in I$. De la afirmación 1) se sigue que $(x, h, b) \in I$. Ahora bien, como $I \subseteq \mathcal{M}\bar{u}$, entonces puede escribirse $(x, h, b) = (c, k, d)(x, h, y)$ para algún $(c, k, d) \in \mathcal{M}$. De ahí que $(x, h, b) = (c, k\mathcal{P}(d, x)h, y)$ y en consecuencia $b = y$. Así $\bar{u} := (x, h, y) = (x, h, b) \in I$ y por consiguiente $\mathcal{M}\bar{u} \subseteq I$. Se concluye que $\mathcal{M}\bar{u} = I$ y por lo tanto $\mathcal{M}\bar{u}$ es un ideal izquierdo minimal. Usando un argumento similar a este se puede mostrar que todo ideal principal derecho de $\mathcal{M}$ es un ideal derecho minimal. Así, de todo lo anterior se concluye que $\mathcal{M}$ es completamente simple.

□

Corolario 8.2.8.

Toda banda rectangular es un semigrupo completamente simple.

Demostración. Se sigue de las Proposiciones 8.1.1, 8.2.6 y 8.2.7.

□

Así, los semigrupos matriz de Rees sobre un grupo son una especie de fábrica generadora de semigrupos completamente simples. A continuación haremos una pequeña digresión para revisar un sencillo pero útil resultado sobre ideales.

Proposición 8.2.9.

Sea S un semigrupo y suponga que I y J son ideales izquierdo y derecho respectivamente. Entonces

1. $JI \subseteq I \cap J$, y por consiguiente $I \cap J \neq \emptyset$.
2. Si todo elemento de $I \cap J$ es regular entonces $JI = I \cap J$.
3. IJ es un ideal bilátero de S.

4. Para cada $\emptyset \neq X \subseteq S$ el conjunto IXJ es un ideal bilátero de S. (Cuando $X = \{a\}$ se escribe IaJ en lugar de $I\{a\}J$)

Demostración. 1) Recordar que $JI := \{ji | i \in I \text{ y } j \in J\}$. Si $a \in JI$, entonces $a = ji$ para algunos $i \in I$ y $j \in J$. Como I es ideal izquierdo, entonces $a = ji \in I$, y puesto que J es ideal derecho, entonces $a = ji \in J$. De ahí que $a \in I \cap J$ y por consiguiente $JI \subseteq I \cap J$. 2) Sea $a \in I \cap J$. Por hipótesis debe existir $x \in S$ para el cual $a = axa$. Debido a que I es ideal izquierdo, entonces $xa \in I$. Así que $a = a(xa) \in JI$ y por consiguiente $JI = I \cap J$. 4) Sean $x \in S$ y $a \in IXJ$. Entonces $a = itj$ para algunos $i \in I$, $j \in J$ y $t \in X$. De ahí que $xa = x(itj) = (xi)tj$, pero como $xi \in I$, entonces $xa \in IXJ$. Por otro lado, $ax = (itj)x = it(jx)$ con $jx \in J$. Luego $ax \in IXJ$. Por consiguiente IXJ es un ideal bilátero. La prueba de 3) es similar a esta y se omite.

□

Ahora bien, aparte de la misma definición ¿bajo qué condiciones se puede implicar que un semigrupo es completamente simple? En el sentido de esta pregunta es que van los siguientes tres resultados.

Proposición 8.2.10.

Si un semigrupo simple contiene al menos un idempotente minimal, entonces el semigrupo debe ser completamente simple.

Demostración. Sea S un semigrupo simple y sea α un idempotente minimal. La prueba consiste en exhibir que S contiene un ideal izquierdo y uno derecho minimal. **Afirmación:** $S\alpha$ es un ideal izquierdo minimal. En efecto, suponga que I es un ideal izquierdo de S tal que $I \subseteq S\alpha$. Tómese $x \in I$. Entonces $Sx \subseteq I$ y además $x = s\alpha$ para algún $s \in S$. De ahí que $x = x\alpha$. Ahora bien, puesto que S es simple y debido a que $S\alpha x\alpha S$ es un ideal bilátero (ver Proposición 8.2.9) se deduce que $S = S\alpha x\alpha S$. Por otra parte, como $\alpha \in S$, entonces puede escribirse $\alpha = p\alpha x\alpha q$ para algunos $p, q \in S$. Hágase $u := p\alpha$ y $v := \alpha q$. No es difícil ver que $u = u\alpha$ y $v = \alpha v$. Entonces $\alpha = uxv$ con $u\alpha = u$ y $\alpha v = v$. Sea $\beta := v\alpha ux$. Observe que

$$\begin{aligned} \beta^2 &= (v\alpha ux)(v\alpha ux) \\ &= v\alpha(uxv)\alpha ux \\ &= v\alpha\alpha\alpha ux \\ &= v\alpha ux \\ &= \beta \end{aligned}$$

Por lo tanto β es un idempotente. Más aún, $\alpha\beta = \alpha(v\alpha ux) = (\alpha v)\alpha ux = v\alpha ux = \beta$ y a la vez $\beta\alpha = (v\alpha ux)\alpha = v\alpha u(x\alpha) = v\alpha ux = \beta$. Por consiguiente $\beta \leq \alpha$, y al ser α idempotente minimal, entonces $\alpha = \beta$. De ahí que $\alpha = v\alpha ux \in Sx \subseteq I$ y en consecuencia $\alpha \in I$. Por lo tanto $S\alpha \subseteq I$ y en definitiva $I = S\alpha$. Se concluye que $S\alpha$ es un ideal izquierdo minimal. Usando un argumento análogo a este (haciendo ahora $\beta := xv\alpha u$) se muestra que αS es un ideal derecho minimal. Por consiguiente S es completamente simple.

□

Proposición 8.2.11.

Todo semigrupo simple y completamente regular debe ser completamente simple.

Demostración. Sea S un semigrupo simple y completamente regular. Mostraremos que bajo estas hipótesis todo idempotente de S es minimal: sean α y β idempotentes tales que $\alpha \leq \beta$. Luego, $\alpha\beta = \alpha = \beta\alpha$. Por otro lado, puesto que S es simple, entonces $S = S\alpha\alpha\alpha S$, y debido a que $\beta \in S$ puede escribirse $\beta = p\alpha\alpha\alpha q$ para algunos $p, q \in S$. Hágase $u := p\alpha$ y $v := \alpha q$. No es difícil ver que $u = u\alpha$ y $v = \alpha v$. De lo anterior se tiene que $\beta = u\alpha v$ con $u\alpha = u$ y $\alpha v = v$. Observe que, entonces $\beta = u\alpha v = u(\alpha\beta)v = (u\alpha)\beta v = u\beta v$ i,e, $\beta = u\beta v$. Enseguida, y debido a que la prueba se basa en ellas, enlistaremos las identidades hasta aquí obtenidas

$$\alpha\beta = \alpha = \beta\alpha \tag{8.2}$$
$$\beta = u\alpha v \tag{8.3}$$
$$\beta = u\beta v \tag{8.4}$$

Ahora bien, de que S sea completamente regular se sigue que existen $\gamma, \delta \in E(S)$ tales que $u \in H_\gamma$ y $v \in H_\delta$ (ver Proposición 7.3.12). De la identidad (8.3) se obtiene que $\gamma\beta = \gamma(u\alpha v) = (\gamma u)\alpha v = u\alpha v = \beta$ y a la vez $\beta\delta = (u\alpha v)\delta = u\alpha(v\delta) = u\alpha v = \beta$. Por lo tanto $\gamma\beta = \beta = \beta\delta$. De esto último se sigue que $\gamma\beta\alpha = \beta\alpha$ y $\alpha\beta\delta = \alpha\beta$, lo que combinado con (8.2) resulta en que $\gamma\alpha = \alpha = \alpha\delta$. Por otro lado, sea u^{-1} el inverso de u en el grupo H_γ y sea v^{-1} el inverso de v en el grupo H_δ. De (8.3) se deduce que $u^{-1}\beta v^{-1} = u^{-1}(u\alpha v)v^{-1} = (u^{-1}u)\alpha(vv^{-1}) = \gamma\alpha\delta = (\gamma\alpha)\delta = \alpha\delta = \alpha$, o lo que es lo mismo $u^{-1}\beta v^{-1} = \alpha$. En cuanto a la igualdad (8.4), de ella se desprende que $u^{-1}\beta v^{-1} = u^{-1}(u\beta v)v^{-1} = (u^{-1}u)\beta(vv^{-1}) = \gamma\beta\delta = (\gamma\beta)\delta = \beta\delta = \beta$ y por lo tanto $u^{-1}\beta v^{-1} = \beta$. Así, tenemos simultáneamente que $u^{-1}\beta v^{-1} = \alpha$ y $u^{-1}\beta v^{-1} = \beta$ y por consiguiente $\alpha = \beta$. Se concluye que todo idempotente de S es minimal. Para deducir que S es completamente simple solo bastará con aplicar la Proposición 8.2.10. □

Proposición 8.2.12.

Si en un semigrupo regular todo idempotente es minimal, entonces el semigrupo debe ser completamente simple.

Demostración. Sea S un semigrupo regular en el que cualquiera de sus idempotentes es minimal. **Afirmación 1:** Todo ideal izquierdo (derecho) de S contiene idempotentes. En efecto, sea I un ideal izquierdo (J un ideal derecho) y tómese $a \in I$ ($a \in J$). Puesto que S es regular, entonces existe $x \in S$ tal que $a = axa$. De ahí que $xa \in E(S)$ ($ax \in E(S)$), pero debido a que $a \in I$ ($a \in J$) se sigue entonces que $xa \in I$ ($ax \in J$). Por consiguiente I (J) contiene idempotentes. **Afirmación 2:** La intersección de cualquier ideal izquierdo con cualquier ideal derecho contiene idempotentes. En efecto, sea I un ideal izquierdo y sea J un ideal derecho. Tomemos $\alpha \in I$ y $\beta \in J$ ambos idempotentes y sea x un pseudoinverso de $\alpha\beta$. Entonces $g := \beta x\alpha\beta x\alpha$ es un idempotente (véase la demostración de la Proposición 7.3.7). Si $u := \beta x\alpha\beta x$ y $v := x\alpha\beta x\alpha$, entonces es claro que $g = u\alpha$ y $g = \beta v$. De ahí que

$g \in I$ y $g \in J$. Por lo tanto $g \in I \cap J$ y así la intersección $I \cap J$ contiene idempotentes. **Afirmación 3:** Para cada $\alpha \in E(S)$ el ideal $S\alpha$ es un ideal izquierdo minimal y el ideal αS es un ideal derecho minimal. En efecto, sean I un ideal izquierdo y J un ideal derecho tales que $I \subseteq S\alpha$ y $J \subseteq \alpha S$. Entonces $I \cap J \subseteq S\alpha \cap \alpha S = M_\alpha$ (véase Observación 7.1.10). Tómese $\beta \in I \cap J$ idempotente, entonces $\beta \in M_\alpha$, y debido a que M_α es un monoide con neutro α ha de suceder que $\beta\alpha = \beta = \alpha\beta$ y por lo tanto $\beta \leq \alpha$. Así, como todo idempotente se supone minimal se sigue que $\beta = \alpha$. De ahí que $\alpha \in I \cap J$ y en consecuencia $S\alpha \subseteq I$ y $\alpha S \subseteq J$. Por consiguiente $I = S\alpha$, $J = \alpha S$ y la afirmación queda establecida. **Afirmación 4:** Para cada $x \in S$ el ideal Sx es un ideal izquierdo minimal y el ideal xS es un ideal derecho minimal. En efecto, si $x \in S$ de la Proposición 7.3.9 se sigue que existen $\alpha, \beta \in E(S)$ para los cuales $x\mathcal{L}\alpha$ y $x\mathcal{R}\beta$, o lo que es lo mismo, tales que $Sx = S\alpha$ y $xS = \beta S$. De esto último y de la afirmación 3 se sigue lo deseado. Hasta este punto, para establecer que S es completamente simple solo resta averiguar si S es simple. Si podemos exhibir eso la demostración quedará completa. **Afirmación 5:** S es simple. En efecto, sean $a, b \in S$ arbitrarios. Observar que $ab \in Sb$ y $ba \in Sa$. De ahí que $Sab \subseteq Sb$ y $Sba \subseteq Sa$. Por lo tanto, de la afirmación 4 se sigue que $Sab = Sb$ y $Sba = Sa$. Así $a \in Sa = Sba$, $b \in Sb = Sab$ y en consecuencia puede escribirse $a = xba$ y $b = yab$ para algunos $x, y \in S$, de manera que de la Proposición 7.3.15 se deduce que $SaS = SbS$ y por lo tanto $a\mathcal{J}b$. Podemos concluir así que $S \times S = \mathcal{J}$ y por consiguiente, de la Proposición 8.2.3 se sigue que S es un semigrupo simple. □

Observación 8.2.13.

Recordar que si α es un idempotente del semigrupo S, entonces la $\mathcal{H}$-clase de α, H_α, coincide con el grupo del idempotente α, el cual es un grupo bajo la misma operación de S. Además, el elemento neutro de tal grupo es el propio α, de manera que α se comporta como tal para cualquier elemento de H_α. Así mismo, todo elemento de H_α debe tener un inverso con respecto del neutro α. Más aún, puesto que un grupo no contiene otro idempotente salvo su elemento neutro, se sigue que el único idempotente que pertenece a H_α es el propio α. Quizá lo anteriormente dicho suene solo a la repetición de la definición de grupo, pero lo que se trata de decir es que si un semigrupo contiene al menos un elemento idempotente, entonces sin importar las carencias que tal semigrupo tenga, este se comportará localmente como un grupo. El uso de las virtudes de las $\mathcal{H}$-clases de elementos idempotentes ya se ha podido observar en la prueba de la Proposición 8.2.11 y tales atributos se seguirán usando en lo posterior •

Hasta ahora se han establecido algunas condiciones que implican que un semigrupo sea completamente simple, pero ¿qué propiedades tienen los semigrupos completamente simples?, ¿serán ciertos los recíprocos de las tres proposiciones anteriores? La siguiente proposición será de utilidad con el fin de contestar estas preguntas.

Proposición 8.2.14.

Sea S un semigrupo y suponga que I es un ideal izquierdo minimal y que J es un ideal derecho minimal. Entonces

1. Todo elemento de $I \cap J$ es regular, y por lo tanto $I \cap J = JI$.
2. $I \cap J$ contiene idempotentes, más aún, $I \cap J$ contiene un solo idempotente el cual debe ser minimal.
3. Para cada $x \in I$ ocurre que $L_x = I = S^1x$.
4. Para cada $y \in J$ ocurre que $R_y = J = yS^1$.
5. $I \cap J$ es un grupo. Más precisamente $I \cap J = H_\alpha$ para algún idempotente α.

Demostración. **Afirmación:** Para cada $a \in I \cap J$ existen $x, y \in S$ tales que $a^2y = a = xa^2$ y $ay = xa$. En efecto, tómese $a \in I \cap J$ arbitrario. Al ser I y J ideales: izquierdo y derecho respectivamente, se deduce que $a^2 \in I \cap J$. De ahí que $a^2 \in I$ y $a^2 \in J$ y por consiguiente $Sa^2 \subseteq I$ y $a^2S \subseteq J$. Ahora bien, puesto que I es un ideal izquierdo minimal y J es un ideal derecho minimal se sigue que $Sa^2 = I$ y $a^2S = J$. Así que $a \in Sa^2$ y $a \in a^2S$, de manera que puede escribirse $a = xa^2$ y $a = a^2y$ para algunos $x, y \in S$. De estas igualdades se desprende que $ay = (xa^2)y = x(a^2y) = xa$ i,e, $ay = xa$. Por consiguiente la afirmación queda establecida. **1) y 2)** Sea $a \in I \cap J$. Entonces de acuerdo a lo anterior, deben existir $x, y \in S$ para los cuales $a^2y = a = xa^2$ y $ay = xa$. Así que $axa = a(xa) = a(ay) = a^2y = a$ i,e $a = axa$ (por consiguiente todo elemento de $I \cap J$ es regular, y en consecuencia $I \cap J = JI$), de ahí que $xa \in E(S)$. Ahora bien, observe que como $a \in I$, entonces $xa \in I$, y también como $a \in J$, entonces $ay \in J$, pero $ay = xa$. Por consiguiente xa es un idempotente que pertenece a $I \cap J$. Se concluye que $I \cap J$ contiene idempotentes. **Afirmación:** Si α es un idempotente tal que $\alpha \in I \cap J$, entonces $I \cap J = M_\alpha$. En efecto, si $\alpha \in I \cap J$, entonces $\alpha \in I$ y $\alpha \in J$ y por lo tanto $S\alpha \subseteq I$ y $\alpha S \subseteq J$. De ahí que $S\alpha = I$ y $\alpha S = J$. Así que $S\alpha \cap \alpha S = I \cap J$, o lo que es lo mismo $I \cap J = M_\alpha$ (véase Observación 7.1.10). Suponga que α y β son idempotentes que pertenecen a $I \cap J$. De la anterior afirmación se sigue que $M_\alpha = I \cap J = M_\beta$ y por lo tanto $M_\alpha = M_\beta$. De ahí que $\alpha \in M_\beta$ y $\beta \in M_\alpha$, y puesto que M_α y M_β son monoides con neutros α y β respectivamente, se deduce que $\alpha\beta = \alpha$ y a la vez $\alpha\beta = \beta$. Por consiguiente $\alpha = \beta$ y así puede concluirse que $I \cap J$ contiene exactamente un idempotente, digamos α. Debido a que α es el único idempotente que pertenece a $I \cap J = M_\alpha$ se sigue entonces que $M_\alpha \cap E(S) = \{\alpha\}$, de manera que la Proposición 7.1.9 permite concluir que α es un idempotente minimal. **4)** Sea $y \in J$ arbitrario. Entonces $yS^1 \subseteq J$ y por lo tanto $yS^1 = J$. Ahora bien, para cada $b \in R_y$ sucede que $b \in bS^1 = yS^1 = J$, de donde se ve que todo elemento de R_y pertenece a J y por consiguiente $R_y \subseteq J$. Por otro lado si $b \in J$, entonces $bS^1 \subseteq J$ y así $bS^1 = J = yS^1$. De ahí que $b \in R_y$ y en consecuencia $J \subseteq R_y$. En definitiva $R_y = J = yS^1$ siempre que $y \in J$. La prueba de **3)** es similar a esta y se omite. **5)** Sea α el único idempotente de $I \cap J$. Entonces de **3)** y **4)** se sigue que $I = L_\alpha$ y $J = R_\alpha$, de manera que $I \cap J = L_\alpha \cap R_\alpha = H_\alpha$. □

Proposición 8.2.15.

Sea S un semigrupo completamente simple y sean I un ideal izquierdo minimal y J un ideal derecho minimal. Entonces:

1. $S = IH_\alpha J$ con $I \cap J = H_\alpha = JI$ y α idempotente minimal.

2. Si $a, c \in I$, $g, h \in H_\alpha$ y $b, d \in J$ son tales que $agb = chd$, entonces $aS = cS$ y $Sb = Sd$.

3. S es completamente regular.

4. Para cada $x \in S$, Sx es ideal izquierdo minimal y xS es ideal derecho minimal.

Demostración. Suponga que S es un semigrupo completamente simple. Luego, S debe contener ideales minimales izquierdo y derecho. Sea I un ideal izquierdo minimal y sea J un ideal derecho minimal. De la Proposición 8.2.14 puede concluirse que $JI = I \cap J = H_\alpha$ para algún α idempotente minimal. Como $\alpha \in I \cap J$ de la Proposición 8.2.14 se desprende que $I = S\alpha$ y $J = \alpha S$. Así si $x \in I$, entonces $x = t\alpha$ para algún $t \in S$, de manera que $x\alpha = t\alpha^2 = \alpha = x$ i,e, para cada $x \in I$ se satisface que $x = x\alpha$. De manera análoga se verifica que $y = \alpha y$ para cada $y \in J$. Ahora bien, como S es simple y debido a que $IH_\alpha J$ es un ideal bilátero se sigue que $S = IH_\alpha J$. Así, todo elemento de S es de la forma agb para algunos $a \in I$, $g \in H_\alpha$ y $b \in J$. Con respecto a que H_α es un grupo, para cada $g \in H_\alpha$ denotemos por g^{-1} al inverso de g en el grupo H_α. Así, de que $JI = H_\alpha$ se ve que si $a \in I$ y $b \in J$, entonces $ba \in JI = H_\alpha$ de forma que puede considerarse a su inverso $(ba)^{-1}$. En particular, si $a \in I$ y $b \in J$, entonces αa y $b\alpha$ deben ser ambos miembros del grupo H_α. Para $a \in I$ se tiene que $(\alpha a)^{-1}(\alpha a) = \alpha$, pero puesto que α es el neutro de H_α y $(\alpha a)^{-1} \in H_\alpha$, entonces $(\alpha a)^{-1}\alpha = (\alpha a)^{-1}$, de donde $\alpha = (\alpha a)^{-1}(\alpha a) = [(\alpha a)^{-1}\alpha]a = (\alpha a)^{-1}a$ i,e, para cada $a \in I$, $(\alpha a)^{-1}a = \alpha$. De manera análoga, se sigue que para cada $b \in J$, $b(b\alpha)^{-1} = \alpha$. **Afirmación :** Si $a, c \in I$, $g, h \in H_\alpha$ y $b, d \in J$ son tales que $agb = chd$, entonces $aS^1 = cS^1$ y $S^1b = S^1d$. En efecto

$$\begin{aligned}
& agb = chd \\
\Longrightarrow \quad & agb(b\alpha)^{-1} = chd(b\alpha)^{-1} \\
\Longrightarrow \quad & ag\alpha = chd(b\alpha)^{-1} \\
\Longrightarrow \quad & ag = chd(b\alpha)^{-1} \\
\Longrightarrow \quad & agg^{-1} = chd(b\alpha)^{-1}g^{-1} \\
\Longrightarrow \quad & a\alpha = chd(b\alpha)^{-1}g^{-1} \\
\Longrightarrow \quad & a = chd(b\alpha)^{-1}g^{-1}
\end{aligned}$$

mientras que

$$\begin{aligned} & agb = chd \\ \Longrightarrow \quad & agb(d\alpha)^{-1} = chd(d\alpha)^{-1} \\ \Longrightarrow \quad & agb(d\alpha)^{-1} = ch\alpha \\ \Longrightarrow \quad & agb(d\alpha)^{-1} = ch \\ \Longrightarrow \quad & agb(d\alpha)^{-1}h^{-1} = chh^{-1} \\ \Longrightarrow \quad & agb(d\alpha)^{-1}h^{-1} = c\alpha \\ \Longrightarrow \quad & agb(d\alpha)^{-1}h^{-1} = c \end{aligned}$$

Asi, de la Proposición 7.2.7 se concluye que $aS^1 = cS^1$. De manera similar se muestra que $S^1b = S^1d$. Por otra parte, para cada $a \in I$ y para cada $b \in J$ se tiene que $a(ba)^{-1}b$ es idempotente, pues $[a(ba)^{-1}b][a(ba)^{-1}b] = a(ba)^{-1}[(ba)(ba)^{-1}]b = a(ba)^{-1}\alpha b = a(ba)^{-1}b$. Tómese $x \in S$ arbitrario. Entonces puede escribirse $x = agb$ para algunos $a \in I$, $g \in H_\alpha$ y $b \in J$. Sea $y := a(ba)^{-1}g^{-1}(ba)^{-1}b$. Entonces

$$\begin{aligned} xy &= (agb)[a(ba)^{-1}g^{-1}(ba)^{-1}b] \\ &= ag(ba)(ba)^{-1}g^{-1}(ba)^{-1}b \\ &= ag\alpha g^{-1}(ba)^{-1}b \\ &= agg^{-1}(ba)^{-1}b \\ &= a\alpha(ba)^{-1}b \\ &= a(ba)^{-1}b \end{aligned}$$

y

$$\begin{aligned} yx &= [a(ba)^{-1}g^{-1}(ba)^{-1}b](agb) \\ &= a(ba)^{-1}g^{-1}(ba)^{-1}(ba)gb \\ &= a(ba)^{-1}g^{-1}\alpha gb \\ &= a(ba)^{-1}g^{-1}gb \\ &= a(ba)^{-1}\alpha b \\ &= a(ba)^{-1}b \end{aligned}$$

Por consiguiente $xy = yx$ y así y conmuta con x. Más aún

$$\begin{aligned} xyx &= (xy)x \\ &= [a(ba)^{-1}b](agb) \\ &= a(ba)^{-1}(ba)gb \\ &= a\alpha gb \\ &= agb \\ &= x \end{aligned}$$

De ahí que y es un pseudoinverso conmutativo de x. De que $x \in S$ fue elegido arbitrariamente puede concluirse que S es completamente regular. De esto último y de acuerdo con la Observación 7.3.6 las equivalencias de Green para S toman la forma:

$$\begin{aligned} a\mathcal{L}b &\iff Sa = Sb \\ a\mathcal{R}b &\iff aS = bS \\ a\mathcal{J}b &\iff SaS = SbS \end{aligned}$$

Afirmación: Para cada $a \in I$ y para cada $b \in J$, aS es un ideal derecho minimal y Sb es un ideal izquierdo minimal. En efecto, sea $a \in I$ y suponga que I' es un ideal derecho tal que $I' \subseteq aS$. Tómese $x \in I'$. Entonces $xS \subseteq I'$ y $x = at$ para algún $t \in S$. Ahora bien, como $S = IH_\alpha J$, entonces $t = chb$ para algunos $c \in I$, $h \in H_\alpha$, y $b \in J$, de manera que $x = at = (a\alpha)(chb) = a[(\alpha c)h]b$, pero $\alpha c \in JI = H_\alpha$, así que $g := (\alpha c)h \in H_\alpha$ y por consiguiente $x = agb$ con $a \in I$, $g \in H_\alpha$ y $b \in J$. Observe que

$$\begin{aligned} x[a(ba)^{-1}g^{-1}] &= (agb)[a(ba)^{-1}g^{-1}] \\ &= ag(ba)(ba)^{-1}g^{-1} \\ &= ag\alpha g^{-1} \\ &= agg^{-1} \\ &= a\alpha \\ &= a \end{aligned}$$

Por lo tanto a es de la forma xs con $s \in S$. De ello se sigue que $a \in xS$ y en consecuencia $aS \subseteq xS \subseteq I'$. Por consiguiente $aS \subseteq I'$ y en definitiva $I' = aS$. Se concluye que aS es un ideal derecho minimal. Con una técnica totalmente análoga a esta y haciendo las modificaciones pertinentes se exhibe que si $b \in J$, entonces Sb es un ideal izquierdo minimal. A partir de esto puede mostrarse que para cada $x \in S$, Sx es un ideal izquierdo minimal y xS es un ideal derecho minimal. En efecto, tómese $x \in S$ arbitrario. Entonces $x = agb$ para algunos $a \in I$, $g \in H_\alpha$ y $b \in J$. De ahí que $x \in aS$ y $x \in Sb$, de donde $xS \subseteq aS$ y $Sx \subseteq Sb$. Así que de la afirmación anterior se sigue que $Sx = Sb$ y $xS = aS$ y por consiguiente Sx es ideal izquierdo minimal y xS es ideal derecho minimal. □

Corolario 8.2.16.

Si S es un semigrupo completamente simple, entonces:

1. Para cada $x, y \in S$ se tiene que $Sx \cap yS$ es un grupo. Más precisamente $Sx \cap yS = H_\alpha$ para algún α idempotente minimal.
2. $\mathcal{D} = S \times S$.
3. Todo idempotente de S debe ser minimal.

Demostración. Sean $x, y \in S$. De acuerdo con la Proposición 8.2.15 $I := Sx$ es un ideal izquierdo minimal y $J := yS$ es un ideal derecho minimal. Así que de la Proposición 8.2.14 se sigue que $Sx \cap yS = H_\alpha$ para algún idempotente minimal α. Más aún, de la Proposición 8.2.14 se sigue que $L_x = Sx$ y $R_y = yS$, de donde $L_x \cap R_y = Sx \cap yS = H_\alpha \neq \emptyset$. Tómese $u \in L_x \cap R_y$. Entonces $y\mathcal{R}u$ y $u\mathcal{L}x$, o lo que es lo mismo $y\mathcal{D}x$. De ahí que $\mathcal{D} = S \times S$. Finalmente, para cada $\alpha \in E(S)$ se tiene que $M_\alpha = S\alpha \cap \alpha S = L_\alpha \cap R_\alpha = H_\alpha$, de donde $M_\alpha \cap E(S) = H_\alpha \cap E(S) = \{\alpha\}$. Por consiguiente, de la Proposición 7.1.9 se deduce que cada idempotente de S es minimal. □

La Proposicion 8.2.15 y el Corolario 8.2.16 permiten concluir que los recíprocos de las Proposiciones 8.2.10, 8.2.11 y 8.2.12 son todos verdaderos. Así, se tiene lo siguiente.

Teorema. 8.2.17.

Los siguientes enunciados son equivalentes para un semigrupo S.

1. S es completamente simple.
2. S es simple y contiene al menos un idempotente minimal.
3. S es simple y completamente regular.
4. S es regular y todo idempotente es minimal •

Sea S un semigrupo completamente simple. De acuerdo con la Proposición 8.2.15 S es también completamente regular. Así, de acuerdo con la Observación 7.3.13 la colección

$$\mathcal{F} := \{H_\alpha \mid \alpha \in E(S)\}$$

constituye una partición de S. Sin embargo, en este caso, todos los miembros de $\mathcal{F}$ tienen el mismo tamaño como se establece adelante.

Proposición 8.2.18.

Si S es un semigrupo completamente simple, entonces para cada $\alpha, \beta \in E(S)$ los grupos H_α y H_β son equipotentes.

Demostración. Antes que nada observe primero que si γ es idempotente, entonces $H_\gamma = L_\gamma \cap R_\gamma = S\gamma \cap \gamma S = \{\gamma x \gamma \mid x \in S\}$ (véanse las Proposiciones 8.2.14 y 8.2.15 y la Observación 7.1.10). Ahora, sean $\alpha, \beta \in E(S)$ y tómense $u \in S\alpha \cap \beta S$ y $v \in \alpha S \cap S\beta$ arbitrarios. Entonces, de acuerdo al inciso 4 de la Proposición 8.2.15 y a los incisos 3 y 4

de la Proposición 8.2.14 debe suceder que $S\alpha = Su$, $\alpha S = vS$, $\beta S = uS$ y $S\beta = Sv$. De estas igualdades se desprende que

$$\alpha = au \tag{8.5}$$
$$u = b\alpha \tag{8.6}$$
$$\alpha = vp \tag{8.7}$$
$$v = \alpha q \tag{8.8}$$
$$u = \beta c \tag{8.9}$$
$$v = r\beta \tag{8.10}$$

para algunos $a, b, c, p, q, r \in S$. Ahora bien, de las igualdades (8.6),(8.8), (8.9) y (8.10) se sigue que

$$u\alpha = u \tag{8.11}$$
$$\alpha v = v \tag{8.12}$$
$$\beta u = u \tag{8.13}$$
$$v\beta = v \tag{8.14}$$

Observar que si $g \in H_\alpha$, entonces $ugv = (\beta u)g(v\beta) = \beta(ugv)\beta \in H_\beta$. Por lo tanto tiene sentido considerar a la función $f : H_\alpha \longrightarrow H_\beta$ definida por $f(g) := ugv$. **Afirmación:** f es biyectiva. En efecto, suponga que $g, h \in H_\alpha$ son tales que $f(g) = f(h)$. Entonces $ugv = uhv$ de manera que $a(ugv)p = a(uhv)p$, de donde $(au)g(vp) = (au)h(vp)$. De esta última igualdad y de (8.5) y (8.7) se sigue que $\alpha g\alpha = \alpha h\alpha$ y en consecuencia $g = h$. Por consiguiente f es inyectiva. Por otra parte, de que $\beta S = uS$ y $S\beta = Sv$ se desprende que $H_\beta = \beta S \cap S\beta = uS \cap Sv = (uS)(Sv)$. Así si $t \in H_\beta$, entonces $t = uxv$ para algún $x \in S$, pero de acuerdo a (8.11) y (8.12), $t = (u\alpha)x(\alpha v) = u(\alpha x\alpha)v$ con $\alpha x\alpha \in H_\alpha$. Por consiguiente $t = f(\alpha x\alpha)$ y en consecuencia f es sobreyectiva. En definitiva f es una biyección. □

Una característica sobresaliente de la demostración anterior es que construye una función biyectiva a partir de dos elementos elegidos arbitrariamente. Más precisamente, si $u \in S\alpha \cap \beta S$ y $v \in \alpha S \cap S\beta$, entonces la función $f : H_\alpha \longrightarrow H_\beta$ definida por $f(g) := ugv$ es una biyección. Por otro lado, resulta que las $\mathcal{H}$-clases de elementos idempotentes en un semigrupo completamente simple no solo son equipotentes, sino que también son isomorfas entre sí como grupos. Para demostrar este hecho nos apoyaremos del siguiente resultado.

Proposición 8.2.19.

Sea S un semigrupo completamente simple. Si $\alpha, \beta \in E(S)$, entonces para cada $u \in S\alpha \cap \beta S$ existe $v \in \alpha S \cap S\beta$ tal que $vu = \alpha$ y $uv = \beta$.

Demostración. Sea $u \in S\alpha \cap \beta S$. Puesto que $S\alpha$ y βS son ideales izquierdo y derecho minimales, se sigue que $Su = S\alpha$ y $uS = \beta S$. De ahí que existen $x, y, z, w \in S$ para los cuales

$$u = x\alpha \tag{8.15}$$
$$\alpha = yu \tag{8.16}$$
$$u = \beta z \tag{8.17}$$
$$\beta = uw \tag{8.18}$$

De (8.15) se sigue que $u\alpha = x\alpha^2 = x\alpha = u$, lo que combinado con (8.16) resulta en que $u = uyu$. Por otra parte, de (8.17) se sigue que $\beta u = \beta^2 z = \beta z = u$, lo que en conjunto con (8.18) da como resultado que $u = uwu$. Sea $v := yuw$. Observe que de acuerdo a (8.16) puede escribirse $v = \alpha w$, mientras que de acuerdo a (8.18), $v = y\beta$. Por consiguiente $v \in \alpha S \cap S\beta$. Finalmente,

$$\begin{aligned} uv &= u(yuw) \\ &= (uyu)w \\ &= uw \\ &= \beta \end{aligned}$$

y

$$\begin{aligned} vu &= (yuw)u \\ &= y(uwu) \\ &= yu \\ &= \alpha \end{aligned}$$

□

Corolario 8.2.20.

Si S es un semigrupo completamente simple, entonces para cada $\alpha, \beta \in E(S)$ se tiene que $H_\alpha \cong H_\beta$.

Demostración. Elíjase $u \in S\alpha \cap \beta S$. Entonces debe existir $v \in \alpha S \cap S\beta$ para el cual $vu = \alpha$. De acuerdo a la demostración de la Proposición 8.2.18 la función $f : H_\alpha \longrightarrow H_\beta$ dada por $f(g) := ugv$ debe ser biyectiva. Más aún, se tiene que para cada $g, h \in H_\alpha$

$$\begin{aligned} f(g)f(h) &= (ugv)(uhv) \\ &= ug(vu)hv \\ &= ug\alpha hv \\ &= ughv \\ &= f(gh) \end{aligned}$$

Por consiguiente f es un isomorfismo de grupos y el resultado se sigue. □

8.3. Teorema de Lagrange para semigrupos

Recordar que un Teorema de Lagrange sobre grupos finitos afirma que el orden de todo subgrupo de un grupo finito es un divisor del orden del grupo. Los semigrupos finitos y completamente simples también cuentan con tal atributo. Antes de formalizar esto último, se revisa una propiedad más de las $\mathcal{H}$-clases de elementos idempotentes.

Proposición 8.3.1.

Sea S un semigrupo y $H \subseteq S$. Suponga que H es un grupo bajo la misma operación de S y sea α el elemento neutro de H. Entonces $H \subseteq H_\alpha$.

Demostración. Se tiene que $H_\alpha = \{x \in M_\alpha \mid xx' = \alpha = x'x \text{ para algún } x' \in S\}$ (Véase Proposición 7.1.8). Ahora bien, debido a que H es un grupo con neutro α, entonces para cada $x \in H$ debe suceder que $x\alpha = x = \alpha x$ y $xx' = \alpha = x'x$ para algún $x' \in H$. De esto se sigue que $H \subseteq H_\alpha$. □

Así, si α es un idempotente del semigrupo S, entonces H_α es el grupo más grande que contiene a α en el sentido de que cualquier subgrupo de S que tenga a α como elemento debe estar contenido en H_α.

Teorema. 8.3.2. *De Lagrange para semigrupos.*

Sea S un semigrupo finito y completamente simple. Entonces

1. Para cada $\alpha \in E(S)$, $|S| = |H_\alpha||E(S)|$.
2. Si $H \subseteq S$ es un grupo bajo la misma operación de S entonces $|H|$ es un divisor de $|S|$.

Demostración. **1)** Según la Proposición 8.2.18 todas las $\mathcal{H}$-clases de elementos idempotentes deben tener el mismo número de elementos, digamos k. Así, $k = |H_\alpha|$ para cada $\alpha \in E(S)$. Ahora bien, puesto que todo semigrupo completamente simple es completamente regular, entonces la colección $\mathcal{F} := \{H_\alpha \mid \alpha \in E(S)\}$ es una partición de S, de manera que puede escribirse $S = \bigcup_{\alpha \in E(S)} H_\alpha$. De ahí que

$$\begin{aligned} |S| &= \left| \bigcup_{\alpha \in E(S)} H_\alpha \right| \\ &= \sum_{\alpha \in E(S)} |H_\alpha| \\ &= \sum_{\alpha \in E(S)} k \\ &= k|E(S)| \end{aligned}$$

Por consiguiente para cada $\alpha \in E(S)$, $|S| = |H_\alpha||E(S)|$.

2) Suponga que $H \subseteq S$ es un grupo bajo la misma operación de S y sea α el neutro de H. Entonces $H \subseteq H_\alpha$. En particular H es un subgrupo de H_α, de manera que por el terorema de Lagrange $|H|$ debe ser un divisor de $|H_\alpha|$, pero de acuerdo a 1) $|H_\alpha|$ es un divisor de $|S|$. Por consiguiente $|H|$ es un divisor de $|S|$. □

8.4. Un teorema de Rees

Después de haber revisado ya cierta cantidad de información sobre semigrupos completamente simples, es de notar que solo se ha dado un ejemplo de ellos, a saber, los semigrupos matriz de Rees sobre un grupo. Resulta interesante el hecho de que, salvo isomorfismo, este es el único ejemplo que puede darse. Más precisamente, se tiene que todo semigrupo completamente simple debe ser isomorfo a algún semigrupo de la forma $\mathcal{M}(G, A, B, \mathcal{P})$. Este interesante resultado es atribuido al matemático D. Rees. La prueba que en este trabajo se presenta está basada en los resultados anteriores y consiste en hallar un grupo, dos conjuntos adecuados y una función entre estos, de tal suerte que el semigrupo matriz de Rees que se obtiene sea isomorfo al semigrupo dado. Ahora bien, a partir de un semigrupo completamente simple, ¿cómo hallamos un grupo que tenga algo que ver con él?. La respuesta es sencilla: tomaremos un ideal izquierdo minimal, un ideal derecho minimal y después consideraremos su intersección, que por resultados anteriores debe ser un grupo. En seguida, tomaremos al elemento neutro de este grupo y dejaremos fijos a nuestro par de ideales y al elemento neutro que denotaremos por α. Una vez que ya tenemos al grupo que tiene que ver con el semigrupo dado, queda hallar un par de conjuntos y una función que relacione a nuestros ingredientes. De nuevo, este par de conjuntos será obtenido a partir de los ideales que hemos tomado. Resulta que lo mejor para definir a tales conjuntos es la de hacer que cada uno de sus miembros sea un idempotente, pues aprovecharemos el hecho de que todo grupo solo cuenta con un elemento idempotente, a saber, su elemento neutro. Lo que haremos será considerar a los conjuntos de la forma $S\alpha \cap \beta S$ y $\alpha S \cap S\beta$ (que por resultados anteriores deben ser grupos) y haremos correr a β sobre el conjunto de idempotentes $E(S)$. Después, seleccionaremos a cada uno de los elementos neutros de estos grupos y a partir de ellos es que definiremos a los conjuntos requeridos. Finalmente, definiremos una función adecuada que relacione a lo anterior y construiremos un isomorfismo entre nuestro semigrupo completamente simple y el semigrupo matriz de Rees obtenido con todos estos ingredientes.

Teorema. 8.4.1. *Teorema de Rees.*

Todo semigrupo completamente simple es isomorfo a algún semigrupo matriz de Rees sobre un grupo.

Demostración. Suponga que S es un semigrupo completamente simple y sean I un ideal izquierdo minimal y J un ideal derecho minimal. De acuerdo a la Proposición 8.2.15 debe suceder que $I \cap J = H_\alpha = JI$ con α un idempotente. Además, se tiene que $I = S\alpha$ y $J = \alpha S$. Dejemos fijos a los ideales I y J y también al idempotente α. Ahora bien, para

cada $\beta \in E(S)$ considere a los conjuntos $S\alpha \cap \beta S$ y $\alpha S \cap S\beta$ que según el Corolario 8.2.16 deben ser grupos. Para cada $\beta \in E(S)$ sea u_β el elemento neutro de $S\alpha \cap \beta S$ y sea v_β el elemento neutro de $\alpha S \cap S\beta$. Se definen los siguientes conjuntos:

$$A := \{u_\beta \mid \beta \in E(S)\} \quad \text{y} \quad B := \{v_\beta \mid \beta \in E(S)\}$$

Observe que por definición, cada elemento de A es un idempotente que pertenece al ideal $I = S\alpha$ y cada elemento de B es un idempotente que pertenece al ideal $J = \alpha S$. Debido a esto y a que $H_\alpha = JI$ es que tiene sentido considerar a la función $\mathcal{P} : B \times A \longrightarrow H_\alpha$ definida por $\mathcal{P}(v_\beta, u_\delta) := v_\beta u_\delta$. **Afirmación:** $S \cong \mathcal{M}(H_\alpha, A, B, \mathcal{P})$. En efecto, considere a la función $\phi : \mathcal{M}(H_\alpha, A, B, \mathcal{P}) \longrightarrow S$ definida por $\phi(u_\beta, g, v_\delta) := u_\beta g v_\delta$. Veamos que ϕ es inyectiva: si (u_β, g, v_δ) y $(u_{\beta'}, h, v_{\delta'})$ son tales que $\phi(u_\beta, g, v_\delta) = \phi(u_{\beta'}, h, v_{\delta'})$ entonces $u_\beta g v_\delta = u_{\beta'} h v_{\delta'}$. Así, del inciso 2 de la Proposición 8.2.15 se sigue que $u_\beta S = u_{\beta'} S$ y $Sv_\delta = Sv_{\delta'}$. Por otro lado, puesto que u_β es por definición el elemento neutro de $S\alpha \cap \beta S$, se sigue que en particular $u_\beta \in \beta S$ y por consiguiente $u_\beta S = \beta S$. De la misma forma se concluye que $u_{\beta'} S = \beta' S$. Ahora bien, puesto que por definición v_δ es el elemento neutro de $\alpha S \cap S\delta$ se sigue en particular que $v_\delta \in S\delta$ y en consecuencia $Sv_\delta = S\delta$. Del mismo modo se verifica que $Sv_{\delta'} = S\delta'$. De las igualdades anteriores se deduce que $S\alpha \cap \beta S = S\alpha \cap u_\beta S = S\alpha \cap u_{\beta'} S = S\alpha \cap \beta' S$ y también $\alpha S \cap S\delta = \alpha S \cap Sv_\delta = \alpha S \cap Sv_{\delta'} = \alpha S \cap S\delta'$. De ahí que u_β y $u_{\beta'}$ son neutros del grupo $S\alpha \cap \beta S = S\alpha \cap \beta' S$ y v_δ, $v_{\delta'}$ son neutros del grupo $\alpha S \cap S\delta = \alpha S \cap S\delta'$. Por consiguiente $u_\beta = u_{\beta'}$ y $v_\delta = v_{\delta'}$. Así, la igualdad $u_\beta g v_\delta = u_{\beta'} h v_{\delta'}$ toma la forma $u_\beta g v_\delta = u_\beta h v_\delta$. Ahora bien, puesto que $A \subseteq I$ y $B \subseteq J$ aunado a que $JI = H_\alpha$ se tiene entonces que αu_β y $v_\delta \alpha$ pertenecen ambos al grupo H_α. Denotemos por $(\alpha u_\beta)^{-1}$ y $(v_\delta \alpha)^{-1}$ a los inversos de αu_β y $v_\delta \alpha$, respectivamente, en el grupo H_α. Entonces

$$\begin{aligned}
& u_\beta g v_\delta = u_\beta h v_\delta \\
\Longrightarrow \quad & \alpha(u_\beta g v_\delta)\alpha = \alpha(u_\beta h v_\delta)\alpha \\
\Longrightarrow \quad & (\alpha u_\beta) g (v_\delta \alpha) = (\alpha u_\beta) h (v_\delta \alpha) \\
\Longrightarrow \quad & (\alpha u_\beta)^{-1}(\alpha u_\beta) g (v_\delta \alpha)(v_\delta \alpha)^{-1} = (\alpha u_\beta)^{-1}(\alpha u_\beta) h (v_\delta \alpha)(v_\delta \alpha)^{-1} \\
\Longrightarrow \quad & \alpha g \alpha = \alpha h \alpha \\
\Longrightarrow \quad & g = h
\end{aligned}$$

Por consiguiente $(u_\beta, g, v_\delta) = (u_{\beta'}, h, v_{\delta'})$ y así ϕ debe ser inyectiva. Veamos que ϕ es sobreyectiva: como S es también completamente regular (ver Proposición 8.2.15), entonces puede escribirse $S = \bigcup_{\beta \in E(S)} H_\beta$. Asi, para $x \in S$ arbitrario, existe $\beta \in E(S)$ tal que $x \in H_\beta$. De acuerdo a la prueba de la Proposición 8.2.18 la función $f : H_\alpha \longrightarrow H_\beta$ dada por $f(g) := u_\beta g v_\beta$ es una biyección. De ahí que $x = u_\beta g v_\beta$ para algún $g \in H_\alpha$ y por lo tanto $x = \phi(u_\beta, g, v_\beta)$. Se concluye que ϕ debe ser sobreyectiva y por consiguiente una

biyección. Finalmente, veamos que ϕ es un morfismo de semigrupos:

$$\begin{aligned}\phi[(u_\beta, g, v_\delta)(u_{\beta'}, h, v_{\delta'})] &= \phi(u_\beta, g\mathcal{P}(v_\delta, u_{\beta'})h, v_{\delta'}) \\ &= \phi(u_\beta, g(v_\delta u_{\beta'})h, v_{\delta'}) \\ &= u_\beta g(v_\delta u_{\beta'})h v_{\delta'} \\ &= (u_\beta g v_\delta)(u_{\beta'} h v_{\delta'}) \\ &= \phi(u_\beta, g, v_\delta)\phi(u_{\beta'}, h, v_{\delta'})\end{aligned}$$

Así, ϕ es un isomorfismo de semigrupos y por consiguiente $S \cong \mathcal{M}(H_\alpha, A, B, \mathcal{P})$. □

Observe que de acuerdo a las Proposiciones 8.2.6 y 8.2.7 el recíproco de este teorema también se verifica. Recolectamos todos los resultados sobre semigrupos completamene simples como sigue:

Teorema. 8.4.2.

Los siguientes enunciados son equivalentes para un semigrupo S:

1. S es completamente simple.
2. S es simple y contiene al menos un idempotente minimal.
3. S es simple y completamente regular.
4. S es regular y cualquiera de sus idempotentes es minimal.
5. S es isomorfo a algún semigrupo de la forma $\mathcal{M}(G, A, B, \mathcal{P})$ •

.

Capítulo 9

Otras clases importantes de semigrupos

9.1. Semigrupos ortodoxos

No siempre el producto de dos idempotentes es un idempotente. En efecto, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ y $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ son idempotentes de $M_2(\mathbb{R})$ pero $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ no lo es. Si sucede que en un semigrupo regular el producto de cualesquiera dos idempotentes es de nuevo un idempotente, entonces a tal semigrupo se le concede un nombre especial.

Definición 9.1.1.

Decimos que el semigrupo S es un **semigrupo ortodoxo** si

- S es regular.
- $E(S)$ es un subsemigrupo de S •

Ejemplo 9.1.2.

Toda banda rectangular es un semigrupo ortodoxo, pues en esta clase de semigrupos regulares cualquiera de sus elementos es un idempotente. Adicionalmente, todo grupo es un semigrupo ortodoxo. Un ejemplo de un semigrupo ortodoxo que no es banda rectangular ni grupo es el monoide bicíclico (ver Definición 10.0.2 y Proposición 10.0.4) •

Proposición 9.1.3.

Los siguientes enunciados son equivalentes para un semigrupo regular S:

1. S es ortodoxo.
2. Para cada $x, y \in S$

$$x' \in V(x) \quad \text{y} \quad y' \in V(y) \Longrightarrow y'x' \in V(xy) \text{ (véase Definición 7.3.1).}$$

3. Para cada $\alpha \in E(S)$, $V(\alpha) \subseteq E(S)$.

Demostración. 1) $\Longrightarrow$ 2) Sean $x, y \in S$ y tómense $x' \in V(x)$ y $y' \in V(y)$. Entonces tienen lugar las siguientes igualdades:

$$xx'x = x \tag{9.1}$$
$$x'xx' = x' \tag{9.2}$$
$$yy'y = y \tag{9.3}$$
$$y'yy' = y' \tag{9.4}$$

De las igualdades (9.1) y (9.3) se sigue que $x'x$ y yy' son idempotentes. Por consiguiente $x'xyy'$ y $yy'x'x$ deben ser también idempotentes. Ahora bien, observe que

$$\begin{aligned} xy &= (xx'x)(yy'y) \\ &= x(x'xyy')y \\ &= x(x'xyy'x'xyy')y \\ &= (xx'x)yy'x'x(yy'y) \\ &= (xy)(y'x')(xy) \end{aligned}$$

y además

$$\begin{aligned} y'x' &= (y'yy')(x'xx') \\ &= y'(yy'x'x)x' \\ &= y'(yy'x'xyy'x'x)x' \\ &= (y'yy')x'xyy'(x'xx') \\ &= (y'x')(xy)(y'x') \end{aligned}$$

Por consiguiente $y'x' \in V(xy)$.

2) $\Longrightarrow$ 3) Sea $\alpha \in E(S)$ y tómese $x \in V(\alpha)$. Entonces $x = x\alpha x$. Ahora bien, de la hipótesis se sigue que $x^2 \in V(\alpha^2) = V(\alpha)$ y por lo tanto $\alpha x^2 \alpha = \alpha$. Así que $x^2 = (x\alpha x)(x\alpha x) = x\alpha x^2 \alpha x = x\alpha x = x$. De ahí que $x \in E(S)$ y por consiguiente $V(\alpha) \subseteq E(S)$.

3) $\Longrightarrow$ 1) Sean $\alpha, \beta \in E(S)$. Puesto que S es regular de la Proposición 7.3.7 se sigue que existe $g \in E(S)$ tal que $g\alpha = g = \beta g$ y $\alpha g \beta = \alpha\beta$. Así que

$$\begin{aligned} g\alpha\beta g &= (g\alpha)(\beta g) \\ &= gg \\ &= g^2 \\ &= g \end{aligned}$$

y

$$\begin{aligned}\alpha\beta g\alpha\beta &= \alpha(\beta g)\alpha\beta\\ &= \alpha g\alpha\beta\\ &= \alpha(g\alpha)\beta\\ &= \alpha g\beta\\ &= \alpha\beta\end{aligned}$$

Por consiguiente $\alpha\beta \in V(g)$. Ahora bien, por hipótesis debe suceder que $V(g) \subseteq E(S)$. En consecuencia $\alpha\beta \in E(S)$ y así $E(S)$ es subsemigrupo de S. Por consiguiente S es ortodoxo.

□

Hagamos una digresión para revisar los siguientes resultados con respecto al producto directo de dos semigrupos (ver Definición 5.1.1).

Proposición 9.1.4.

Sean S y T semigrupos. Entonces

1. $E(S \times T) = E(S) \times E(T)$.
2. $S \times T$ es regular si S y T lo son.
3. $S \times T$ es ortodoxo si S y T lo son.
4. $S \times T$ es completamente simple si S y T lo son.

Demostración. **1)** Sea $(s,t) \in E(S \times T)$. Entonces $(s,t)(s,t) = (s,t)$, de donde $(s^2, t^2) = (s,t)$ y en consecuencia $s^2 = s$ y $t^2 = t$. De ahí que $(s,t) \in E(S) \times E(T)$ y por lo tanto $E(S\times T) \subseteq E(S)\times E(T)$. Tómese ahora $(s,t) \in E(S)\times E(T)$. Entonces $(s,t)(s,t) = (s^2, t^2) = (s,t)$. De ahí que $(s,t) \in E(S\times T)$ y por consiguiente $E(S)\times E(T) \subseteq E(S\times T)$. En definitiva $E(S \times T) = E(S) \times E(T)$. **2)** Suponga que S y T son semigrupos regulares y sea $(s,t) \in S\times T$ arbitrario. Para s existe $x \in S$ tal que $s = sxs$ y para t existe $y \in T$ tal que $t = tyt$. Así, $(s,t)(x,y)(s,t) = (sx,ty)(s,t) = (sxs,tyt) = (s,t)$. Por consiguiente $S \times T$ es regular. **3)** Suponga que S y T son semigrupos ortodoxos. Entonces S y T deben ser regulares y por consiguiente $S \times T$ es regular. Tómense $(s,t),(x,y) \in E(S \times T)$. Del inciso 1) se sigue que $s,x \in E(S)$ y $t,y \in E(T)$. Así, puesto que S y T son ortodoxos debe suceder que $sx \in E(S)$ y $ty \in E(T)$. Por consiguiente $(s,t)(x,y) = (sx,ty) \in E(S)\times E(T) = E(S\times T)$ y así $S \times T$ es ortodoxo. **4)** Suponga que S y T son semigrupos completamente simples. En particular S y T deben ser regulares y por consiguiente $S \times T$ es también regular. Ahora bien, sean $(s,t),(x,y) \in E(S \times T) = E(S) \times E(T)$ tales que $(s,t) \leq (x,y)$. Entonces $(s,t)(x,y) = (s,t) = (x,y)(s,t)$ y por consiguiente $(sx,ty) = (s,t) = (xs,yt)$. De ahí que $sx = s = xs$ y $ty = t = yt$, o lo que es lo mismo $s \leq x$ y $t \leq y$. De esto último y de que todos los idempotentes de S y T son minimales se deduce que $s = x$ y $t = y$. Así,

$(s,t)=(x,y)$ y por lo tanto todo idempotente de $S\times T$ es minimal. La Proposición 8.2.12 permite concluir que $S\times T$ es completamente simple.

□

A continuación se introduce a otra clase de semigrupos.

Definición 9.1.5.

Se dice que el semigrupo S es un **grupo rectangular** si S es isomorfo a algún semigrupo de la forma $G\times B$ donde G es un grupo y B una banda rectangular •

Observe que como todo grupo y toda banda rectangular son ortodoxos y completamente simples, entonces de la proposición anterior se sigue que todo grupo rectangular es ortodoxo y completamente simple. De hecho veremos adelante que el recíproco también se verifica.

Proposición 9.1.6.

Todo semigrupo ortodoxo y completamente simple debe ser un grupo rectangular.

Demostración. Sea S un semigrupo ortodoxo y completamente simple. Suponga que I es un ideal izquierdo minimal y que J es un ideal derecho minimal. Entonces $I\cap J=H_\alpha=JI$ para algún idempotente α. Considere a la función $\mathcal{P}:B\times A\longrightarrow H_\alpha$ dada por $\mathcal{P}(v_\beta,u_\delta):=v_\beta u_\delta$ siendo A y B definidos como en la prueba del Teorema 8.4.1. Ahora bien, como todos los elementos de A y B son idempotentes, entonces de que S es ortodoxo se sigue que para cada $u_\delta\in A$ y cada $v_\beta\in B$ el elemento $\mathcal{P}(v_\beta,u_\delta):=v_\beta u_\delta$ es un idempotente del grupo H_α. En consecuencia $\mathcal{P}(v_\beta,u_\delta)=\alpha$. Por otra parte, de la prueba del Teorema 8.4.1 se tiene que $S\cong\mathcal{M}(H_\alpha,A,B,\mathcal{P}):=A\times H_\alpha\times B$. Considere a la banda rectangular $A\times B$ con operación binaria dada por $(u_\beta,v_\delta)(u_{\beta'},v_{\delta'}):=(u_\beta,v_{\delta'})$ (véase el primero de los Ejemplos 6.0.2). **Afirmación:** $\mathcal{M}(H_\alpha,A,B,\mathcal{P})\cong H_\alpha\times(A\times B)$. En efecto, sea la función $f:\mathcal{M}(H_\alpha,A,B,\mathcal{P})\longrightarrow H_\alpha\times(A\times B)$ definida por $f(u_\beta,g,v_\delta):=(g,(u_\beta,v_\delta))$. No es difícil ver que f es una función biyectiva. Más aún,

$$\begin{aligned}f(u_\beta,g,v_\delta)f(u_{\beta'},h,v_{\delta'})&=(g,(u_\beta,v_\delta))(h,(u_{\beta'},v_{\delta'}))\\&=(gh,(u_\beta,v_\delta)(u_{\beta'},v_{\delta'}))\\&=(gh,(u_\beta,v_{\delta'}))\end{aligned}$$

mientras que

$$\begin{aligned}f[(u_\beta,g,v_\delta)(u_{\beta'},h,v_{\delta'})]&=f(u_\beta,g\mathcal{P}(v_\delta,u_{\beta'})h,v_{\delta'})\\&=f(u_\beta,g\alpha h,v_{\delta'})\\&=f(u_\beta,gh,v_{\delta'})\\&=(gh,(u_\beta,v_{\delta'}))\end{aligned}$$

Por lo tanto f es un isomorfismo de semigrupos y $\mathcal{M}(H_\alpha,A,B,\mathcal{P})\cong H_\alpha\times(A\times B)$. De esto último se deduce que $S\cong H_\alpha\times(A\times B)$ y el resultado se sigue. □

Así, ortodoxo y completamente simple equivale a grupo rectangular.

9.2. Semigrupos inversos

Recordar que una banda (ver Definición 7.1.3) es un semigrupo en el que cualquiera de sus elementos es idempotente. Ahora bien, suponga que S es una banda conmutativa i,e, una banda en la que cualesquiera dos elementos conmutan. Sobre S se define la siguiente relación:

$$a \leq b \iff ab = a$$

Observe que $\leq$ es reflexiva, pues para cada $a \in S$, $a^2 = a$. Además, si $a \leq b$ y $b \leq a$ entonces $ab = a$ y $ba = b$, lo que combinado con que S es conmutativo resulta en que $a = b$ y por consiguiente $\leq$ es antisimétrica. Por otra parte, si $a \leq b$ y $b \leq c$ entonces $ab = a$ y $bc = b$. De ahí que $ac = (ab)c = a(bc) = ab = a$ y por lo tanto $a \leq c$. Así que $\leq$ es transitiva y por consiguiente una relación de orden parcial. Sean $a, b \in S$. Entonces $ab \leq a$ y $ab \leq b$, pues $(ab)a = (ba)a = ba^2 = ba = ab$ y $(ab)b = ab^2 = ab$. Por consiguiente ab es cota inferior de $\{a, b\}$. Más aún, si c es cualquier cota inferior de $\{a, b\}$ entonces $c \leq a$ y $c \leq b$, de donde $ca = c$ y $cb = c$. Así que $cab = cb = c$ y entonces $c \leq ab$. Puede concluirse que $ab = inf\{a, b\}$ y por consiguiente $(S, \leq)$ es una semiretícula inferior (ver Definición 1.3.12). E inversamente, sea $(X, \leq)$ una semiretícula inferior. Sobre X se define la siguiente operación binaria:

$$ab := a \wedge b$$

Entonces, de la Proposición 1.3.13 se sigue que X junto con tal operación binaria dan lugar a una banda conmutativa. Se puede concluir que toda banda conmutativa induce una semiretícula inferior y que toda semiretícula inferior induce una banda conmutativa. De manera similar y haciendo las modificaciones pertinentes, se exhibe que toda banda conmutativa induce una semiretícula superior y que toda semiretícula superior induce una banda conmutativa. Es debido a esto que se usará la palabra semiretícula como sinónimo de banda conmutativa. Una vez realizada esta discusión se introduce a los llamados semigrupos inversos.

Definición 9.2.1.

Se dice que el semigrupo S es un **semigrupo inverso** si para cada $a \in S$ el conjunto $V(a)$ (véase Definición 7.3.1) tiene exactamente un elemento •

Puesto que todo inverso (en el sentido de la Definición 7.3.1) es en particular un pseudo-inverso, se tiene entonces que por definición, todo semigrupo inverso debe ser también un semigrupo regular.

Ejemplo 9.2.2.

Todo grupo es un semigrupo inverso. En efecto, sea G un grupo. Puesto que G es en particular un monoide, entonces de acuerdo a la Observación 7.3.2, inverso en el sentido de la Definición 3.2.9 implica inverso en el sentido de la Definición 7.3.1. Y viceversa, sea $y \in G$ un inverso de $x \in G$ en el sentido de la Definición 7.3.1. Entonces $xyx = x$. Ahora bien, sea x^{-1} el inverso de x en el sentido de la Definición 3.2.9. Se tiene que

$$\begin{aligned} & xyx = x \\ \Longrightarrow \quad & x^{-1}xyxx^{-1} = x^{-1}xx^{-1} \\ \Longrightarrow \quad & eye = ex^{-1} \\ \Longrightarrow \quad & y = x^{-1} \end{aligned}$$

Por consiguiente, inverso en el sentido de la Definición 7.3.1 implica inverso en el sentido de la Definición 3.2.9. Se concluye que en todo grupo, inverso en el sentido de la Definición 3.2.9 equivale a inverso en el sentido de la Definición 7.3.1. De esto último, y de que todo elemento de un grupo tiene un único inverso en el sentido de la Definición 3.2.9 se deduce que todo grupo es un semigrupo inverso •

A continuación, se establecen algunas formas equivalentes de definir a un semigrupo inverso.

Proposición 9.2.3.

Los siguientes enunciados son equivalentes para un semigrupo S:

1. S es regular y $E(S)$ es una semiretícula (subsemigrupo conmutativo de S).
2. Para cada $x \in S$ existen únicos $\alpha, \beta \in E(S)$ tales que $x\mathcal{L}\alpha$ y $x\mathcal{R}\beta$.
3. S es un semigrupo inverso.

Demostración. 1) $\Longrightarrow$ 2) Sea $x \in S$. Como S es regular, entonces de la Proposición 7.3.9 se sigue que existen $\alpha, \beta \in E(S)$ tales que $x\mathcal{L}\alpha$ y $x\mathcal{R}\beta$. Suponga ahora que α' es otro idempotente para el cual $x\mathcal{L}\alpha'$. Entonces $\alpha\mathcal{L}\alpha'$, de manera que $S\alpha = S\alpha'$ y por lo tanto $\alpha = s\alpha'$ y $\alpha' = t\alpha$ para algunos $s, t \in S$. De estas igualdades se sigue que $\alpha\alpha' = \alpha$ y $\alpha'\alpha = \alpha'$. Ahora bien, como $E(S)$ es una semiretícula, entonces cualesquiera dos idempotentes conmutan. En particular $\alpha\alpha' = \alpha'\alpha$ y por consiguiente $\alpha = \alpha'$. Así, α es el único idempotente para el cual $x\mathcal{L}\alpha$. De manera análoga se exhibe que β es el único idempotente tal que $x\mathcal{R}\beta$.

2) $\Longrightarrow$ 3) Sea $a \in S$ arbitrario y tómense $x, y \in V(a)$. Entonces tienen lugar las siguientes igualdades:

$$axa = a \tag{9.5}$$
$$xax = x \tag{9.6}$$
$$aya = a \tag{9.7}$$
$$yay = y \tag{9.8}$$

De estas igualdades junto con la Proposición 7.2.7 se deduce que xa, ax, ya, y ay son idempotentes tales que $a\mathcal{L}xa$, $a\mathcal{L}ya$, $a\mathcal{R}ax$ y $a\mathcal{R}ay$. Por consiguiente, de la hipótesis se sigue que $xa = ya$ y $ax = ay$. De esto se desprende que $x = xax = yax$ y $y = yay = yax$. Por consiguiente $x = y$ y así $a \in S$ tiene un único inverso. Se concluye que S es un semigrupo inverso.

3) $\Longrightarrow$ 1) Si S es un semigrupo inverso entonces, en particular, también debe ser regular. **Afirmación:** Para cada $\gamma \in E(S)$ se tiene que $V(\gamma) = \{\gamma\}$. En efecto si $\gamma \in E(S)$, entonces $\gamma\gamma\gamma = \gamma$ y por lo tanto $\gamma \in V(\gamma)$. Así, de que S es inverso se deduce que $V(\gamma) = \{\gamma\}$. De esto último y de la Proposición 9.1.3 se sigue que S debe ser ortodoxo i,e, $E(S)$ es un subsemigrupo de S. Para exhibir que $E(S)$ es una semiretícula solo resta entonces mostrar que cualesquiera dos idempotentes de S conmutan: si α y β son idempotentes, entonces $\alpha\beta$ y $\beta\alpha$ también son idempotentes. Más aún, $(\alpha\beta)(\beta\alpha)(\alpha\beta) = \alpha\beta^2\alpha^2\beta = \alpha\beta\alpha\beta = \alpha\beta$ y a la vez $(\beta\alpha)(\alpha\beta)(\beta\alpha) = \beta\alpha^2\beta^2\alpha = \beta\alpha\beta\alpha = \beta\alpha$. De ahí que $\beta\alpha \in V(\alpha\beta) = \{\alpha\beta\}$ y por consiguiente $\alpha\beta = \beta\alpha$. □

Observe que de esta proposición se sigue que todo semigrupo inverso debe ser ortodoxo. Por otra parte, anteriormente se vio que grupo rectangular equivale a semigrupo completamente simple y ortodoxo. Ahora bien, ¿qué se obtendrá de un semigrupo completamente simple e inverso?.

Proposición 9.2.4.

El semigrupo S es un grupo si y sólo si S es completamente simple e inverso.

Demostración. $\Longleftarrow$) Suponga que S es un semigrupo completamente simple e inverso y sea $\alpha \in E(S)$ arbitrario. **Afirmación:** $E(S) = \{\alpha\}$. En efecto, sea $\beta \in E(S)$. Debido a que S es inverso, entonces $E(S)$ es una semiretícula. De ahí que $\alpha\beta = \beta\alpha \in E(S)$. Ahora bien como S es completamente simple, entonces $H_\alpha = S\alpha \cap \alpha S$. Observe que $\alpha\beta = \beta\alpha \in S\alpha \cap \alpha S = H_\alpha$. Luego, $\alpha\beta = \beta\alpha$ es un idempotente del grupo H_α y por consiguiente $\alpha\beta = \alpha = \beta\alpha$, o lo que es lo mismo, $\alpha \leq \beta$. Como todo idempotente de S es minimal (pues S es completamente simple) se concluye que $\alpha = \beta$ y por consiguiente $E(S) = \{\alpha\}$. Finalmente, de que todo semigrupo completamente simple es también completamente regular se sigue que $S = \bigcup_{\beta \in E(S)} H_\beta = \bigcup_{\beta \in \{\alpha\}} H_\beta = H_\alpha$ y por consiguiente S es un grupo.

$\Longrightarrow$) Se sigue de los Ejemplos 8.2.2 y 9.2.2 □

9.3. Semiretículas de subsemigrupos

En el estudio de otras estructuras algebraicas tales como los grupos, se encuentran resultados como el Teorema fundamental de los grupos abelianos finitos que afirma que todo grupo abeliano finito es isomorfo al producto directo de grupos cíclicos, los cuales son de cierta forma, grupos más conocidos. También, dentro del álgebra lineal existe la noción de suma directa de subespacios, y de igual forma, existen teoremas que afirman que bajo

ciertas condiciones, un espacio vectorial es suma directa de ciertos subespacios de éste. En general, este proceso de descomponer una estructura en otras más conocidas también prevalece dentro de la teoría de semigrupos.

Definición 9.3.1.

Sea S un semigrupo y sea $\mathcal{F} = \{S_i \mid i \in I\}$ una familia de subconjuntos de S indexada por el conjunto I. Se dice que S es **semiretícula de sus subsemigrupos** S_i si se verifica lo siguiente:

1. $\mathcal{F}$ es una partición de S (véase Definición 1.2.6).
2. I es una semiretícula (banda conmutativa) (véase Definición 7.1.3).
3. Para cada $i, j \in I$ se tiene que $S_i S_j \subseteq S_{ij}$ donde ij denota la operación en I.

Si en adición, cada miembro de $\mathcal{F}$ verifica una cierta propiedad $\mathcal{T}$, entonces se dice que S es **semiretícula de subsemigrupos del tipo** $\mathcal{T}$ •

Observación 9.3.2.

Suponga que S es un semigrupo y que $\mathcal{F} = \{S_i \mid i \in I\}$ es una familia de subconjuntos de S que verifica todas las condiciones de la definición anterior. Entonces S es, por definición, semiretícula de sus subsemigrupos S_i. Sin embargo, y a pesar del nombre, la Definición 9.3.1 no exige que los S_i sean subsemigrupos de S. No obstante, puede probarse que de hecho lo son. En efecto, observe primero que cada miembro de $\mathcal{F}$ debe ser no vacío, pues $\mathcal{F}$ es partición de S. Así si $x, y \in S_i$, entonces $xy \in S_i S_i \subseteq S_{i^2} = S_i$. De ahí que $xy \in S_i$ y por consiguiente cada S_i es un subsemigrupo de S •

Antes de continuar, es preciso hacer algunas observaciones a la prueba de la Proposición 8.2.11, la cual afirma que todo semigrupo simple y completamente regular debe ser completamente simple. La demostración consiste en mostrar que bajo estas dos hipòtesis, cualesquiera dos idempotentes α y β tales que $\alpha\beta = \alpha = \beta\alpha$ deben ser iguales. Para llevar a cabo esta tarea, es fundamental poder establecer desde el inicio la identidad $\beta = u\alpha v$ donde $u, v \in S$ son tales que $u\alpha = u$ y $\alpha v = v$. Esto es posible a partir de suponer que S es un semigrupo simple, y de hecho, esta es la única vez que se hace uso de tal hipótesis. Todo lo siguiente y que se desprende de la identidad $\beta = u\alpha v$ únicamente hace uso de suponer que S es completamente regular. Así, si se remueve la hipótesis de ser un semigrupo simple y en su lugar se da por hecho que puede escribirse $\beta = u\alpha v$ con $u = u\alpha$ y $v = \alpha v$ entonces de igual forma podrá implicarse que $\alpha = \beta$. Todo lo anterior permite establecer el siguiente resultado.

Proposición 9.3.3.

Sea S un semigrupo completamente regular y suponga que α y β son idempotentes de S tales que $\alpha\beta = \alpha = \beta\alpha$. Si $\beta = u\alpha v$ para algunos $u, v \in S$ con $u\alpha = u$ y $v = \alpha v$, entonces $\alpha = \beta$.

Demostración. A partir de la identidad $\beta = u\alpha v$ úsese la misma técnica que aparece en la prueba de la Proposición 8.2.11. □

A continuación se muestra un primer resultado con respecto a las semiretículas de subsemigrupos.

Proposición 9.3.4.

Todo semigrupo completamente regular es semiretícula de semigrupos completamente simples.

Demostración. Sea S un semigrupo completamente regular. Es preciso hallar una familia $\mathcal{F}$ de subconjuntos de S que cumpla todas las condiciones que exige la Definición 9.3.1. En particular, tal familia deberá estar indexada por una banda conmutativa. Ahora bien, ¿cómo obtenemos una banda conmutativa que tenga alguna relación con S?. Pues bien, de acuerdo con la Proposición 7.3.16 la relación $\mathcal{J}$ es una congruencia sobre S y además el semigrupo cociente $\frac{S}{\mathcal{J}}$ es una banda conmutativa. Más aún, como $\mathcal{J}$ es relación de equivalencia entonces $\frac{S}{\mathcal{J}}$ es una partición de S (ver Proposición 1.2.7). Hágase $I := \frac{S}{\mathcal{J}}$ y para cada $J_a \in I$ defínase $S_{J_a} := J_a$. Considere a la familia $\mathcal{F} := \{S_{J_a} \mid J_a \in I\}$. Es claro que $\mathcal{F} = \frac{S}{\mathcal{J}}$. Luego $\mathcal{F}$ es una partición de S. Por otra parte, sean $J_a, J_b \in I$ y tómense $x \in S_{J_a}$ y $y \in S_{J_b}$. Entonces $x \in J_a$ y $y \in J_b$ de manera que $x\mathcal{J}a$ y $y\mathcal{J}b$. Así, como $\mathcal{J}$ es una congruencia se sigue entonces que $xy\mathcal{J}ab$ y en consecuencia $xy \in J_{ab}$, o lo que es lo mismo $xy \in S_{J_{ab}}$. De ahí que $S_{J_a}S_{J_b} \subseteq S_{J_{ab}}$. Ahora bien, recuerde que la operación en $I := \frac{S}{\mathcal{J}}$, que denotaremos por $\cdot$, es el producto entre clases de equivalencia, así que $J_a \cdot J_b = J_{ab}$. Por lo tanto $S_{J_{ab}} = S_{J_a \cdot J_b}$. Se puede concluir de todo esto que $S_{J_a}S_{J_b} \subseteq S_{J_a \cdot J_b}$ y por consiguiente $\mathcal{F}$ cumple todos los requisitos que aparecen en la Definición 9.3.1. Para establecer el resultado exhibiremos que todos los miembros de $\mathcal{F}$ son subsemigrupos completamente simples: de acuerdo a la Observación 9.3.2 cada miembro de $\mathcal{F}$ es un subsemigrupo de S, más aún, sea $x \in S_{J_a} := J_a$. Como S es regular, entonces $V(x) \neq \emptyset$. Así, si $y \in V(x)$ debe ocurrir que $x = xyx$ y $y = yxy$. Ahora bien, puesto que $\mathcal{F}$ es partición de S existe $J_b \in I$ tal que $y \in J_b$. De ahí que $x = xyx \in J_aJ_bJ_a \subseteq J_{aba} = J_{a^2b} = J_{ab}$ y por consiguiente $x \in J_{ab}$. Así que $x \in J_a \cap J_{ab}$ y por lo tanto $J_a = J_{ab}$. En cuanto a la identidad $y = yxy$, de esta se sigue que $y \in J_bJ_aJ_b \subseteq J_{bab} = J_{b^2a} = J_{ba} = J_{ab} = J_a$. Por consiguiente $y \in S_{J_a} := J_a$. Observe que entonces y es un pseudoinverso de x que pertenece a J_a. Por consiguiente $S_{J_a} := J_a$ es un semigrupo regular. Ahora bien, sean α y β idempotentes de $S_{J_a} := J_a$ (que en particular son idempotentes de S) tales que $\alpha \leq \beta$. Entonces $\alpha\beta = \alpha = \beta\alpha$. Puesto que $\alpha, \beta \in J_a$ se sigue que $\alpha\mathcal{J}\beta$ y por lo tanto $S\alpha S = S\beta S$. De esto se deduce que $\beta = x\alpha y$ para algunos $x, y \in S$. Ahora bien, como α es idempotente, entonces $\beta = x\alpha y = (x\alpha)\alpha(\alpha y) = u\alpha v$ donde $u := x\alpha$ y $v := \alpha y$. No es difícil ver que $u = u\alpha$ y $v = \alpha v$. Finalmente, debido a que S es completamente regular la Proposición 9.3.3 permite concluir que $\alpha = \beta$. Por consiguiente J_a es un semigrupo regular en el que cualquiera de sus idempotentes es minimal. Por lo tanto de la Proposición 8.2.12 se concluye que cada $S_{J_a} := J_a$ es completamente simple. □

Recuerde que todo semigrupo completamente simple es también completamente regular. Sin embargo, aunque el recíproco no se verifica sabemos ahora que todo semigrupo completamente regular se puede descomponer en semigrupos completamente simples. A continuación se establece otro resultado de este tipo, sin embargo, se necesitará hacer uso del siguiente resultado auxiliar.

Proposición 9.3.5.

Los siguientes enunciados son equivalentes para un semigrupo S:

1. S es completamente simple y $E(S) = S$.
2. S es una banda rectangular.

Demostración. 1) $\Longrightarrow$ 2) Sean $a, b \in S = E(S)$ arbitrarios. De que S es completamente simple se sigue que $H_a = Sa \cap aS$. Ahora bien, como el único idempotente del grupo H_a es a, entonces de que $E(S) = S$ se deduce que $H_a = \{a\}$. Así, observe que $aba \in Sa \cap aS = \{a\}$ y por lo tanto $aba = a$. En definitiva S es una banda rectangular.

2) $\Longrightarrow$ 1) Se sigue de la Proposición 6.0.4 y del Corolario 8.2.8. □

Proposición 9.3.6.

Toda banda es semiretícula de bandas rectangulares.

Demostración. Sea B una banda i,e, un semigrupo para el cual $E(B) = B$. Entonces para cada $a \in B$ se verifica que $a = aaa$ y por consiguiente B es completamente regular. Así, de la Proposición 9.3.4 se sigue que existe una familia $\mathcal{F} := \{S_i \mid i \in I\}$ de subsemigrupos completamente simples que verifica todas las condiciones de la Definición 9.3.1. Ahora bien, como todo elemento de B es idempotente, entonces en particular, cada elemento de cada subsemigrupo S_i también es idempotente. Por lo tanto para cada $i \in I$ se tiene que $E(S_i) = S_i$. De acuerdo con esto, la Proposición 9.3.5 permite deducir que cada S_i es una banda rectangular y la prueba queda terminada. □

9.4. Semigrupos de Clifford

Para finalizar nuestro estudio de los semigrupos regulares se introduce a los llamados semigrupos de Clifford.

Definición 9.4.1.

Decimos que el semigrupo S es un **semigrupo de Clifford** si:

1. S es regular.
2. $E(S) \subseteq Z(S)$ •

Así, un semigrupo de Clifford es un semigrupo regular en el que cada idempotente es central (véase Definición 6.0.7).

Proposición 9.4.2.

Los siguientes enunciados son equivalentes para un semigrupo S:

1. S es un semigrupo de Clifford.
2. S es completamente regular e inverso.
3. S es semiretícula de grupos.

Demostración. 1) $\Longrightarrow$ 2) Suponga que S es un semigrupo de Clifford y tómense $\alpha, \beta \in E(S)$ arbitrarios. Entonces de que $E(S) \subseteq Z(S)$ se sigue que $\alpha\beta = \beta\alpha$ y en consecuencia $(\alpha\beta)^2 = (\alpha\beta)(\alpha\beta) = \alpha(\beta\alpha)\beta = \alpha(\alpha\beta)\beta = \alpha^2\beta^2 = \alpha\beta$. Por consiguiente $\alpha\beta \in E(S)$. De todo esto se puede concluir que $E(S)$ es un subsemigrupo conmutativo de S, o lo que es lo mismo, $E(S)$ es una semiretícula. Así que de esto último aunado a que S es regular se deduce de la Proposición 9.2.3 que S es inverso. Ahora bien, sea $a \in S$ arbitrario. Puesto que S es regular debe existir $x \in S$ tal que $axa = a$. De esta igualdad se sigue que $ax, xa \in E(S) \subseteq Z(S)$. Como una consecuencia de lo anterior observe que

$$\begin{aligned} xa &= (xa)(xa) \\ &= x(ax)a \\ &= (ax)xa \\ &= ax^2a \end{aligned}$$

mientras que

$$\begin{aligned} ax &= (ax)(ax) \\ &= a(xa)x \\ &= ax(xa) \\ &= ax^2a \end{aligned}$$

Por consiguiente $ax = xa$ y así x es un pseudoinverso conmutativo de a. De ahí que S es completamente regular.

2) $\Longrightarrow$ 3) Suponga que S es un semigrupo completamente regular e inverso. De acuerdo a la Proposición 9.3.4 existe una familia $\mathcal{F} := \{S_i \mid i \in I\}$ de subsemigrupos completamente simples que verifica todas las condiciones de la Definición 9.3.1. **Afirmación:** Cada S_i es un semigrupo inverso. En efecto, para cada $a \in S_i$ sea $V_i(a)$ el conjunto de inversos de a en el semigrupo S_i. Puesto que S_i es completamente simple se sigue que en particular debe ser regular. Así $V_i(a) \neq \emptyset$. Debido a que la operación binaria de $S_i \subseteq S$ es la misma que la de S se sigue entonces que $V_i(a) \subseteq V(a)$ i,e, todo inverso de a en S_i es un inverso de a en S. Ahora bien, como S es, por hipótesis, un semigrupo inverso, entonces $V(a)$ tiene exactamente un elemento. Por consiguiente, de que $\emptyset \neq V_i(a) \subseteq V(a)$ se deduce que $V_i(a) = V(a)$ de manera que $V_i(a)$ tiene exactamente un elemento. De ahí que cada S_i

es un semigrupo inverso. Tenemos entonces que cada S_i es un semigrupo completamente simple e inverso y así de la Proposición 9.2.4 se sigue que cada S_i debe ser un grupo. Por consiguiente S es una semiretícula de grupos.

3) $\Longrightarrow$ 1) Suponga que S es una semiretícula de grupos. Entonces existe una familia $\mathcal{F} = \{S_i \mid i \in I\}$ de subgrupos de S que satisface todas las condiciones de la Definición 9.3.1. Para cada $i \in I$ sea $\alpha_i \in E(S)$ el elemento neutro de S_i. Según la Proposición 8.3.1 debe suceder que $S_i \subseteq H_{\alpha_i}$. Luego, se tiene que $S = \bigcup_{i\in I} S_i \subseteq \bigcup_{i\in I} H_{\alpha_i} \subseteq \bigcup_{\alpha\in E(S)} H_\alpha$ y por lo tanto $S = \bigcup_{\alpha\in E(S)} H_\alpha$. De ahí que S es completamente regular y en particular regular. Así, para cada $a \in S$ sucede que $V(a) \neq \emptyset$. Más aún, $V(a)$ tiene exactamente un elemento. En efecto, sea $a \in S$. Puesto que $S = \bigcup_{i\in I} S_i$ se tiene que $a \in S_i$ para algún $i \in I$. Sea $\alpha_i \in E(S)$ el elemento neutro del grupo S_i. Entonces existe $b \in S_i$ tal que $ab = \alpha_i = ba$. De esto se sigue que $aba = \alpha_i a = a$ y $bab = \alpha_i b = b$. Por consiguiente $b \in V(a)$. Veamos que $V(a) = \{b\}$. Si $x \in V(a)$, entonces $x = xax$ y $a = axa$, además, se tiene que $x \in S_j$ para algún $j \in I$. Así, se tiene que $a = axa \in S_iS_jS_i \subseteq S_{iji} = S_{i^2j} = S_{ij}$. Por consiguiente $a \in S_{ij}$ a la vez que $a \in S_i$. Luego, de que los miembros de $\mathcal{F}$ son disjuntos por pares se concluye que $S_i = S_{ij}$. En cuanto a la identidad $x = xax$, de ella se sigue que $x = xax \in S_jS_iS_j \subseteq S_{jij} = S_{ij^2} = S_{ij} = S_i$. Por consiguiente $x \in S_i$. Ahora bien, observe que

$$\begin{aligned} & a = axa \\ \Longrightarrow \quad & bab = baxab \\ \Longrightarrow \quad & b = \alpha_i x \alpha_i \\ \Longrightarrow \quad & b = x \end{aligned}$$

Por consiguiente $V(a) = \{b\}$. En particular $V(a)$ tiene exactamente un elemento, de manera que S debe ser un semigrupo inverso. Tenemos así que de acuerdo a la Proposición 9.2.3 $E(S)$ debe ser un subsemigrupo conmutativo de S, en especial, el producto de dos idempotentes debe ser un idempotente, además de que cualesquiera dos de ellos conmutan. Estos hechos nos permitirán exhibir que todo idempotente de S es central. En efecto, sean $\alpha \in E(S)$ y $x \in S$ arbitrarios. Se tiene que $x \in S_i$ y $\alpha \in S_j$ para algunos $i, j \in I$. Denotemos por $\alpha_i \in E(S)$ al elemento neutro del grupo S_i y sea $x^{-1} \in S_i$ el inverso de x en el sentido de la Definición 3.2.9. Observe que $\alpha\alpha_i \in S_jS_i \subseteq S_{ji} = S_{ij}$ y $x\alpha x^{-1} \in S_iS_jS_i \subseteq S_{iji} = S_{i^2j} = S_{ij}$ i,e, $\alpha\alpha_i = \alpha_i\alpha$ (pues cualesquiera dos idempotentes conmutan) y $x\alpha x^{-1}$ pertenecen ambos al grupo S_{ij}. **Afirmación:** $x\alpha x^{-1}$ es idempotente. En efecto

$$\begin{aligned}(x\alpha x^{-1})^2 &= (x\alpha x^{-1})(x\alpha x^{-1}) \\ &= x\alpha(x^{-1}x)\alpha x^{-1} \\ &= x\alpha\alpha_i\alpha x^{-1} \\ &= x\alpha_i\alpha\alpha x^{-1} \\ &= (x\alpha_i)\alpha\alpha x^{-1} \\ &= x\alpha^2 x^{-1} \\ &= x\alpha x^{-1}\end{aligned}$$

Por consiguiente $\alpha\alpha_i = \alpha_i\alpha$ y $x\alpha x^{-1}$ son idempotentes que pertenecen al grupo S_{ij}. En consecuencia $x\alpha x^{-1} = \alpha\alpha_i$. De esta identidad se sigue que

$$\begin{aligned}& & (x\alpha x^{-1})x &= (\alpha\alpha_i)x \\ \Longrightarrow & & x\alpha(x^{-1}x) &= \alpha(\alpha_i x) \\ \Longrightarrow & & x\alpha\alpha_i &= \alpha x \\ \Longrightarrow & & x\alpha_i\alpha &= \alpha x \\ \Longrightarrow & & (x\alpha_i)\alpha &= \alpha x \\ \Longrightarrow & & x\alpha &= \alpha x\end{aligned}$$

De esto se sigue que todo idempotente conmuta con cualquier elemento de S i,e, $E(S) \subseteq Z(S)$. Por consiguiente S es un semigrupo de Clifford.

□

.

Capítulo 10

El monoide bicíclico

En lo sucesivo $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. El presente capítulo tiene por objetivo estudiar a aquellos monoides M con neutro e que son generados por dos elementos, digamos u y v, tales que $uv = e$ pero $vu \neq e$. Veamos a continuación que uno de tales monoides existe.

Observación 10.0.1.

Existe un monoide M con neutro e tal que $M = \langle u, v\rangle$ para algunos $u, v \in M$ con $uv = e$ y $vu \neq e$. En efecto, considere al monoide $\mathcal{T}_{\mathbb{N}}$ (ver Ejemplo 3.4.4) y sea $v \in \mathcal{T}_{\mathbb{N}}$ definida por $v(n) := 2n$. No es difícil ver que v es inyectiva pero no sobreyectiva. Por lo tanto existe $u \in \mathcal{T}_{\mathbb{N}}$ tal que $u \circ v = id_{\mathbb{N}}$ y $v \circ u \neq id_{\mathbb{N}}$. Sea M el submonoide de $\mathcal{T}_{\mathbb{N}}$ definido por $M = \langle u, v\rangle$. Es claro entonces que M cumple las condiciones requeridas •

Sea M un monoide con neutro e tal que $M = \langle u, v\rangle$ para algunos $u, v \in M$ con $uv = e$ y $vu \neq e$. En la siguiente sucesión de afirmaciones se establecen algunas propiedades que debe tener el monoide M.

Afirmación 1: Para cada $n \in \mathbb{N}_0$ se cumple que $u^n v^n = e$. En efecto, se procede por inducción sobre n: para $n = 0$ se tiene que $u^0 v^0 = ee = e$ (ver Definición 3.3.1). Suponga ahora que para $n \geq 1$, $u^n v^n = e$. Entonces $u(u^n v^n)v = uev$, de donde $u^{n+1}v^{n+1} = uv = e$ y por lo tanto la afirmación es válida para $n + 1$, lo que completa la inducción.

Afirmación 2: Para cada $m, n \in \mathbb{N}_0$

$$u^n v^m = \begin{cases} u^{n-m} & si \quad n > m. \\ v^{m-n} & si \quad n \leq m. \end{cases}$$

En efecto si $n > m$, entonces puede escribirse $n = m + r$ para algún $r \geq 1$. Así que $u^n v^m = u^{m+r} v^m = u^r (u^m v^m) = u^r e = u^r = u^{n-m}$. En caso de que $n \leq m$, puede escribirse $m = n + s$ para algún $s \geq 0$. Luego, $u^n v^m = u^n v^{n+s} = (u^n v^n)v^s = ev^s = v^s = v^{m-n}$.

Afirmación 3: $M = \{v^m u^n \mid m, n \in \mathbb{N}_0\}$. En efecto, considere al conjunto $A := \{v^m u^n \mid m, n \in \mathbb{N}_0\}$ y $X := \{u, v\}$. Probaremos por inducción que para cada $n \in \mathbb{N}$:

$$\text{Si } x_1, x_2, \ldots, x_n \in X, \text{ entonces } x_1x_2\cdots x_n \in A.$$

El caso $n = 1$ se verifica de inmediato. Suponga ahora que la proposición es válida para $n \geq 1$ y sean $x_1, x_2, \ldots, x_n, x_{n+1} \in X$. De la hipótesis se tiene que $x_1x_2\cdots x_n \in A$, luego puede escribirse $x_1x_2\cdots x_n = v^s u^t$ para algunos $s, t \in \mathbb{N}_0$. Si ocurre que $x_{n+1} = u$, entonces

$$x_1x_2\cdots x_nx_{n+1} = v^s u^t u = v^s u^{t+1} \in A$$

Si $x_{n+1} = v$ se tiene que

$$x_1x_2\cdots x_nx_{n+1} = v^s u^t v$$

Observe que si $t = 0$, entonces $v^s u^t v = v^s e v = v^s v = v^{s+1} \in A$ y si $t \geq 1$, entonces $v^s u^t v = v^s(u^t v) = v^s u^{t-1} \in A$. En cualquier caso se concluye que

$$x_1x_2\cdots x_nx_{n+1} \in A$$

Así la proposición es válida para $n + 1$ y la inducción queda completa. Por otra parte, es claro que $A \subseteq M$, y además, por hipótesis

$$M = \langle u, v\rangle = \{x_1x_2\cdots x_n \mid n \in \mathbb{N} \quad \text{y} \quad x_i \in \{u, v\}\}$$

Por consiguiente, de lo anteriormente probado se sigue que $M = A$.

Afirmación 4: $v^m = e \iff m = 0$. En efecto, suponga que $v^m = e$ y que $m \geq 1$. Entonces $u^m = u^m e = u^m v^m = e$, de donde $v^m u^m = ee = e$. Esto último se puede reescribir como $v^{m-1}(vu)u^{m-1} = e$, de manera que multiplicando a la izquierda por u^{m-1} y a la derecha por v^{m-1} en la identidad anterior se obtiene que $u^{m-1}v^{m-1}(vu)u^{m-1}v^{m-1} = u^{m-1}v^{m-1}$ y por consiguiente $vu = e$, lo cual es una contradicción. Se concluye así que $m = 0$. La implicación restante se verifica de inmediato.

Afirmación 5: $u^n = e \iff n = 0$. En efecto, suponga que $u^n = e$, entonces $v^n = ev^n = u^n v^n = e$ y por consiguiente $n = 0$. La implicación restante se verifica de inmediato.

Afirmación 6: $u^n v^m = e \iff n = m$. En efecto si $n > m$, entonces $u^{n-m} = u^n v^m = e$ y por lo tanto $n - m = 0$, de donde $n = m$, lo cual es una contradicción. Por consiguiente debe ser que $n \leq m$. Así, $v^{m-n} = u^n v^m = e$ y por tanto $m - n = 0$. De ahí que $m = n$. La implicación restante es evidente.

Afirmación 7: $v^k u^k = e \iff k = 0$. En efecto, suponga que $v^k u^k = e$ y que $k \geq 1$. Entonces $v^{k-1}(vu)u^{k-1} = e$, de manera que multiplicando a la izquierda por u^{k-1} y a la derecha por v^{k-1} en la identidad anterior se obtiene que $u^{k-1}v^{k-1}(vu)u^{k-1}v^{k-1} = u^{k-1}v^{k-1}$ y por consiguiente $vu = e$, lo cual es una contradicción. Se concluye así que $k = 0$. La implicación restante se verifica de inmediato.

Afirmación 8: $u^n = u^s \iff n = s$. En efecto si $u^n = u^s$, entonces $u^n v^s = u^s v^s = e$ y en consecuencia $n = s$. La implicación restante es evidente.

Afirmación 9: $v^m = v^r \iff m = r$. En efecto si $v^m = v^r$, entonces $u^r v^m = u^r v^r = e$ y por consiguiente $m = r$. La implicación restante es evidente.

Afirmación 10: $v^m u^n = v^{m+k} u^s \implies k = 0 \quad \text{y} \quad n = s$. En efecto, la identidad $v^m u^n = v^{m+k} u^s$ puede reescribirse como $v^m u^n = v^m v^k u^s$ de donde se obtiene que $u^m v^m u^n = u^m v^m v^k u^s$ y por consiguiente $u^n = v^k u^s$. Ahora bien, multiplicando a la derecha por v^s a ambos miembros de esta identidad se obtiene que $u^n v^s = v^k$, de donde $u^{n+k} v^s = u^k v^k = e$ y por consiguiente $n + k = s$. La igualdad $v^m u^n = v^{m+k} u^s$ toma entonces la forma $v^m u^n = v^{m+k} u^{n+k}$ o lo que es lo mismo $v^m u^n = v^m v^k u^k u^n$. Multiplicando esta identidad a la izquierda por u^m y a la derecha por v^n se obtiene que $(u^m v^m)(u^n v^n) = (u^m v^m) v^k u^k (u^n v^n)$ y en consecuencia $v^k u^k = e$, de manera que $k = 0$. Finalmente, de que $n + k = s$ se deduce que $n = s$.

Afirmación 11: $v^m u^n = v^r u^s \implies m = r \quad \text{y} \quad n = s$. En efecto, suponga sin perder generalidad que $m \leq r$. Entonces $r = m + k$ para algún $k \geq 0$. La identidad $v^m u^n = v^r u^s$ toma entonces la forma $v^m u^n = v^{m+k} u^s$ de donde se sigue que $k = 0$ y $n = s$. Finalmente, de la igualdad $r = m + k$ se deduce que $m = r$.

Afirmación 12: $(v^m u^n)(v^p u^q) = v^{m-n+\text{máx}(n,p)} u^{q-p+\text{máx}(n,p)}$. En efecto, puesto que

$$u^n v^p = \begin{cases} u^{n-p} & si \quad n > p. \\ v^{p-n} & si \quad n \leq p. \end{cases}$$

entonces

$$(v^m u^n)(v^p u^q) = \begin{cases} v^m u^{q-p+n} & si \quad n > p. \\ v^{m-n+p} u^q & si \quad n \leq p. \end{cases}$$

o lo que es lo mismo

$$(v^m u^n)(v^p u^q) = \begin{cases} v^{m-n+n} u^{q-p+n} & si \quad n > p. \\ v^{m-n+p} u^{q-p+p} & si \quad n \leq p. \end{cases}$$

y por consiguiente

$$(v^m u^n)(v^p u^q) = v^{m-n+\text{máx}(n,p)} u^{q-p+\text{máx}(n,p)}$$

Una vez establecido todo esto, de las afirmaciones 3 y 11 se deduce que para cada $x \in M$ existen únicos $m, n \in \mathbb{N}_0$ tales que $x = v^m u^n$. Ahora bien, esto último asegura que la relación $f : M \longrightarrow \mathbb{N}_0 \times \mathbb{N}_0$ definida por $f(x) := (m, n)$ donde $m, n \in \mathbb{N}_0$ son los únicos enteros no negativos tales que $x = v^m u^n$ es una función. Más aún, si $g : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow M$ es definida por $g(m, n) := v^m u^n$ entonces $g(f(v^m u^n)) = g(m, n) = v^m u^n$ y $f(g(m, n)) = f(v^m u^n) = (m, n)$ y por consiguiente $g \circ f = id_M$ y $f \circ g = id_{\mathbb{N}_0 \times \mathbb{N}_0}$. Se sigue así que f es una función biyectiva con inversa g. Denotemos por $\mathbb{B}$ al conjunto $\mathbb{N}_0 \times \mathbb{N}_0$. De acuerdo con el Ejemplo 3.7.18 a partir del monoide M y de las funciones f y g puede definirse sobre

el conjunto $\mathbb{B}$ una operación binaria asociativa de manera que $\mathbb{B}$ sea un monoide con tal operación, a saber:

$$\begin{aligned}(m,n)(p,q) :&= f[g(m,n)g(p,q)]\\ &= f[(v^m u^n)(v^p u^q)]\\ &= f(v^{m-n+\max(n,p)}u^{q-p+\max(n,p)})\\ &= (m-n+\max(n,p), q-p+\max(n,p))\end{aligned}$$

Y más aún, el Ejemplo 3.7.18 afirma que f debe ser un isomorfismo de semigrupos. A $\mathbb{B}$ junto con la operación anterior se le concede un nombre especial.

Definición 10.0.2.

A $\mathbb{B} := \mathbb{N}_0 \times \mathbb{N}_0$ con la operación binaria asociativa dada por

$$(m,n)(p,q) := (m-n+\max(n,p), q-p+\max(n,p))$$

se le llama **monoide bicíclico** •

Con esta nueva definición podemos resumir toda la discusión previa como sigue:

Proposición 10.0.3.

Todo monoide M con neutro e generado por dos elementos u y v tales que $uv = e$ pero $vu \neq e$ es isomorfo al monoide bicíclico.

Demostración. Se sigue de la discusión anterior. □

A continuación se exhiben algunas propiedades del monoide $\mathbb{B}$.

Proposición 10.0.4.

1. $E(\mathbb{B}) = \{(n,n) \mid n \in \mathbb{N}_0\}$ (ver Definición 7.1.1).
2. $\mathbb{B}$ es un semigrupo regular (ver Definición 7.3.4).
3. $\mathbb{B}$ es un semigrupo inverso (ver Definición 9.2.1).

Demostración. **1)** Sea $n \in \mathbb{N}_0$. Entonces

$$\begin{aligned}(n,n)^2 &= (n,n)(n,n)\\ &= (n-n+\max(n,n), n-n+\max(n,n))\\ &= (n-n+n, n-n+n)\\ &= (n,n)\end{aligned}$$

Por consiguiente toda pareja de la forma (n, n) es un idempotente de $\mathbb{B}$. Y viceversa, si $(m, n) \in E(\mathbb{B})$ entonces

$$\begin{aligned}(m, n) &= (m, n)^2 \\ &= (m, n)(m, n) \\ &= (m - n + \text{máx}(n, m), n - m + \text{máx}(n, m)) \\ &= (m - n + \text{máx}(n, m), n - m + \text{máx}(n, m))\end{aligned}$$

De manera que $m = m - n + \text{máx}(n, m)$ y $n = n - m + \text{máx}(n, m)$, o lo que es lo mismo $n = \text{máx}(n, m)$ y $m = \text{máx}(n, m)$. Por consiguiente $m = n$ y en definitiva $E(\mathbb{B}) = \{(n, n) \mid n \in \mathbb{N}_0\}$.

2) Sea $(m, n) \in \mathbb{B}$ arbitrario. Observe que

$$\begin{aligned}(m, n)(n, m)(m, n) &= (m - n + \text{máx}(n, n), m - n + \text{máx}(n, n))(m, n) \\ &= (m, m)(m, n) \\ &= (m - m + \text{máx}(m, m), n - m + \text{máx}(m, m)) \\ &= (m, n)\end{aligned}$$

Por consiguiente (n, m) es pseudoinverso de (m, n) y así $\mathbb{B}$ es regular.

3) Para cualesquiera dos idempotentes de $\mathbb{B}$ se tiene que

$$\begin{aligned}(m, m)(n, n) &= (m - m + \text{máx}(n, m), n - n + \text{máx}(n, m)) \\ &= (\text{máx}(n, m), \text{máx}(n, m))\end{aligned}$$

y también

$$\begin{aligned}(n, n)(m, m) &= (n - n + \text{máx}(n, m), m - m + \text{máx}(n, m)) \\ &= (\text{máx}(n, m), \text{máx}(n, m))\end{aligned}$$

De esto se sigue que el producto de dos idempotentes es de nuevo un idempotente, además de que cualesquiera dos de ellos conmutan. Por consiguiente $E(\mathbb{B})$ es un subsemigrupo conmutativo de $\mathbb{B}$. Esto último aunado a que $\mathbb{B}$ es regular permite concluir de acuerdo a la Proposición 9.2.3 que $\mathbb{B}$ es un semigrupo inverso.

□

Ahora que sabemos quienes son los idempotentes de $\mathbb{B}$ podemos establecer un criterio para saber cuando uno es menor o igual que otro (véase Proposición 7.1.4).

Proposición 10.0.5.

$$(m, m) \leq (n, n) \iff n \leq m$$

Demostración. $\Longrightarrow$) Si $(m, m) \leq (n, n)$ entonces

$$(m, m) = (m, m)(n, n) = (\text{máx}(n, m), \text{máx}(n, m))$$

y por lo tanto $m = \text{máx}(n, m)$. De ahí que $n \leq m$.

$\Longleftarrow$) Si $n \leq m$, entonces

$$\begin{aligned}(m, m)(n, n) &= (\text{máx}(n, m), \text{máx}(n, m)) \\ &= (m, m)\end{aligned}$$

y por consiguiente $(m, m) \leq (n, n)$.

□

Corolario 10.0.6.

$\mathbb{B}$ no contiene idempotentes minimales.

Demostración. Sea $(n, n) \in E(\mathbb{B})$ arbitrario y tómese $m > n$. Entonces debe suceder que $(m, m) \leq (n, n)$ y $(n, n) \neq (m, m)$. Por consiguiente ningún idempotente de $\mathbb{B}$ es minimal.

□

En cuanto a los ideales de $\mathbb{B}$ se tiene lo siguiente (véase 7.2.4).

Proposición 10.0.7.

1. $\mathbb{B}$ es un semigrupo simple (ver Definición 8.2.1).
2. $\mathbb{B}$ es de ideales principales izquierdos (ver Definición 7.2.5).
3. $\mathbb{B}$ es de ideales principales derechos (ver Definición 7.2.5).

Demostración. **1)** Sea I un ideal bilátero de $\mathbb{B}$ y sean $(m, n) \in \mathbb{B}$ y $(x, y) \in I$ arbitrarios. Entonces $(x, y)(y, x) \in I$, o lo que es lo mismo $(x, x) \in I$. De ahí que $(m, x) = (m, x)(x, x) \in I$ y $(x, n) = (x, x)(x, n) \in I$ y por lo tanto $(m, n) = (m, x)(x, n) \in I$. Se deduce de esto que $\mathbb{B} = I$ y por consiguiente $\mathbb{B}$ es simple.

2) Sea I un ideal izquierdo de $\mathbb{B}$ y sea $(m, n) \in I$. Entonces se tiene que $(n, n) = (n, m)(m, n) \in I$. Por consiguiente

$$A := \{n \in \mathbb{N}_0 \mid (n, n) \in I\} \neq \emptyset$$

Sea $p := \min A$ y definamos $\bar{p} := (p, p)$. Es claro que $\mathbb{B}\bar{p} \subseteq I$. Ahora bien, si $(x, y) \in I$ es arbitrario, entonces $(y, y) = (y, x)(x, y) \in I$ y por consiguiente $y \in A$. En consecuencia $p \leq y$. Así, de la Proposición 10.0.5 se sigue que $(y, y) \leq (p, p)$ o lo que es lo mismo $(y, y)(p, p) = (y, y)$. De esto se deduce que

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

y en consecuencia $(x, y) \in \mathbb{B}\bar{p}$. Por consiguiente $I \subseteq \mathbb{B}\bar{p}$ y con ello $I = \mathbb{B}\bar{p}$. Así, I es un ideal principal izquierdo. La prueba de **3)** es similar a la anterior y por eso se omite.

□

Más aún, de la demostración anterior se aprecia que todo ideal izquierdo (derecho) de $\mathbb{B}$ es de la forma $\mathbb{B}\bar{n}$ ($\bar{n}\mathbb{B}$) donde $\bar{n} := (n, n)$ i,e, todo ideal izquierdo y todo ideal derecho es generado por un idempotente. Para cada $n \in \mathbb{N}_0$ sea $I_n := \mathbb{B}\bar{n}$ y $J_n := \bar{n}\mathbb{B}$ donde $\bar{n} := (n, n)$. Entonces la familia

$$\mathcal{F} := \{I_n \mid n \in \mathbb{N}_0\}$$

contiene a todos los ideales izquierdos de $\mathbb{B}$ y la familia

$$\mathcal{G} := \{J_n \mid n \in \mathbb{N}_0\}$$

contiene a todos los ideales derechos de $\mathbb{B}$. Hagamos ahora una ligera digresión para revisar el siguiente resultado.

Proposición 10.0.8.

Sea S un semigrupo y sean $\alpha, \beta \in E(S)$. Si $\alpha < \beta$ entonces $S\alpha \subsetneq S\beta$ y $\alpha S \subsetneq \beta S$.

Demostración. Suponga que $\alpha < \beta$. Entonces de la Proposición 7.1.11 se sigue que $S\alpha \subseteq S\beta$ y $\alpha S \subseteq \beta S$. **Afirmación:** $\beta \notin \alpha S$ y $\beta \notin S\alpha$. En efecto, suponga que $\beta \in \alpha S$. Entonces puede escribirse $\beta = \alpha x$ para algún $x \in S$ y por lo tanto $\alpha\beta = \alpha^2 x = \alpha x = \beta$. Ahora bien, puesto que $\alpha < \beta$, entonces $\alpha\beta = \alpha$ con $\alpha \neq \beta$. Así que $\alpha = \alpha\beta = \beta$, lo cual es una contradicción. Por consiguiente $\beta \notin \alpha S$. De manera análoga se muestra que $\beta \notin S\alpha$. Esto último sumado a que $\beta \in S\beta$ y $\beta \in \beta S$ permite concluir que $S\alpha \subsetneq S\beta$ y $\alpha S \subsetneq \beta S$.

□

Retomando a las familias $\mathcal{F}$ y $\mathcal{G}$ en ellas se verifica lo siguiente.

Proposición 10.0.9.

Para cada $n \in \mathbb{N}_0$ se tiene que $I_{n+1} \subsetneq I_n$ y $J_{n+1} \subsetneq J_n$. En consecuencia $\mathcal{F}$ y $\mathcal{G}$ son cadenas descendentes que no se estacionan.

Demostración. Sea $n \in \mathbb{N}_0$. Puesto que $n < n+1$ de la Proposición 10.0.5 se sigue que $(n+1, n+1) < (n, n)$ de manera que de la Proposición 10.0.8 se deduce que $I_{n+1} \subsetneq I_n$ y $J_{n+1} \subsetneq J_n$.

□

Corolario 10.0.10.

$\mathbb{B}$ no es completamente simple.

Demostración. De que $\mathcal{F}$ y $\mathcal{G}$ son cadenas descendentes que no se estacionan se sigue que $\mathbb{B}$ no contiene ideales izquierdos minimales ni ideales derechos minimales. Por consiguiente $\mathbb{B}$ no puede ser completamente simple.

□

.

Conclusiones

Los semigrupos son de las estructuras más básicas del álgebra en el sentido de que éstos solo cuentan con una operación binaria asociativa. Así que las carencias exigen cierta dosis de esfuerzo al momento de establecer resultados concernientes a ellos. Una buena técnica para obtener ideas al momento de trabajar con semigrupos es la de importar técnicas, métodos o conceptos ya conocidos de otras estructuras más complejas. Un ejemplo de ello es el concepto de semigrupo cociente o el concepto de ideal de un semigrupo, que como es de esperarse, fueron inspirados en el de grupo cociente y en el de ideal de un anillo. Con respecto a los semigrupos regulares, en esta parte del trabajo se pudo apreciar que los elementos idempotentes fueron una parte fundamental de la teoría, pues a partir de ellos es posible definir grupos, de manera que puede tratarse a un semigrupo regular localmente como si fuese un grupo y aprovechar entonces las propiedades que tales estructuras poseen. Algunas veces también fue necesario obtener elementos con propiedades particulares que nos ayuden a resolver ciertas cuestiones. Por ejemplo, es fructífero obtener maneras de conseguir idempotentes a partir de otros elementos dados. Varios de estos métodos se pueden encontrar en las pruebas de la sección de semigrupos regulares. En cuanto al orden como concepto básico en el estudio de los semigrupos, dotar al conjunto de idempotentes de un semigrupo de cierta relación de orden parcial resultó indispensable en el estudio de los semigrupos completamente simples, pues como pudo verse, este tipo de semigrupos regulares tiene la característica de que cualquiera de sus idempotentes es minimal, además de que, de hecho, los semigrupos completamente simples están definidos por medio de ideales minimales, definición que en el fondo resulta de ordenar a los ideales izquierdos y derechos a través de la inclusión y entonces considerar a sus elementos minimales. También resulta interesante el hecho de que cierto tipo de semigrupos (a saber, las bandas conmutativas), permiten definir a ciertas estructuras de orden (a saber, las semiretículas inferiores y superiores), y viceversa. Finalmente, las relaciones de Green son herramientas importantes dentro de la teoría de semigrupos, pues como se vio, a partir de ellas se pueden definir relaciones de equivalencia que permiten descomponer a un semigrupo en clases, en algunos casos, más sencillas de manipular.

.

Bibliografía

[1] M. Kilp, U. Knauer y A. Mikhalev. *Monoids, Acts and Categories*. Walter de Gruyter, 2000.

[2] J.M. Howie. *Fundamentals of Semigroup Theory*. London Mathematical Society Monographs, 1996.

[3] S. Lang. *Algebra*. Springer-Verlag, Graduate Texts in Mathematics, Vol.211, 2002.

[4] J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, Graduate Texts in Mathematics, Vol.148, 1995.

[5] J. Adámek, H. Herrlich y G.E Strecker. *Abstract and Concrete Categories: The Joy of Cats*. Dover Books on Mathematics, 1990.

[6] F. Borceux. *Handbook of Categorical Algebra. Volume 1: Basic Category Theory*. Cambridge University Press, 1994.

[7] T. Leinster. *Basic Category Theory*. Cambridge University Press, 2014.

[8] F. Hernández. *Teoría de conjuntos. Una introducción*. Instituto de Matemáticas, UNAM, 2019.