Tema 1: Semigrupos

1. Semigrupos: Conceptos fundamentales.

Recordemos que un **sistema algebraico** es un conjunto S con una o varias operaciones sobre él, siendo una **operación ó ley de composición interna** una aplicación de $S \times S$ en S. Usualmente, se denotan las operaciones mediante símbolos: $*, +$, etc. entendiendo que $a + b$ es al imagen del par $(a, b) \in S \times S$ mediante la operación definida $+$ en S.

Ejemplo. $(\mathbb{N}, +)$, $(\mathbb{Z}, -)$ son ejemplos de sistemas algebraicos con una única operación.

Como es sabido, las operaciones pueden presentar diversas propiedades. Supongamos que $(S, .)$ es un sistema algebraico. Entonces, . puede verificar las siguientes propiedades:

(i) **Asociativa**: $\forall a, b, c \in S$, $(a.b).c = a.(b.c)$.

(ii) **Conmutativa**: $\forall a, b \in S$, $a.b = b.a$.

(iii) **Existencia de elemento neutro o identidad**: $\exists e \in S$ tal que $\forall a \in S$, $a.e = a = e.a$.

(iv) **Existencia de elemento opuesto o inverso**: $\forall a \in S$, $\exists a^{-1} \in S$, tal que $a.a^{-1} = e = a^{-1}.a$, donde e es el elemento nuetro de ..

Un elemento de un monoide se dice que es **inversible** si tiene elemento inverso.

A veces se suele hablar de elemento neutro a derecha o a izquierda. Así, un elemento $d \in S$ se dice que es un **elemento neutro a derecha** si para todo $x \in S$ se cumple $x.d = x$ y un elemento $l \in S$ se dice que es un **elemento neutro a izquierda** si para todo $x \in S$ se cumple $l.x = x$. Lo mismo sucede con los elementos inversos: si se cumple sólo una de las igualdades se dice que es un elemento inverso a derecha o a izquierda.

Definición. Sea $(S, .)$ un sistema algebraico. Se dice que $(S, .)$ es un **semigrupo** si . verifica la propiedad asociativa.

Un semigrupo $(S, .)$ se dice que es **conmutativo**, si . es conmutativa.

Un semigrupo $(S, .)$ se dice que es **monoide** si . tiene elemento neutro.

Un monoide $(S, .)$ se dice que es un **grupo**, si . verifica la existencia de elemento inverso para todo $a \in S$.

Ejemplos.

(1) $(\mathbb{N}, +)$ es un semigrupo y $(\mathbb{Z}, -)$ no lo es.

(2) $(\mathbb{R}, *)$, donde $a * b = 2a + 2b$ no es un semigrupo.

(3) $(\mathbb{N} \cup \{0\}, +)$ es un monoide conmutativo.

(4) $(S, *)$, donde $s_1 * s_2 = s_1$ para todo $s_1, s_2 \in S$, es un semigrupo que no tiene elemento identidad si $|S| \geq 2$.

Se dice que un semigrupo $(S, .)$ es finito si el conjunto S es finito.

Para los semigrupos finitos podemos construir la llamada **tabla del semigrupo** que viene dada por:

$\cdot$	s_1	s_2	$\ldots$	s_n
s_1	$s_1 \cdot s_1$	$s_1 \cdot s_2$	$\ldots$	$s_1 \cdot s_n$
s_2	$s_2 \cdot s_1$	$s_2 \cdot s_2$	$\ldots$	$s_2 \cdot s_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
s_n	$s_n \cdot s_1$	$s_n \cdot s_2$	$\ldots$	$s_n \cdot s_n$

En el caso de que S sea un monoide finito con $|S| \geq 2$ podemos extraer algunas consecuencias de su tabla: no aparecen dos filas ni dos columnas distintas iguales. Además, para localizar los posibles elementos neutros bastará con localizar aquellos elementos que verifiquen $s.s = s$, esto es los elementos **idempotentes** y entre éstos examinar si son o no elementos neutros.

En relación a los elementos idempotentes es fácil demostrar que en un grupo el único elemento idempotente es el elemento identidad. En cambio, en un semigrupo puede haber más de un elemento idempotente. Por ejemplo, si consideramos $(\mathbb{Z}, .)$ el elemento 0 es idempotente y no es el elemento identidad en este semigrupo.

Otros elementos interesantes en un sistema algebraico son los **elementos cero**

Definición. Sea $(S, .)$ un sistema algebraico y $s \in S$. Se dice que s es un **elemento cero a derecha** si para todo $x \in S$ se verifica $x.s = s$.

Definición. Sea $(S, .)$ un sistema algebraico y $s \in S$. Se dice que s es un **elemento cero a izquierda** si para todo $x \in S$ se verifica $s.x = s$.

Definición. Sea $(S, .)$ un sistema algebraico y $s \in S$. Se dice que s es un **elemento cero** si para todo $x \in S$ se verifica $x.s = s = s.x$.

Es inmediato demostrar:

Proposición 1.1. *Sea $(S, .)$ un sistema algebraico. Si $r \in S$ es un elemento cero a derecha y $l \in S$ es un elemento cero z izquierda, entonces $s = l$.*

Como consecuencia de esta proposición, se tiene:

Corolario 1.2. *Sea $(S, .)$ un sistema algebraico. Si existe un elemento cero, entonces éste es único.*

Por otro lado, es evidente que todo elemento cero de un semigrupo es un elemento idempotente.

Ejemplos.

(1) En el monoide $S = \{f : \mathbb{R}\times\mathbb{R} \to \mathbb{R}\times\mathbb{R} \mid f \text{ es aplicación}\}$ con la operación composición de aplicaciones ($f \circ g$ es la imagen por la operación del par (f, g))los elementos inversibles son las aplicaciones biyectivas. Existen elementos cero a izquierda son las aplicaciones constantes y tiene elementos idempotentes, como por ejemplo aplicaciones del tipo $f(x, y) = (x, c)$ donde c es una constante ó $f(x, y) = (c, y)$ ó las aplicaciones constantes.

(2) Sea S un conjunto no vacío. Si $\mathfrak{B}(S) = \{M \mid M \subseteq S\}$, sabemos que $(\mathfrak{B}(S), \cap)$ es un monoide con elemento neutro S y en el que todo elemento es idempotente. Además, $\emptyset$ verifica que es un elemento cero.

La siguiente construcción nos permite adjuntar un elemento cero y un elemento identidad a aquellos semigrupos que no los posean:

Teorema 1.3. *Sea $(S, .)$ un semigrupo sin elemento cero y $0 \notin S$. En $S' = S \cup \{0\}$ definimos la operación $*$ como sigue*

$$s * s' = \begin{cases} s.s', & \textit{si } s, s' \in S; \\ 0 & \textit{si } s = 0 \textit{ ó } s' = 0. \end{cases}$$

Entonces, 0 es un elemento cero de $(S \cup \{0\}, *)$.

Teorema 1.4. *Sea* $(S, .)$ *un semigrupo sin elemento identidad y* $1 \notin S$*. En* $S' = S \cup \{1\}$ *definimos la operación* $*$ *como sigue*

$$s * s' = \begin{cases} s.s', & si\ s, s' \in S; \\ s & si\ s' = 1 \\ s' & si\ s = 1. \end{cases}$$

Entonces, 1 *es un elemento identidad de* $(S \cup \{1\}, *)$*.*

2. Subsemigrupos.

Definición. Sea $(S, .)$ un semigrupo y $A \subseteq S$. Se dice que A es un **subsemigrupo** de S si $(A, ._{|A})$ es un semigrupo.

Cuando A sea subsemigrupo de S escribiremos: $A \leq S$.

Definición. Sea $(S, .)$ un monoide y $A \subseteq S$. Se dice que A es un **submonoide** de S si $(A, ._{|A})$ es un monoide.

Dado un semigrupo $(S, .)$ y $A \subseteq S$, si denotamos por A^2 al conjunto $\{a.b \mid a, b \in A\}$, podemos dar una caracterización equivalente del concepto de semigrupo. En efecto,

Proposición 2.1. *Sea* $(S, .)$ *un semigrupo y* $A \subseteq S$*. Entonces,* A *es subsemigrupo de* S *si y sólo si* $A^2 \subseteq A$*.*

Ejemplo. $(\mathbb{N}, +)$ es un subsemigrupo de $(\mathbb{Z}, +)$.

Como se observa en el ejemplo anterior, un subsemigrupo de un monoide no tiene que ser necesariamente submonoide. Más aún, si A es un submonoide del monoide S, puede suceder que tenga A y S elementos identidad distintos. Por ejemplo, $(\{0\}, .)$ es un submonoide de $(\mathbb{Z}, .)$. y el elemento neutro del primero es el 0 y del segundo 1.

Por otro lado, puede suceder que un semigrupo o un monoide tengan subsemigrupos que sean además grupos. Por ejemplo, en $(\mathbb{Z}, .)$ el subsemigrupo $(\{1, -1\}, .)$ es un grupo. Al subsemigrupo más grande que sea grupo lo llamaremos grupo de las unidades.

Definición. Sea $(S, .)$ un monoide. Al conjunto $G_S = \{s \in S \mid s \text{ es inversible}\}$ se le llama **grupo de las unidades de** $(S, .)$.

Es inmediato probar que G_S es un conjunto no vacío y que $(G_S, .)$ es un grupo. Cuanto mayor sea G_S más próximo está el monoide S de ser un grupo.

Ejemplo. En el monoide $S = \{f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R} \mid f \text{ es aplicación}\}$ con la operación composición de aplicaciones ($f \circ g$ es la imagen por la operación del par (f, g)) el grupo de las unidades G_S viene dado por $G_S = \{f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R} \mid f \text{ es biyectiva}\}$

Nos ocupamos ahora de estudiar que sucede con la intersección y unión de subsemigrupos.

Proposición 2.2. *Sea $(S, .)$ un semigrupo. Cualquier intersección de subsemigrupos no vacía es un subsemigrupo.*

En cambio, la unión de subsemigrupo no es necesariamente un subsemigrupo. Por ejemplo, si tomamos el semigrupo $(\mathbb{Z}, .)$ y los subsemigrupos $S_1 = \{2^n \mid n \in \mathbb{N}\}$ y $S_2 = \{1, -1\}$ resulta que $S_1 \cup S_2$ no es subsemigrupo de $(\mathbb{Z}, .)$ ya que $-1.2^n \notin S_1 \cup S_2$.

Por otro lado, si $(S, .)$ es un semigrupo y $\emptyset \neq T \subseteq S$, podemos considerar todos los subsemigrupos de S que contengan a T. Entonces, según acabamos de ver, la intersección de éstos es un subsemigrupo, que además es el más pequeño que contiene a T. A este subsemigrupo se le llama **subsemigrupo generado por** T y lo denotaremos por $< T >$. Si $T = \{t_1, \ldots, t_n\}$ escribiremos $< t_1, \ldots, t_n >$ en lugar de $< \{t_1, \ldots, t_n\} >$ para denotar el subsemigrupo generado por T.

Es obvio que T es un subsemigrupo de $(S, .)$ si y sólo si $T =< T >$. Por otro lado, de la propia definición de $< T >$, se sigue que $T \subseteq< T >$. Además, si denotamos por $T^k = \{t_1 \ldots t_k \mid t_1, \ldots t_k \in T\}$, siendo $k \in \mathbb{N}$, podemos dar una caracterización de $< T >$:

Proposición 2.3. *Sea $(S, .)$ un semigrupo y $\emptyset \neq T \subseteq S$. Entonces, $< T >= \cup_{n \in \mathbb{N}} T^n$.*

Cada semigrupo $(S, .)$ verifica que $< S >= S$. Además, si T cumple $< T >= S$ (esto es T **genera a** S y $T \subseteq V \subseteq S$, es claro que $< V >= S$. Entonces, nos intersa buscar los subconjuntos T que sean lo más pequeños posibles y que generen a S.

Definición. Sea $(S, .)$ un semigrupo. Se dice que S está **finitamente generado** si existe T finito tal que T genere a S.

Definición. Sea $(S, .)$ un semigrupo. Se dice que S es **cíclico** si existe $t \in S$ tal que $< t >= S$.

Ejemplos.

(1) El semigrupo $(\mathbb{N}, +)$ es un semigrupo cíclico ya que $< 1 >= \mathbb{N}$.

(2) El semigrupo $(\mathbb{N} \cup \{0\}, +)$ está finitamente generado ya que $< 0, 1 >= \mathbb{N}$ pero no es cíclico.

(3) El semigrupo $(\mathbb{N}, .)$ no es cíclico ni finitamente generado.

3. Homomorfismos de semigrupos.

Un concepto intersante de analizar son las aplicaciones entre semigrupos que conservan las operaciones: los homomorfismos de semigrupos.

Definición. Sean $(S_1, .)$ y $/S_2, *)$ dos semigrupos y $f : S_1 \to S_2$ una aplicación entre ellos. Se dice que f es un **homomorfismo** entre los semigrupos S_1 y S_2 si $\forall x, y \in S_1$ se verifica $f(x.y) = f(x) * f(y)$.

Denotaremos por $Hom(S_1, S_2) = \{f : S_1 \to S_2 \mid f \text{ es homomorfismo}\}$

Un **monomorfismo** es un homomorfismo inyectivo. Un **epimorfismo** es un homomorfismo sobreyectivo. Finalmente, Un **isomorfismo** es un homomorfismo biyectivo. Cuando exista un isomorfismo entre los semigrupos S_1 y S_2 diremos que S_1 y S_2 son **semigrupos isomorfos** y lo denotaresmo por $S_1 \cong S_2$.

Ejemplo. La aplicación $f : (\mathbb{Z}, .) \to (\mathbb{N} \cup \{0\}, .)$ definida por $f(x) = |x|$ es un epimorfismo que no es inyectivo.

Los epimorfismos tienen una propiedad interesante con respecto a los elementos cero e identidad:

Teorema 3.1. *Sea $f : S_1 \to S_2$ un epimorfismo. Entonces,*

(i) Si a es un elemento cero de S_1, entonces $f(a)$ es un elemento cero de S_2.

(ii) Si e es un elemento identidad de S_1, entonces $f(e)$ es un elemento identidad de S_2.

Si f es un homomorfismo no sobreyectivo, el teorema anterior no tiene porqué verificarse. Por ejemplo, el homomorfismo $f : (\mathbb{N}, .) \to (\mathbb{Z}, .)$ definido por $f(n) = 0$ no verifica que $f(1)$ sea un elemento identidad de $(\mathbb{Z}, .)$.

Definición. Sea $(S, .)$ un semigrupo y $\equiv$ una relación de equivalencia sobre S. Se dice que la relación $\equiv$ es **estable** con la operación . si se verifica la siguiente condición: Para todo $a, a', b, b' \in S$ tales que $a \equiv a'$ y $b \equiv b'$, se tiene $a.b \equiv a'.b'$.

Para las relaciones de equivalencia estables, podemos definir en el conjunto cociente una nueva operación $[a].[b] = [a.b]$. Con esta operación, dotamos al conjunto cociente de la estructura de semigrupo. Es fácil demostrar:

Teorema 3.2. *Sea* $(S, .)$ *un semigrupo y* $\equiv$ *una relación de equivalencia estable con la operación* $.$ *. Entonces,* $(S/\equiv, .)$ *es un semigrupo llamado* **semigrupo cociente de** $(S, .)$ **sobre** $\equiv$*. Además, la aplicación* $f : S \to S/\equiv$*, definida por* $f(a) = [a]$ *es un epimorfismo de semigrupos llamado* **epimorfismo canónico***.*

Por otro lado, a partir de un epimorfismo de semigrupos podemos definir una relación de equivalencia estable:

Teorema 3.3. *Sea* $f : S \to S'$ *un epimorfismo de semigrupos y sea* $\equiv$ *la relación definida en* S *mediante* $\forall s_1, s_2 \in S$*,* $s_1 \equiv s_2$ *si y solo si* $f(s_1) = f(s_2)$*. Entonces,*

(i) $\equiv$ *es una relación de equivalencia sobre* S*.*

(ii) La relación $\equiv$ *es estable con la operación definida en* S*.*

(iii) $(S/\equiv, .)$ *es isomorfo a* $(S', .')$*.*

Observación. Si en el enunciado del teorema anterior eliminamos la condición de sobreyectividad en el homomorfismo f , se verificaría (i) e (ii), pero no (iii).

Según el teorema 1.4, podemos construir un monoide a partir de un semigrupo no monoide cuya operación restringida al semigrupo coincida con la del semigrupo. Esto nos permite demostrar una generalización del Teorema de Cayley que pone de manifiesto la importancia de los grupos $(N^N, \circ)$, donde $N^N = \{f : N \to N \mid f \text{ es aplicación}\}$:

Teorema 3.4. *Para cualquier semigrupo* $(S, .)$*, existe un monoide* N *y un monomorfismo* $\psi : S \to N^N$*.*

Demostración. Si S es un monoide, tomamos $N = S$. En otro caso, por el teorema 1.4, construimos el monoide $N = S \cup \{1\}$. Para cada $s \in S$, definimos $f_s : N \to N$, mediante $f_s(x) = s.x$. Entonces, la aplicación $\psi : S \to N^N$ dada por $\psi(s) = f_s$ es un monomorfismo. □

Observación. El hecho de ser N un monoide es fundamental para probar la inyectividad de la aplicación ψ construida.

4. Producto directo de semigrupos.

Sean $(S_1, ._1)$ y $(S_2, ._2)$ dos semigrupos. En el conjunto $S_1 \times S_2 = \{(s_1, s_2) \mid s_i \in S_i,\ i = 1, 2\}$ definimos la operación $*$ $(s_1, s_2) * (s_1', s_2') = (s_1 ._1 s_1', s_2 ._2 s_2')$. Es fácil demostrar que con la operación anterior dotamos a $S_1 \times S_2$ de la estructura de semigrupo, al que llamaremos

producto directo de $(S_1, \cdot_1)$ **y** $(S_2, \cdot_2)$. De forma análoga, se define el producto directo de un número finito de semigrupos.

Ejemplo. Si tomamos $(\mathbb{Z}, +)$ y $(\mathbb{N}, .)$ podemos definir en $\mathbb{Z} \times \mathbb{N}$ la operación $*$ $(z, n) * (z', n') = (z + z', n.n')$.

Cuando tenemos un producto directo de un número finito de semigrupos , aparecen unas aplicaciones llamadas **proyecciones** $\pi_i : \prod_{j=1}^{n} S_j \to S_i$ definida por $\pi_i(s_1, \ldots, s_n) = s_i$. Es fácil comprobar que estas aplicaciones son, en realidad, epimorfismos de semigrupos.

5. Semigrupo libre de palabras.

Analizamos en este párrafo un tipo especial de semigrupos: los llamados semigrupos libres.

Definición. Sea $(F, .)$ un semigrupo y $\emptyset \neq B \subseteq F$. Se dice que F es **semigrupo libre** sobre B, si cada aplicación $f : B \to S$, donde S es un semigrupo arbitrario, se puede extenser de forma única a un homomorfismo $h : F \to S$, es decir,

$$\forall S \text{ semigrupo y } \forall f : B \to S \text{ aplicación}, \exists! h \in \mathrm{Hom}(F, S), \text{ tal que } h|_B = f.$$

Cuando F es un semigrupo libre sobre B, se suele decir que B es **base** de F.

En relación a este concepto, aparecen de forma inmediata diversas cuestiones, como por ejemplo, si todo semigrupo es semigrupo libre para alguna base B, o si dos bases de un mismo semigrupo libre deben tener el mismo cardinal. Con los siguientes resultados, vamos a ver que la respuesta a la primera cuestión es negativa y a la segunda afirmativa.

Teorema 5.1. *Sea F un semigrupo libre con base B. Entonces, $< B >= F$.*

Observación. El teorema anterior nos indica que el semigrupo libre con base B coincide con el semigrupo generado por B.

Otra cuestión que surge de manera inmediata es si dado cualquier subconjunto B podemos construir un semigrupo libre con base B.

Teorema 5.2. *Sea B un subconjunto no vacío. Entonces, existe F semigrupo libre con base B.*

Observación. El teorema anterior ha permitido describir cómo son los elementos y cómo operar en el semigrupo libre con base B. A esta operación se le suele llamar **concatenación**.

A continuación justificamos por qué hemos indicado “el” semigrupo libre y no “un” semigrupo libre.

Teorema 5.3. *Sean F y F' dos semigrupos libre de bases B y B', respectivamente. Entonces, F y F' son isomorfos si y solo si $|B| = |B'|$.*

Como consecuencia del teorema anterior, tenemos los siguientes corolarios:

Corolario 5.4. *Dado un conjunto B no vacío, el semigrupo libre con base B es único, salvo isomorfismos.*

Corolario 5.5. *Si B y B' son dos bases para el semigrupo libre F, entonces $|B| = |B'|$.*

En lo que sigue, denotaremos por F_B el semigrupo libre con base B y a veces escribiremos F_β para denotar el semigrupo libre con base un conjunto B con β elementos. A sus elementos se les suele llamar **palabras** sobre el alfabeto B. Si además consideramos Λ la palabra vacía, denotaremos por Ω_B a $F_B \cup \{\Lambda\}$.

Hasta ahora los resultados vistos nos han permitido describir como es el semigrupo libre con base B. De esta descripción, podemos deducir que F_B es infinito, luego no existen semigrupos libres de cardinal finito. Por otro lado, si $|B| = 1$, sabemos que $F_B = \{b, b^2, b^3, \ldots\}$ y es posible establecer un isomorfismo entre F_B y el semigrupo $(\mathbb{N}, +)$ (basta considerar $h : F_B \to \mathbb{N}$ definida por $h(b_k) = k$). En particular, F_B será conmutativo cuando $|B| = 1$. En cambio, si $|B| \geq 2$, como $b_1b_2 \neq b_2b_1$ si $b_1 \neq b_2$, podemos deducir que F_B no es conmutativo.

Otra de las características de los semigrupos libres es que cualquier semigrupo es la imagen homomorfa de un semigrupo libre, tal y como lo indica el siguiente resultado:

Teorema 5.6. *Sea S un semigrupo con sistema generador E y F el semigrupo libre con base E. Entonces, existe un epimorfismo $h : F_E \to S$.*

Por otro lado, los semigrupos libres nos sirven para describir los semigrupos en términos de generadores y relaciones:

Definición. Sea S un semigrupo generado por un conjunto X y $\equiv$ una relación de equivalencia definida sobre F_X tal que $S \cong F_X/\equiv$. Entonces, al par (X, R) se le llama **presentación de** S y a los elementos de R **relaciones definitorias de** S.

Ejemplo. Consideremos el semigrupo $(\mathbb{Z}_4, .)$. Sea $X = \{2, 3\}$ y $x_1 = 2$ y $x_2 = 3$. Definimos la relación de equivalencia que se deduce de las siguientes igualdades: $x_2^3 = x_2$, $x_1x_2 = x_2x_1$, $x_2x_1 = x_1$, $x_1^2 = x_1^3$. Entonces, las clases de equivalencia vendrán dadas por

$a_0 = [x_1^2]$, $a_1 = [x_2^2]$, $a_3 = [x_1]$ y $a_4 = [x_2]$. Entonces, si definimos en $F_X/\equiv$ la operación: $[y] * [z] = [yz]$, tenemos la siguiente tabla:

$\cdot$	a_0	a_1	a_2	a_3
a_0	a_0	a_0	a_0	a_0
a_1	a_0	a_1	a_2	a_2
a_2	a_0	a_2	a_0	a_2
a_3	a_0	a_3	a_2	a_1

Al comparar la tabla anterior con la que se obtiene para $(\mathbb{Z}_4, .)$, observamos que se puede establecer un isomorfismo ψ entre $(\mathbb{Z}_4, .)$ y $(F_X/\equiv, *)$, dado por $\psi(i) = a_i$.

Para finalizar este apartado, señalamos que se puede realizar una construcción análoga de monoides libres: basta reemplazar "semigrupo" por "monoide" en la definición de semigrupo libre. Además, empleando los mismos razonamientos, se puede demostrar que, salvo isomorfismos, existe un único monoide libre con base B, siendo B un conjunto no vacío y que cualquier monoide es imagen homomorfa de un monoide libre.