Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Departamento de Matemática - Escuela de Ciencias Exactas y Naturales
COMPLEMENTOS DE MATEMÁTICA II
Licenciatura en Ciencias de la Computación - Año 2023
Docentes: Francisco Vittone - Mauro Lucci - Delfina Martin

Unidad 4: Operaciones en un conjunto - Semigrupos, monoides y grupos.

---

1. Operaciones binarias

En los distintos cursos de la carrera han aparecido conjuntos con operaciones diferentes. Partiendo de los conjuntos numéricos con la suma y el producto, pasando por los conjuntos de matrices con la suma y la multiplicación, los conjuntos de polinomios o de funciones, etc. En la unidad anterior hemos presentado un conjunto con dos operaciones, los retículos, que no forman parte de las operaciones usuales, pero comparten con éstas propiedades como la asociatividad o la conmutatividad.

A partir de esta unidad estudiaremos de forma abstracta un conjunto con una operación en él definida, y veremos que las distintas propiedades que tiene o no tiene dicha operación dan lugar a estructuras algebraicas distintas. Comenzamos repasando algunos conceptos básicos:

Definición **1.** *Sea X un conjunto. Una* ***operación*** *(binaria) en X es una función $* : X \times X \to X$. Normalmente denotamos $x * y := *(x, y)$. Se dice que:*

- *$*$ es* ***asociativa*** *si para cada $x, y, z \in X$, $*(x, *(y, z)) = *(*(x, y), z)$, o sea*

$$x * (y * z) = (x * y) * z.$$

- *$*$ admite un* ***elemento neutro a derecha*** *si existe $e_d \in X$ tal que $*(x, e_d) = x$ para cada $x \in X$, o sea,*

$$x * e_d = x.$$

  $*$ admite un ***elemento neutro a izquierda*** *si existe $e_i \in X$ tal que $*(e_i, x) = x$ para cada $x \in X$, o sea,*

$$e_i * x = x.$$

  Decimos que $*$ admite un ***elemento neutro*** *o* ***elemento identidad*** *si existe $e \in X$ tal que e es un neutro a derecha y un neutro a izquierda.*

- *Si $*$ admite un elemento neutro e, decimos que un elemento $x \in X$ admite un* ***inverso a derecha*** *para $*$ si existe un elemento $x_d^* \in X$ tal que $x * x_d^* = *(x, x_d^*) = e$ y admite un* ***invervsor a izquierda*** *existe $x_i^* \in X$ tal que $x_i^* * x = *(x_i^*, x) = e$.*

  $x \in X$ admite un ***inverso*** *si existe $x^* \in X$ tal que x^* es inverso a izquierda y a derecha de x.*

- *Un elemento $a \in X$ se dice un* ***elemento absorvente a derecha*** *para $*$ si $x * a = a$ para cada $x \in X$, y se dice un* ***elemento absorvente a izquierda*** *para $*$ si $a * x = a$ para cada $x \in X$. a es un* ***elemento absorvente*** *si es absorvente a derecha e izquierda.*

- *$*$ es* ***conmutativa*** *si para cada $x, y, z \in X$, $*(x, y) = *(y, x)$, o sea*

$$x * y = y * x.$$

Analicemos a continuación las propiedades que tienen las operaciones con las que normalmente trabajamos.

Ejemplos **1.** 1. Consideremos la suma $(+)$ en el conjunto $\mathbb{N}$ de los números naturales. Entonces $\mathbb{N}$ es asociativa y conmutativa, pero no existe elemento neutro a derecha ni a izquierda. Por lo tanto tampoco tiene sentido hablar del inverso de ningún elemento.

   Si ahora consideramos el producto $(\cdot)$ en $\mathbb{N}$, $\cdot$ es nuevamente una operación asociativa y conmutativa, con elemento neutro (el 1), y donde 1 es el único elemento que admite un inverso.

   Tanto la suma como el producto no admiten elementos absorventes.

   Pasemos a $\mathbb{Z}$. En este caso la suma, además de ser asociativa y conmutativa admite un elemento neutro, el 0, y cada $k \in \mathbb{Z}$ admite un inverso, en este caso $-k$. El producto en $\mathbb{Z}$ tiene las mismas propiedades que en $\mathbb{N}$, solo que aquí existen dos elementos *invertibles*, es decir que admiten un inverso: 1 y -1. El 0 es además un elemento absorvente para el producto.

   En $\mathbb{Q}$ y $\mathbb{R}$ tanto la suma como el producto son operaciones asociativas, conmutativas, con elemento neutro (0 y 1 respectivamente). Todo elemento admite un inverso para la suma (su opuesto), y todo elemento, salvo el 0, admite un inverso para el producto (su recíproco). El 0 es un elemento absorvente para el producto.

2. Consideremos el conjunto $M_{n\times n}$ de matrices $n \times n$ a coeficientes reales. En $M_{n\times n}$ podemos definir la operación suma, que es asociativa, conmutativa, admite un elemento neutro (la matriz $0_{n\times n}$ cuyas entradas son todas 0), y todo elemento admite un inverso (si $M = (m_{ij}) \in M_{n\times n}$, su inverso para la suma es la matriz $-M$ cuyas entradas son $(-M)_{ij} = -m_{ij}$). Todas las propiedades de la suma de matrices son consecuencia de las propiedades análogas de la suma de números reales.

   En $M_{n\times n}$ tenemos además definido el producto de matrices: si $M = (m_{ij})$, $R = (r_{ij}) \in \mathcal{M}_{n\times n}$, entonces

$$(MR)_{ij} = \sum_{k=1}^{n} m_{ik} r_{kj} \tag{1}$$

   Es fácil ver que el producto de matrices así definido es asociativo y admite un elemento neutro, la matriz identidad Id, cuyas entradas son 1 en la diagonal y 0 en el resto. No todo elemento admite un inverso. De hecho, sabemos del álgebra lineal que $M \in M_{n\times n}$ admite inverso si y sólo si $\det(M) \neq 0$. La matriz $0_{n\times n}$ cuyas entradas son todas 0 es un elemento absorvente para el producto. Esta operación tampoco es conmutativa (dejamos como ejercicio dar un contraejemplo).

3. Consideremos un retículo $(L, \vee, \wedge)$. Las operaciones $\vee$ y $\wedge$ son dos operaciones binarias en L que resultan asociativas y conmutativas. No siempre admiten un elemento neutro. De hecho, hemos visto en la unidad anterior que de existir un neutro para $\vee$, se debe verificar $x \vee e = x$ para todo $x \in X$ (como la operación es conmutativa, cualquier neutro a derecha lo será también a izquierda) y esto ocurre si y sólo si L tiene un elemento mínimo. En caso de tener además un elemento máximo, 1, éste es un elemento absorvente para $\vee$, dado que $x \vee 1 = 1 \vee x = 1$ para cada $x \in X$.

   De manera similar, $\wedge$ admite un elemento neutro si y sólo si L tiene un máximo. En este caso, el elemento absorvente, si existe, será el mínimo de L.

   En particular, en un retículo acotado tanto $\wedge$ como $\vee$ admiten un elemento neutro y un elemento absorvente. Además, en ambos casos, ningún elemento salvo el neutro admiten un inverso (ejercicio).

   En particular podemos considerar los siguientes ejemplos:

   - Si $X \neq \emptyset$, la unión e intesersección de conjuntos son operaciones asociativas y conmutativas en $\mathcal{P}(X)$, con elemento neutro ($\emptyset$ y X respectivamente), donde ningún otro elemento distinto del neutro admite un inverso.
   - En D_n,, mcd y mcm son operaciones asociativas y conmutativas, con neutros 1 y n respectivamente, y tales que ningún otro elemento admite inverso.

     Si consideramos estas operaciones en $\mathbb{N}$, entonces ambas son asociativas y conmutativas, pero sólo mcd admite un elemento neutro.
   - Si consideramos el conjunto totalmente ordenado $\{0, 1\}$, las operaciones $\vee$ y $\wedge$ son asociativas, conmutativas, con elemento neutro 1 y 0. Este es el único caso de un conjunto totalmente ordenado que es un álgebra de Boole. Las operaciones $\vee$ y $\wedge$ en este caso suelen denotarse por $+$ y $\cdot$ respectivamente, y vienen dadas por las siguientes tablas:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

4. Sea $B = \{0, 1\}$ con el orden usual y las operaciones $+ = \vee$ y $\cdot = \wedge$ definidas en el ejemplo antarior. Sea $M_{n\times n}(B)$ el conjunto de matrices $n \times n$ cuyos coeficientes están en B. Podemos definir una suma en $M_{n\times n}(B)$ de la siguiente manera: si $M = (m_{ij})$, $R = (r_{ij})$ (observemos que M y R son matrices de 0 y 1), entonces

$$(M + N)_{ij} = m_{ij} + r_{ij}$$

   donde la última suma es la operación $+ = \vee$ en B. Como la suma en B es asociativa, es fácil ver que la suma en $\mathcal{M}_{n\times n}(B)$ es asociativa y que la matriz $0_{n\times n}$ es un elemento neutro. Sin embargo, ningún otro elemento de $\mathcal{M}_{n\times n}(B)$ admite un inverso (¿por qué?).

   Como la suma es asociativa, podemos también definir el producto de matrices de $M_{n\times n}(B)$ mediante ecuación (1), donde la suma y el producto en este caso son las operaciones de B. Dejamos como ejercicio

probar que el producto en $M_{n\times n}(B)$ es asociativo (¿qué propiedad de B garantiza esta propiedad de $M_{n\times n}(B)$?). La matriz identidad es nuevamente un elemento neutro. ¿Qué matrices admiten un inverso?

5. Sea $A \neq \emptyset$ y sea $\mathcal{F}(A) = \{f : A \to A\}$ el conjunto de las funciones de A en A. Entonces es posible componer dos elementos de $\mathcal{F}(A)$ y obtener otro elemento del mismo conjunto, con lo cual la composición de funciones es una operación bien definida en $\mathcal{F}(A)$.

   Esta operación es asociativa, no conmutativa, y la función identidad $Id : A \to A$ tal que $Id(x) = x$ es el elemento neutro. Si una función es biyectiva, entonces admite un inverso. Sin embargo pueden existir funciones no biyectivas que admitan un inverso a derecha o izquierda.

   Consideremos por ejemplo $A = \mathbb{N}$ y sea $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = 2n$. Entonces si $g : \mathbb{N} \to \mathbb{N}$ es tal que

$$g(n) = \begin{cases} \frac{n}{2} \text{ si n es par} \\ n \text{ si n es impar} \end{cases}$$

   resulta $g \circ f(n) = n$ para cada $n \in \mathbb{N}$, es decir, $g \circ f = Id$. Es claro que $f \circ g \neq Id$, y por lo tanto g es un inverso a izquierda de f. En realidad f admite infinitos inversos a izquierda, ya que podríamos haber definido g de cualquier manera sobre los impares y aún así seguiremos teniendo $g \circ f = Id$.

   Observemos que f no admite ningún inverso a derecha. En efecto, si $h : \mathbb{N} \to \mathbb{N}$ fuese un inverso a derecha de f, tendríamos que para cada $n \in \mathbb{N}$,

$$n = Id(n) = f \circ h(n) = 2h(n)$$

   pero esto implicaría que todo número natural es múltiplo de 2, lo cual es falso.

6. Muchas veces para construir ejemplos o contraejemplos de conjuntos con alguna operación que pretendemos que satisfaga o no una cierta propiedad es útil considerar conjuntos finitos y una operación que esté dada por una tabla. Consideremos un conjunto de tres elementos $X = \{a, b, c\}$ con una operación $*$ definida por:

$*$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

   .

   Es inmediato de la tabla que a es el elemento neutro de $*$. Sin embargo, tenemos que

$$b * b = a,\ b * c = c * b = a$$

   con lo cual b admite dos inversos distintos para $*$. Lo mismo ocurre con c. Como la tabla es simétrica respecto de la diagonal, la operación $*$ es conmutativa. Sin embargo no es asociativa, como se observa haciendo

$$b * (b * c) = b * a = b, \quad (b * b) * c = a * c = c.$$

Podemos de la misma manera construir una operación con más de un elemento neutro a derecha (a y b lo son para $\odot$) o más de un elemento neutro a izquierda (a y b lo son para $\diamond$):

$$\begin{array}{c|ccc} \odot & a & b & c \\ \hline a & a & a & c \\ b & b & b & a \\ c & c & c & a \end{array}, \qquad \begin{array}{c|ccc} \diamond & a & b & c \\ \hline a & a & b & c \\ b & a & b & c \\ c & c & a & a \end{array}.$$

7. **Producto de operaciones.** Sean $*_X$ una operación en un conjunto X y $*_Y$ una operación en un conjunto Y. Podemos definir una operación producto $*$ en $X \times Y$ poniendo

$$(x, y) * (x', y') = (x *_X x', y *_Y y')$$

Si $*_X$ y $*_Y$ son asociativas, entonces $*$ es asociativa. En efecto,

$$\begin{aligned} ((x, y) * (x', y')) * (x'', y'') &= (x *_X x', y *_Y y') * (x'', y'') = ((x *_X x') *_X x'', (y *_Y y') *_Y y'') \\ &= (x *_X (x' *_X x''), y *_Y (y' *_Y y'')) = (x, y) * (x' *_X x'', y' *_Y y'') \\ &= (x, y) * ((x', y') * (x'', y'')). \end{aligned}$$

De manera similar se prueban las siguientes propiedades:

a) si e_X es un elemento neutro (a derecha, izquierda o bilátero) en X y e_Y es un elemento neutro del mismo tipo al de e_X en Y, entonces (e_X, e_Y) es un neutro en $X \times Y$ (a derecha, izquierda o bilátero resp.).

b) si $x \in X$ e $y \in Y$ admiten un elemento inverso x^*, y^* respectivamente (a derecha, izquierda o bilátero), entonces (x^*, y^*) es un inverso (a derecha, izquierda o bilátero resp.) de (x, y) en $X \times Y$.

c) si $*_X$ y $*_Y$ son conmutativas, entonces $*$ es conmutativa.

En los ejemplos anteriores vimos que una operación puede tener más de un neutro a izquierda o derecha, pero no consideramos ningún ejemplo de una operación con más de un neutro. Como veremos, esto no es posible:

Lema **1.** *Sea $*$ una operación en un conjunto X. Si $*$ admite un elemento neutro, éste es único*

Demostración. Supongamos que e y e' son elementos neutros para una operación $*$. Entonces tendremos por un lado que $*(e, e') = e'$, pues e es elemento neutro, pero al mismo tiempo $*(e, e') = e$, pues también e' es neutro. Como $*$ es una función, y por ende cada elemento puede tener una única imagen, concluimos que $e = e'$. □

Como vimos en el último ejemplo, incluso si una operación admite un neutro (único) un elemento puede admitir más de un elemento inverso. Esto sin embargo no puede ocurrir si la operación es asociativa:

Lema **2.** *Sea $*$ una operación en un conjunto X que es asociativa y admite un elemento neutro. Si un elemento admite un inverso, entonces el inverso es único.*

Demostración. Sea $*$ una operación asociativa en X que admite un neutro $e \in X$. Supongamos que existe $x \in X$ que admite dos inversos. Es decir, existen x^*, $x^{**} \in X$ tales que

$$x * x^* = x^* * x = e, \quad x * x^{**} = x^{**} * x = e.$$

Tendremos entonces

$$x^{**} = x^{**} * e = x^{**} * (x * x^*) = (x^{**} * x) * x^* = e * x^* = x^*.$$

□

Notación 3. *Si $*$ es una operación en X con elemento neutro y un elemento $x \in X$ admite un único elemento inverso (por ejemplo si $*$ es asociativa), éste de denota por x^{-1}.*

Observación **1.** *Es importante notar que la asociatividad de la operación no garantiza, aún existiendo elemento neutro, que cada elemento tenga un inverso (aunque sabemos que en caso de existir, éste será único). Si consideramos el producto en $\mathbb{Z}$, por ejemplo, existe un elemento neutro que es 1 y aún así casi ningún elemento admite un inverso (únicamente 1 y -1).*

Por otra parte, incluso si la operación es asociativa y admite un elemento neutro, un elemento puede tener más de un inverso a derecha o izquierda (ver item 5 de los Ejemplos 5). En este caso, estos inversos laterales no podrán ser inversos (biláteros).

Lema **4.** *Sea X un conjunto con una operación binaria $*$ que admite un elemento neutro. Entonces:*

1. *Si x^* es un inverso a derecha (resp. a izquierda) de $x \in X$, entonces x es un inverso a izquierda (resp. a derecha) de x^*.*
2. *Si x admite un inverso x^{-1}, entonces x es también el inverso de x^{-1}, esto es, $(x^{-1})^{-1} = x$.*
3. *Si $*$ es asociativa y x e y admiten inversos, entonces $x * y$ admite un inverso y $(x * y)^{-1} = y^{-1} * x^{-1}$*

Demostración. Las dos primeras propiedades son inmediatas de la definición de inverso. Probemos la última. Supongamso que $*$ es asociativa y x e y admiten inversos. Entonces

$$(x * y) * (y^{-1} * x^{-1}) = ((x * y) * y^{-1}) * x^{-1} = (x * (y * y^{-1})) * x^{-1} = (x * e) * x^{-1} = x * x^{-1} = e.$$

La prueba de que $(y^{-1} * x^{-1}) * (x * y) = e$ es análoga. □

Definición: Sea X un conjunto con una operación $*$ y sea $Y \subset X$. Decimos que $*$ es **cerrada** en Y (o que Y es un **subconjunto cerrado** para $*$) si para cada $x, y \in Y$, $*(x, y) \in Y$. Decimos que $*$ es en Y la **operación inducida** desde X, o **heredada** de X.

Ejemplos **2.** 1. Si restringimos la composición de funciones en el conjunto $\mathcal{F}(A)$ al conjunto $\mathcal{B}(A)$ de las funciones biyectivas, obtendremos una operación asociativa, con elemento neutro, y donde todo elemento admite un inverso.

2. Lo mismo ocurre si retringimos el producto de matrices en $\mathcal{M}_{n\times n}$ al conjunto $GL(n,\mathbb{R})$ de matrices no singulares (con determinante distinto de 0). Nuvamente, la operación es asociativa, admite neutro y todo elemento tiene un inverso.

3. El elemento neutro no tiene por qué preservarse cuando restringimos una operación a un subconjunto. Por ejemplo, si restringimos la suma en $\mathbb{Z}$ al conjunto de los números naturales, vemos que la operación sigue siendo asociativa y conmutativa pero no admite neutro (pues $0 \notin \mathbb{N}$).

Las propiedades de una operación $*$ en un conjunto X que se mantienen en un subconjunto cerrado Y para $*$ se denominan **hereditarias**:

Lema **5.** *Sea $*$ una operación en un conjunto X y sea $Y \subset X$ un subconjunto cerrado para $*$. Entonces:*

1. *Si $*$ es asociativa en X, entonces $*$ es asociativa en Y (la asociatividad es una propiedad hereditaria).*
2. *Si $*$ es conmutativa en X, entonces $*$ es conmutativa en Y (la conmutatividad es una propiedad hereditaria).*
3. *Si e es un neutro en X y $e \in Y$, entonces e es un neutro en Y.*
4. *Si Y hereda el neutro de X y $x \in Y$ admite un inverso x^* en X tal que $x^* \in Y$, entonces x^* es un inverso de x para la operación restringida a Y.*

Ejercicio **1.** *Probar el Lema 5.*

2. Operaciones en conjuntos cocientes - Los enteros módulo m

Supongamos que X es un conjunto con una operación $*$ y consideramos una relación de equivalencia $\sim$ en X. Podemos construir el conjunto cociente $X/\sim$. Nos interesa determinar cuándo es posible inducir la operación en X a $X/\sim$:

Definición **2.** *Sea X es un conjunto con una operación $*$ y $\sim$ una relación de equivalencia en X. Decimos que $*$ **se induce al cociente** $X/\sim$ si se verifica que:*

$$\left.\begin{array}{l} x \sim x' \\ y \sim y' \end{array}\right\} \implies x * y \sim x' * y'.$$

Si $*$ se induce al cociente $X/\sim$ queda bien definida una operación en $X/\sim$, que seguiremos denotando por $*$, definida por $* : X/\sim \times X/\sim \to X/\sim$,

$$[x] * [y] := [x * y].$$

Ejemplo **3. Operaciones en $\mathbb{Z}_m$.** Recordemos que $\mathbb{Z}_m$ es el cociente de $\mathbb{Z}$ por la relación de equivalencia

$$x \sim y \;\Leftrightarrow\; x \equiv y\,(m) \;\Leftrightarrow\; x - y = km, \text{ p.a. } k \in \mathbb{Z}.$$

Probaremos que las operaciones de $\mathbb{Z}$ se inducen al cociente. Esto es, si x, x', y, $y' \in \mathbb{Z}$ son tales que $x \equiv x'\,(m)$ y $y \equiv y'\,(m)$. Entonces:

1. $x + y \equiv x' + y'\,(m)$.
2. $xy \equiv x'y'\,(m)$.

Como $x \equiv x'\,(m)$, existe $k \in \mathbb{Z}$ tal que $x - x' = km$. De la misma manera, existirá $k' \in \mathbb{Z}$ tal que $y - y' = k'm$. Luego

$$(x + y) - (x' + y') = (x - x') + (y - y') = (k + k')m,$$

con lo cual $x + y \equiv x' + y'\,(m)$.

Por otra parte,

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') = (yk + x'k')m$$

con lo cual $xy \equiv x'y'\,(m)$.

Esto quiere decir que en $\mathbb{Z}_m$ están bien definidas una operación suma y una operación producto dadas por

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

Observemos algunos ejemplos concretos. Supongamos que en $\mathbb{Z}_5$ queremos hacer $\overline{2} + \overline{4} = \overline{6} = \overline{1}$. Lo que acabamos de probar nos dice que la suma de cualquier representante de $\overline{2}$ con cualquier representante de $\overline{4}$ nos dará siempre un representante de $\overline{1}$. Podemos tomar trivialmente $2 \in \overline{2}$ y $4 \in \overline{4}$ y tendremos que $2 + 4 = 6 \in \overline{1}$. Pero también podríamos haber tomado $7 \in \overline{2}$ y $24 \in \overline{4}$, y tendremos $7 + 24 = 31 \in \overline{1}$. Pueden corroborar la buena definición del producto con los mismos ejemplos.

Teorema **6.** *Sea $*$ una operación en un conjunto X y sea $\sim$ una relación de equivalencia en X tal que $*$ se induce al cociente $X/\sim$. Entonces:*

1. *Si $*$ es asociativa en X, la operación inducida a $X/\sim$ es asociativa.*
2. *Si $*$ es conmutativa en X, la operación inducida a $X/\sim$ es conmutativa.*
3. *Si e es un elemento neutro (a derecha, izquierda o bilátero) para $*$ en X, entonces $[e]$ es un neutro con las mismas características para la operación inducida en $X/\sim$.*
4. *Si $x \in X$ posee un inverso (a izquierda, derecha o bilátero) x^*, entonces $[x^*]$ es un inverso (con las mismas características de x^*) para la operación inducida en $X/\sim$.*

Demostración. 1. Sean $[x], [y], [z] \in Z/\sim$. Entonces

$$([x] * [y]) * [z] = [x * y] * [z] = [(x * y) * z] = [x * (y * z)] = [x] * [y * z] = [x] * ([y] * [z]).$$

2. Es análoga a la del item anterior y la dejamos como ejercicio.

3. Supongamos que e es un neutro a derecha de $*$ (los otros casos son análogos y los dejamos como ejercicio). Entonces para cada $x \in X$, $x * e = x$. Sea $[x] \in X/\sim$ cualquiera. Entonces

$$[x] * [e] = [x * e] = [x]$$

con lo cual $[e]$ es un neutro a derecha en $X/\sim$.

4. Sigue el mismo razonamiento que el item anterior y la dejamos como ejercicio.

□

Ejemplo **4. Operaciones en $\mathbb{Z}_m$ (cont.)** Observemos que la suma en $\mathbb{Z}$ admite un elemento neutro, el 0, con lo cual $\overline{0}$ será un neutro en $\mathbb{Z}_m$. Esto es,

$$\overline{k} + \overline{0} = \overline{k}$$

para cada $\overline{k} \in Z_m$.

Además, $\overline{-k}$ será el inverso de $\overline{k}$, o sea,

$$\overline{k} + \overline{-k} = \overline{-k} + \overline{k} = \overline{0}$$

para cada $\overline{k} \in \mathbb{Z}_m$. Denotamos por $-\overline{k} = \overline{-k}$ Esto permite definir una nueva operación en $\mathbb{Z}_m$, la resta, dada por

$$\overline{k} - \overline{n} = \overline{k} + \overline{-n} = \overline{k-n}.$$

Dejamos como ejercicio verificar qué propiedades tiene esta nueva operación (que no es más que la operación que la resta en $\mathbb{Z}$ induce en $\mathbb{Z}_m$).

Observemos que cada elemento $\overline{k} \in \mathbb{Z}_m$ tiene un representante $k_0 \in \{0, 1, \ldots, m-1\}$. Claramente, incluso si k está en este conjunto, $-k$ no pertenece a él. Pero es fácil verificar que

$$-\overline{k} = \overline{m-k}.$$

En efecto,

$$(m-k) - (-k) = m \implies -k \equiv m - k\,(m).$$

Así, en $\mathbb{Z}_5$ por ejemplo, $-\overline{1} = \overline{-1} = \overline{4}$, $-\overline{2} = \overline{-2} = \overline{3}$, etc.

Analicemos ahora el producto. 1 es el elemento neutro del producto en $\mathbb{Z}$, y por lo tanto $\overline{1}$ será el elemento neutro del producto en $\mathbb{Z}_m$. En $\mathbb{Z}$ ningún elemento salvo 1 y -1 admite un inverso. Pero esto NO implica que los elementos de $\mathbb{Z}_m$ no admitan inverso. Consideremos nuevamente el caso de $\mathbb{Z}_5$. Tenemos:

$$\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{2} = \overline{6} = \overline{1}, \quad \overline{4} \cdot \overline{4} = \overline{16} = \overline{1}.$$

Luego $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$. Es decir, en $\mathbb{Z}_5$ todos los elementos distintos de $\overline{0}$ tienen un inverso multiplicativo.

Si consideramos $\overline{Z_4}$, la tabla de multiplicar es la siguiente:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Por lo tanto en $\mathbb{Z}_4$, los únicos elementos invertibles son $\overline{1}$ y $\overline{3}$

En términos generales, tenemos:

Teorema **7.** *Sea $\overline{k} \in \mathbb{Z}_m$. $\overline{k}$ admite un inverso multiplicativo si y sólo si $mcd(k, m) = 1$ (es decir, k y m son primos relativos).*

Demostración. Recordemos que dos enteros k y m son primos relativos si y sólo si existen $a, b \in \mathbb{Z}$ tales que $ak + bm = 1$.

Observemos que $\overline{k}$ admite un inverso multiplicativo si y sólo si existe $k' \in \mathbb{Z}$ tal que $\overline{k \cdot k'} = 1$, es decir, $kk' \equiv 1\,(m)$. Esto último es equivalente a que exista $x \in \mathbb{Z}$ tal que $1 = kk' + mx$. Es decir, $\overline{k}$ admite un inverso multiplicativo si y sólo si existe una combinación lineal entera de k y m cuyo resultado es 1. □

Corolario **8.** *Si $p \in \mathbb{Z}$ es primo, todo elemento distinto de $\overline{0}$ en $\mathbb{Z}_p$ admite un inverso multiplicativo.*

3. Semigrupos, monoides y grupos.

Como es evidente la existencia y unicidad de elemento neutro y elementos inversos son propiedades fundamentales de una operación. La propiedad asociativa es aquella que asegura que el inverso, en caso de existir sea único, además de tener consecuencias importantes en la aritmética de la operación. Por lo tanto es interesante en sí mismo estudiar de manera abstracta un conjunto con una operación que reúna alguna de estas propiedades, comenzando por la asociatividad.

Definición **3.** *Sea X un conjunto con una operación $\cdot : X \times X \to X$.*

1. *Si $*$ es asociativa, $(X, *)$ se denomina un **semigrupo**.*
2. *Si $(X, *)$ es un semigrupo que admite un elemento neutro, $(X, *)$ se denomina un **monoide**.*
3. *Si $(x, *)$ es un monoide donde todo elemento tiene un elemento inverso, $(X, *)$ se denomina un **grupo**.*
4. *Si $*$ es conmutativa, cualquiera de las estructuras anteriores se dice **conmutativa**. Si $(X, *)$ es un grupo conmutativo, se denomina un **grupo abeliano**.*

Notación 9. *Normalmente denotamos por $(G, \cdot)$ a un grupo con su operación. Cuando la operación es clara por el contexto generalmente se omite. Más aún, es usual denotar $g_1 \cdot g_2$ como $g_1 g_2$ (es decir, yuxtaponiendo los elementos). Es importante observar a esta altura que si bien la operación de manera abstracta se denota por $\cdot$, esta no necesariamente representa lo que comúnmente entendemos por un producto y es posible (y frecuente) utilizar notaciones distintas en los distintos ejemplos.*

Ejemplos **5.**

1. $(\mathbb{N}, +)$ es un semigrupo conmutativo y $(\mathbb{N}, \cdot)$ es un monoide conmutativo. $(\mathbb{N}_0, +)$ es un monoide conmutativo.

2. $(\mathbb{Z}, \cdot)$ es un monoide conmutativo, pero no es un grupo. $(\mathbb{Z}, +)$ es un grupo abeliano, cuyo elemento neutro es el 0 y el inverso de un elemento $k \in \mathbb{Z}$ es su opuesto $-k$.

3. $(\mathbb{Q}, +)$ y $(\mathbb{Q}^*, \cdot)$ son grupos abelianos, donde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. De la misma manera, $(\mathbb{R}, +)$ y $(\mathbb{R}^*, \cdot)$ son grupos abelianos.

4. $(\mathcal{M}_n, \cdot)$, donde $\cdot$ es el producto usual de matrices es un monoide no conmutativo, pero no es un grupo. La operación se induce a Gl_n, el conjunto de matrices inversibles, y $(Gl_n, \cdot)$ es un grupo no abeliano.

5. $(\mathbb{Z}_m, +)$ es un grupo abeliano para cualquier $m \in \mathbb{Z}$. $(\mathbb{Z}_m^*, \cdot)$ es un grupo si y sólo si m es un número primo, donde $\mathbb{Z}_m^* = \mathbb{Z}_m - \{\overline{0}\}$. En ese caso, $(\mathbb{Z}_p^*, \cdot)$ es un grupo abeliano. Este es un ejemplo importante de un grupo finito.

6. $\mathcal{F}(X)$ (el conjunto de funciones de X en X) con la composición de funciones $\circ$ es un monoide no conmutativo. Si nos restringimos a $\mathcal{B}(X)$, el conjunto de funciones biyectivas, entonces $(\mathcal{B}(X), \circ)$ es un grupo no abeliano.

7. El ejemplo anterior admite un caso de particular interes cuando X es un conjunto finito. Supongamos que $X = \{x_1, \cdots, x_n\}$, entonces es fácil ver que $\mathcal{B}(X)$ tiene $n!$ elementos. En efecto, cualquier biyección de X en sí mismo se identifica con una permutación de los elementos de X. Comunmente se denota por S_n al grupo $\mathcal{B}(\{1, \cdots, n\})$ y se llama **grupo simétrico de orden** n.

   Si tomaramos por ejemplo $X = \{1, 2, 3, 4\}$ podremos representar cada función biyectiva $f : X \to X$ a través de dos filas: en la superior listamos todos los elementos de X, y en la inferior colocamos la imagen de cada uno de ellos por f. Así, si escribimos

   $$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

   tendremos que $f(1) = 1$, $f(2) = 3$, $f(3) = 2$ y $f(4) = 4$. O sea, f es la permutación que intercambia 2 y 3 y deja 1 y 4 fijos. Esta forma de representar las funciones biyectivas en un conjunto finito permite describir fácilmente la composición de dos funciones. Consideremos ahora

   $$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Entonces:

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Este ejemplo sencillo muestra que S_n es no abeliano.

8. Para cada $\theta \in \mathbb{R}$, sea $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ una rotación en ángulo θ alrededor del origen de coordenadas. Denotemos por $\mathcal{R} = \{R_\theta : \theta \in \mathbb{R}\}$. Como $R_\theta \circ R_\rho = R_{\theta+\rho}$, la composición de funciones es cerrada en $\mathcal{R}$. Más aún, $R_0 = Id$ y $R_\theta \circ R_{-\theta} = R_{-\theta} \circ R_\theta = Id$. Por lo tanto $(\mathcal{R}, \circ)$ es un grupo. A diferencia de lo que ocurre con $(\mathcal{B}(\mathbb{R}^2), \circ)$, es fácil ver que $(\mathcal{R}, \circ)$ es un grupo abeliano.

   Observemos que la descripción $\theta \leftrightarrow R_\theta$ no es biunívoca: para cada θ y cada $k \in \mathbb{Z}$, $R_\theta = R_{\theta+2k\pi}$.

   Fijemos ahora $n \in \mathbb{N}$ y pongamos $R_n = R_{\frac{2\pi}{n}}$. Para cada $k \in \mathbb{N}_0$ consideremos la $k-$ésima potencia de R_n, es decir, la composición de R_n consigo misma k veces. Así:

$$R_n^0 = Id, \quad R_n^1 = R_n, \quad R_n^2 = R_{\frac{4\pi}{n}}, \ \ldots \ , R_n^{n-1} = R_{\frac{2(n-1)\pi}{n}}, \ R_n^n = R_{\frac{2n\pi}{n}} = R_{2\pi} = Id$$

   y a partir de aquí las potencias se repiten. Pongamos $\mathcal{R}_n = \{R_n^k : 0 \leq k \leq n-1\}$. Entonces la composición es cerrada en $\mathcal{R}_n$, $Id \in \mathcal{R}_n$ y para cada $1 \leq k \leq n-1$, $R_n^k \circ R_n^{n-k} = Id$, o sea, cada elemento admite un inverso. Concluimos que $\mathcal{R}_n$ es un grupo de n elementos.

9. **Estructuras producto.** Sean $(X, *_X)$ e $(Y, *_Y)$ dos conjuntos con operaciones binarias y consideremos el conjunto $(X \times Y, *)$ con la operación producto definida en el item 7 de los Ejemplos 1. Entoces es inmediato a partir de las propiedades de la operación producto que:

   a) si X e Y son semigrupos, entonces $X \times Y$ es un semigrupo.

   b) si X e Y son monoides, entonces $X \times Y$ es un monoide.

   c) si X e Y son grupos, entonces $X \times Y$ es un grupo.

10. **Estructuras cociente.** Si $(X, *)$ es un conjunto con una operación binaria y $\sim$ es una relación de equivalencia X tal que $*$ se induce al cociente $X \sim$, entonces del Teorema 6 resulta que:

    a) si X es un semigrupo, $X/\sim$ es un semigrupo.

    b) si X es un monoide, $X/\sim$ es un monoide.

    c) si X es un grupo, entonces $X/\sim$ es un grupo.

Teorema **10** (Ley de cancelación)**.** *Sea $(X, *)$ un monoide y sean $a, b, c \in X$ tal que a admite un inverso a^{-1}. Entonces*

$$a * b = a * c \implies b = c$$

$$b * a = c * a \implies b = c.$$

Ejercicio **2.** *Demostrar el Teorema 10.*

4. Subestructuras

Nos proponemos ahora definir las **subestructuras** correspondientes a las estructuras algebraicas que hemos definido en el la Definición 3.

Observemos primero que si $(X, *)$ es un semigrupo, entonces si $Y \subset X$ es cerrado para $*$, resulta $(Y, *)$ un semigrupo, dado que la asociatividad se hereda a cualquier subconjunto cerrado.

Si $(X, *)$ es un monoide, no basta con que Y sea cerrado para $*$ para que $(Y, *)$ sea un monoide. En efecto, si tomamos en $\mathbb{Z}$ es conjunto Y de los múltiplos de 2, vemos que Y es un subconjunto cerrado para el producto, pero sin embargo Y no tiene identidad y por lo tanto no es un monoide.

Resulta claro que si Y es cerrado para $*$ y $e \in Y$, $(Y, *)$ es un monoide. ¿Puede ocurrir que un subconjunto Y cerrado para $*$ sea tal que $(Y, *_Y)$ es un monoide pero la identidad en Y es distinta de la identidad en X? La respuesta en este caso también es afirmativa, y un contraejemplo trivial proviene de considerar $Y = \{0\} \subset \mathbb{Z}$. Y es cerrado para el producto y la identidad en Y es trivialmente 0, pero éste no es la identidad en $\mathbb{Z}$ (este ejemplo puede generalizarse a cualquier monoide con un elemento absorvente).

Al igual que como ocurría para los retículos (donde un subconjunto podía ser un retículo sin que la estructura algebraica fuese la heredada del retículo original), cuando queremos definir una subestructura pretendemos que ésta preserve los elementos característicos de la estructura original. Por lo tanto tendremos:

Definición **4.** *Sea $(X, *)$ un conjunto con una operación e $Y \subset X$ un subconjunto cerrado para $*$.*

1. *Si $(X, *)$ es un semigrupo, diremos que $(Y, *)$ es un **subsemigrupo** de Y.*
2. *Si $(X, *)$ es un monoide, diremos que $(Y, *)$ es un **submonoide** de Y si la identidad e de Y pertenece a X.*
3. *Si $(X, *)$ es un grupo con identidad e, diremos que $(Y, *)$ es un **subgrupo** de X si $e \in Y$ y $x^{-1} \in Y$ para cada $x \in Y$ (donde x^{-1} es el inverso de x en X).*

Observemos que todo submonoide de un monoide es un monoide en sí mismo, pero hemos visto que un subconjunto de un monoide puede ser un monoide sin ser un submonoide.

Análogamente, cualquier subgrupo de un grupo es un grupo en sí mismo, pero a diferencia de lo que ocurre con los monoides, cualquier subconjunto cerrado de un grupo que sea a su vez un grupo (con la operación inducida) debe ser un subgrupo. Esto es, si un subconjunto de un grupo es a su vez un grupo, es porque hereda del grupo la identidad y los inversos de todos sus elementos. Más precisamente tenemos:

Teorema **11.** *Sea G un grupo y sea $H \subset G$ un subconjunto cerrado. Si H con la operación heredada es un grupo entonces H es un subgrupo de G.*

Demostración. Supongamos que $H \subset G$ es un subconjunto cerrado de $(G, \cdot)$ tal que $(H, \cdot)$ es un grupo. Supongamos que el elemento neutro de $(G, \cdot)$ es e y el elemento neutro de $(H, \cdot)$ es e'. Entonces para cualquier $a \in H$, tendremos $a \cdot e' = a$. Multiplicando ambos lados a izquierda por a^{-1} vemos que $e' = e$. Es decir que $e \in H$.

A partir de aquí, es inmediato que el inverso de a en $(H, \cdot)$ debe ser a^{-1}, pues de otra manera existiría un elemento $a^* \in H$ tal que $a \cdot a^* = a^* \cdot a = e$. Pero como $H \subset G$, a^* sería un inverso de a también en G, con lo cual $a^* = a^{-1}$.

Concluimos que $e \in H$ y $a^{-1} \in H$ para cada $a \in H$, y por lo tanto H es un subgrupo de G. □

Es posible caracterizar los subgrupos de un grupo a partir de una única condición:

Teorema **12.** *Sea G un grupo y H un subconjunto de G. Entonces H es un subgrupo de G si y sólo si para todo $a, b \in H$ se verifica $ab^{-1} \in H$.*

Demostración. Si H es un subgrupo es inmediato que $ab^{-1} \in H$ para cada $a, b \in H$.

Supongamos entonces que H es un subconjunto de G que verifica que $ab^{-1} \in H$ cada vez que $a, b \in H$. Tomando $a \in H$ cualquiera y aplicando la propiedad anterior al par a, a tenemos que $e = a \cdot a^{-1} \in H$. Aplicandola ahora al par e, a resulta que $a^{-1} = e \cdot a^{-1} \in H$. Finalmente, tomemos $a, b \in H$ y apliquemos la propiedad al par $a, b^{-1} \in H$. Temos

$$a \cdot (b^{-1})^{-1} \in H \;\Rightarrow\; a \cdot b \in H,$$

con lo cual la operación es cerrada en Hn y por lo tanto H es un subgrupo de G □

Ejemplos **6.**

1. Si $(X, *)$ es una de las tres estructuras que estamos estudiando, claramente $Y = X$ y $Y = \{e\}$ son subestructuras de X. Cualquier otra subestructura distinta de ellos se denomina un **subsemigrupo, submoniode o sugrupo propio de** X, según corresponda.

2. Si $(L, \preceq)$ es un retículo y L' es un subretículo, entonces $(L', \vee)$ y $(L', \wedge)$ son subsemigrupos de $(L, \vee)$ y $(L, \wedge)$ respectivamente. Si L es un retículo acotado, entonces L con cualquiera de las dos operaciones es un monoide. Sin embargo L' no necesariamente es un submonoide de L (con las operaciones correspondientes) pues L' no tiene por qué heredar la identidad de L. (ejercicio: dar un ejemplo).

3. El grupo $\mathcal{B}(X)$ de biyecciones de un conjunto X es un submonoide del monoide $\mathcal{F}(X)$ de funciones de X en X.

4. Si $(L, \preceq)$ es un retículo, el conjunto G de isomorfismos de L en sí mismo con la composición de funciones es un subgrupo de $(\mathcal{B}(L), \circ)$. En efecto, si $f, g : X \to X$ son isomorfismos de retículo, entonces $f \circ g^{-1}$ es un isomorfismo de retículos, es decir, $f \circ g^{-1} \in G$ para cada $f, g \in G$.

5. Fijemos $m \in \mathbb{Z}$ y sea $H = (\dot{m})$ el conjunto de múltiplos de m. Sean $z, w \in H$. Entonces existen $k_1, k_2 \in \mathbb{Z}$ tales que $z = k_1 m$, $w = k_2 m$. Luego

   $$z + (-w) = k_1 m - k_2 m = (k_1 - k_2)m \in H$$

   con lo cual H es un subgrupo de $(\mathbb{Z}, +)$.

6. Consideremos el subconjunto $H = \{\overline{0}, \overline{2}, \overline{4}\}$ del grupo $(\mathbb{Z}_6, +)$. Tenemos que el inverso de $\overline{2}$ es $\overline{4}$ y por lo tanto el inverso de $\overline{4}$ es $\overline{2}$. Además

$$\overline{0} + \overline{2} = \overline{2},\ \overline{0} + \overline{4} = \overline{4},\ \overline{2} + \overline{2} = \overline{4},\ \overline{2} + \overline{4} = \overline{0},\ \overline{4} + \overline{4} = \overline{2}$$

es decir, $\overline{a} + \overline{-b} \in H$ para cualquier $\overline{a}, \overline{b} \in H$, y por lo tanto H es un subgrupo propio de $\mathbb{Z}_6$. Si ahora tomamos $K = \{\overline{0}, \overline{1}, \overline{3}, \overline{5}\}$, vemos que $\overline{1} + \overline{3} = \overline{4} \notin K$, con lo cual K no es un subgrupo de $\mathbb{Z}_6$, puesto que la operación ni siquiera es cerrada en K.

5. Morfismos

Sean $(X, *)$, $(Y, \odot)$ con juntos con operaciones binarias. Un **morfismo** de $(X, *)$ en $(Y, *)$ es una función $f : X \to Y$ tal que

$$f(x * y) = f(x) \odot f(y). \tag{2}$$

Como es esperable, no siempre un morfismo entre dos conjuntos con operaciones binarias preserva las demás características que puede tener ese conjunto. Es por eso que para definir un morfismo entre las distintas estructuras algebraicas debemos pensar en qué propiedades extra tendremos que pedirle a la función f.

Definición **5.** *Sean $(X, *)$ e $(Y, \odot)$ dos semigrupos. Una función $f : X \to Y$ que verifique (2) se denomina un **morfismo** u **homomorfismo de semigrupos.***

- *Si $(X, *)$ e $(Y, \odot)$ son monoides, un **homomorfismo de monoides** es un homomorfismo de semigrupos tal que $f(e_X) = e_Y$, donde e_X es la identidad en X y e_Y es la identidad en Y.*
- *Si $(X, *)$ e $(Y, \odot)$ son grupos, un **homomorfismo de grupos** es un homomorfismo de monoides tal que $f(x^{-1}) = f(x)^{-1}$ para cada $x \in X$.*

*Un **isomorfismo** (de semigrupos, monoides o grupos) es un homomorfismo biyectivo (de semigrupos, monoides o grupos resp.) tal que f^{-1} es un homomorfismo (de semigrupos, monoides o grupos resp.)*

Ejemplos **7.** 1. Sea $f : \mathbb{Z} \to \mathbb{Z}$ dado por $f(x) = kx$, con $k \in \mathbb{Z}$ fijo. Entonces

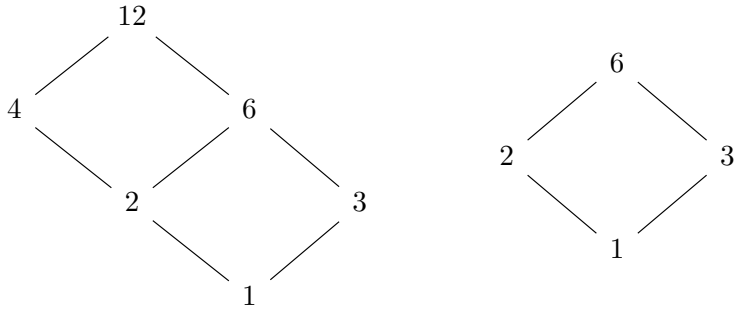
$$f(x + y) = k(x + y) = kx + ky = f(x) + f(y).$$

Luego $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ es un homomorfismo de semigrupos, y como $f(0) = 0$, f es un homomorfismo de monoides. Además $f(-x) = -kx = -f(x)$, con lo cual f es un homomorfismo de grupos.

2. Sean $(L, \preceq) = (L, \vee, \wedge)$ y $(L', \preceq') = (L', \vee', \wedge')$ dos retículos. Entonces $f : L \to L'$ es un morfismo de retículos si $f : (L, \vee) \to (L', \vee)$ y $f : (L, \wedge) \to (L', \wedge)$ son homomorfismos de semigrupos.

   Si L y L' son ambos acotados, entonces son monoides con cada una de sus operaciones join y meet respectivas. Pero no es cierto que un morfismo de retículos de lugar a homomorfismos entre los monoides respectivos, pues un morfismo de retículos no necesariamente envía el máximo y el mínimo de L en el máximo y el mínimo de L'.

Consideremos por ejemplo $f : (D_{12}, |) \to (D_6, |)$ tal que $f(1) = 1$, $f(2) = 2$, $f(3) = 3$, $f(6) = 6$, $f(4) = 2$, $f(12) = 6$:



Si $x, y \in \{1, 2, 3, 6\}$ es claro que $f(x \vee y) = f(x) \vee f(y)$ y $f(x \wedge y) = f(x) \wedge f(y)$. Si $x = 12$, $y \in D_{12}$, entonces

$$f(12 \vee y) = f(12) = 6 = f(12) \vee f(y), \quad f(12 \wedge y) = f(y) = 6 \wedge f(y) = f(12) \wedge f(y).$$

De la conmutatividad de $\vee$ y $\wedge$ obtenemos resultados análogos si $y = 12$ y $x \in D_{12}$ es cualquier elemento.

Finalmente, si $x = 4$, entonces

$$f(4 \vee 1) = f(4) = f(4) \vee f(1), \ \ f(4 \vee 2) = f(4) = 2 = 2 \vee 2 = f(4) \vee f(2), \ \ f(4 \vee 3) = f(12) = 6 = 2 \vee 3 = f(4) \vee f(3),$$

$$f(4 \vee 4) = f(4) = f(4) \vee f(4), \ \ f(4 \vee 6) = f(12) = 6 = 2 \vee 6 = f(4) \vee f(6), \ \ f(4 \vee 12) = f(12) = 6 = 2 \vee 6 = f(4) \vee f(1$$

De manera análoga se comprueba que $f(4 \wedge y) = f(4) \wedge f(y)$.

Concluimos que f es un morfismo de retículos. Además como $f(1) = 1$ y 1 es el elemento neutro de $\vee$, resulta que $f(D_{12}, \vee) \to (D_6, \vee)$ es un homomorfismo de monoides. El elemento neutro de $(D_{12}, \wedge)$ es 12 y el elemento neutro de $(D_6, \wedge)$ es 6. Como $f(12) = 6$, $f : (D_{12}, \wedge) \to (D_6, \wedge)$ también es un homomorfismo de monoides.

Si ahora consideramos la misma función f pero pensada como $f : D_{12} \to D_{12}$, vemos que $f : (D_{12}, \vee) \to (D_{12}, \vee)$ sigue siendo un homomorfismo de monoides pero $f : (D_{12}, \wedge) \to (D_{12}, \wedge)$ no lo es, dado que $f(12) = 6 \neq 12$.

Si tenemos ahora un isomorfismo de retículos $g : (L, \preceq) \to (L', \preceq')$, entonces g será un isomorfismo de semigrupos para cualquiera de las operaciones join y meet en ambos conjuntos. Si L y L' son acotados, como un isomorfismo de retículos es en particular un isomorfismo de orden y éste envía mínimo en mínimo y máximo en máximo, entonces $g : (L, \vee) \to (L', \vee')$ y $g : (L, \wedge) \to (L', \wedge')$ será un isomorfismos de monoides.

En este último ejemplo vemos que la condición de que $f(e_X) = e_Y$ no puede obviarse en la definición de un homomorfismo de monoides. Pero la situación es distinta en el caso de los grupos:

Teorema **13.** *Sean $(G, \cdot)$ y $(H, *)$ dos grupos. Entonces $f : G \to H$ es un homomorfismo de grupos si y sólo si f es un homomorfismo de semigrupos.*

Demostración. Si f es un homomorfismo de grupos es en particular un homomorfismo de semigrupos.

Debemos por lo tanto probar que un homomorfismo de semigrupos entre dos grupos es automáticamente un homomorfismo de grupos. Esto es, debemos ver que $f(e_G) = e_H$ y que $f(x^{-1}) = f(x)^{-1}$ para cada $x \in G$.

Para ver que que f envía el neutro de G en el neutro de H observemos que

$$e_H * f(e_G) = f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$$

Como H es un grupo, $f(e_G)$ admite un inverso $f(e_G)^{-1}$. Luego por el Teorema 10, resulta $e_H = f(e_G)$.

Por otra parte, si $x \in G$, entonces $f(x \cdot x^{-1}) = f(e_G) = e_H$. Luego

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = e_H$$

de donde $f(x^{-1}) = f(x)^{-1}$. □

Ejemplos **8.** 1. Sean $(X, *_X)$ e $(Y, *_Y)$ dos semigrupos y $(X, \times Y, *)$ el semigrupo producto. Sean $p_X : X \times Y \to X$, $p(x, y) = x$ y $p_Y : X \times Y \to Y$, $p_Y(x, y) = y$. Entonces

$$p_X((x, y) * (x', y')) = p_X(x *_X x', y *_Y y') = x *_X x'$$

con lo cual p_X (y análogamente p_Y) es un homomorfismo de semigrupos.

Si X e Y son grupos, en función del Teorema 13 p_X y p_Y son homomorfismos de grupos.

Si X e Y son monoides, como $p_X(e_X, e_Y) = e_X$ y $p_Y(e_X, e_Y) = e_Y$, p_X y p_Y son homomorfismos de monoides.

2. Sea $\sim$ una relación de equivalencia en un semigrupo $(X, *)$ tal que $*$ se induce al semigrupo cociente $X/\sim$. Consideremos la proyección $p : X \to X/\sim$ dada por $p(x) = [x]$. Entonces:

$$p(x * y) = [x * y] = [x] * [y] = p(x) * p(y)$$

con lo cual p es un homomorfismo de semigrupos. En función del Teorema 13, si X es un grupo, entonces p es un homomorfismo de grupos. Como además si $e \in X$ es la identidad de $*$ entonces $[e] \in X/\sim$ es la identidad de la operación inducida y $p(e) = [e]$, resulta que si X es un monoide entonces p es un homomorfismo de monoides.

3. Sea S^1 la circunferencia unitaria en el plano. Observemos que

$$S^1 = \{v \in \mathbb{R}^2 \,:\, \|v\| = 1\} = \{z \in \mathbb{C} \,:\, |z| = 1\}.$$

Pensar a la circunferencia como subconjunto del plano complejo (que geométricamente es equivalente al plano euclídeo $\mathbb{R}^2$) permite analizar como se comporta el producto en $\mathbb{C}$ respecto de S^1.

Si $z, w \in S^1$, entonces $|z \cdot w^{-1}| = \frac{|z|}{|w|} = 1$. Concluimos que S^1 es un subgrupo de $(\mathbb{C}^*, \cdot)$.

Todo elemento $z \in S^1$ admite una representación de la forma $z = \cos(\theta) + i\,\mathrm{sen}(\theta)$, con lo cual la función $f : \mathbb{R} \to S^1$, $f(\theta) = \cos(\theta) + i\,\mathrm{sen}(\theta)$ es una función sobreyectiva.

Por otro lado,

$$f(\theta+\rho) = \cos(\theta+\rho) + i\,\mathrm{sen}(\theta+\rho)$$

Recordemos que $\cos(\theta+\rho) = \cos(\theta)\cos(\rho) - \mathrm{sen}(\theta)\,\mathrm{sen}(\rho)$ y $\mathrm{sen}(\theta+\rho) = \mathrm{sen}(\theta)\cos(\rho) + \cos(\theta)\,\mathrm{sen}(\rho)$. Por otra parte,

$$\begin{aligned} f(\theta)\cdot f(\rho) &= (\cos(\theta) + i\,\mathrm{sen}(\theta))\cdot(\cos(\rho) + i\,\mathrm{sen}(\rho) \\ &= (\cos\theta\cos(\rho) - \mathrm{sen}(\theta)\,\mathrm{sen}\,\rho) + i(\mathrm{sen}(\theta)\cos(\rho) + \cos(\theta)\,\mathrm{sen}(\rho)) = f(\theta+\rho). \end{aligned}$$

Por lo tanto $f : (\mathbb{R}, +) \to (S^1, \cdot)$ es un homomorfismo de grupos.

Finalizaremos esta unidad estudiando algunas propiedades de los isomorfismos.

Teorema **14.** *Todo homomorfismo biyectivo de semigrupos, monoides o grupos es un isomorfismo de semigrupos, monoides o grupos.*

Demostración. Sea $f : (X, *) \to (Y, \odot)$ es un homomorfismo biyectivo. Sean $u, v \in Y$ y $x, y \in X$ tales que $f(x) = u$, $f(y) = v$. Entonces

$$f^{-1}(u \odot v) = f^{-1}(f(x) \odot f(y)) = f^{-1}(f(x * y)) = x * y = f^{-1}(u) * f^{-1}(v).$$

Luego si X e Y son semigrupos, f^{-1} es un homomorfismo de semigrupos y por lo tanto un isomorfismo.

Si X e Y son grupos, por el Teorema 13, f^{-1} es un homomorfismo de grupos.

Finalmente, si X e Y son monoides, como $f(e_X) = e_Y$, entonces $f^{-1}(e_Y) = e_X$ con lo cual f^{-1} también es un homomorfismo de monoides. □

Teorema **15.** *Sean X, Y, Z semigrupos (resp. monoides o grupos) y $f : X \to Y$, $g : Y \to Z$ homomorfismos de semigrupos (resp. monoides o grupos). Entonces:*

1. *Si $g \circ f$ es un homomorfismo de semigrupos (resp. monoides o grupos).*
2. *Si f es un isomorfismo, entonces f^{-1} es un isomorfismo.*
3. *Si f y g son isomorfismos, entonces $g \circ f$ es un isomorfismo.*

Demostración. 1. Sean $(X, *)$, $(Y, \odot)$ y $(Z, \circ)$ semigrupos. Entonces:

$$g \circ f(x * y) = g(f(x * y)) = g(f(x) \odot f(y)) = g(f(x)) \cdot g(f(y)) = g \circ f(x) \cdot g \circ f(y).$$

Luego $g \circ f$ es un homomorfismo de semigrupos. Si X, Y, Z son grupos, en función del Teorema 13, $g \circ f$ es un homomorfismo de grupos.

Si X, Y, Z son monoides, como f y g son homomorfismos de monoides entonces

$$g \circ f(e_X) = g(f(e_X)) = g(e_Y) = e_Z,$$

con lo cual $g \circ f$ es un homomorfismo de monoides.

2. Es inmediata de la definición de isomorfismo.

3. Como f y g son biyectivas, $g \circ f$ es biyectiva. Luego por el primer item, $g \circ f$ es un homomorfismo biyectivo, y por el Teorema 14 $g \circ f$ es un isomorfismo.

□

Sea X un semigrupo, un monoide o un grupo. Sea

$$\mathrm{Iso}(X) = \{f : X \to X \ : \ f \text{ es un isomorfismo}\}.$$

Por el Teorema 15, la composición de funciones es una operación cerrada en $\mathrm{Iso}(X)$. Más aún, es claro que $Id : X \to X$ es un isomorfismo, y si $f \in \mathrm{Iso}(X)$, entonces $f^{-1} \in \mathrm{Iso}(X)$.

Concluimos que $(\mathrm{Iso}(X), \circ)$ es un grupo (que es en realidad un subgrupo de $(\mathcal{B}(X), \circ)$.

Definición **6.** *Sea X un semigrupo, monoide o grupo. El grupo $(\mathrm{Iso}(X), \circ)$ se denomina* ***grupo de isomorfismos*** *de X.*

Lema **16.** *Sea $\mathcal{S}$ el conjunto de todos los semigrupos. Entonces $X \cong Y$ si y sólo si existe un isomorfismo $f : X \to Y$ es una relación de equivalencia. Un resutado análogo vale en el conjunto $\mathcal{M}$ de todos los monoides o el en conjunto $\mathcal{G}$ de todos los grupos.*

Ejercicio **3.** *Demostrar el Lema 16.*