Facultad de Ciencias

Matemáticas Discretas II

Estructuras Algebraicas

(Guía en preparación)

Dr. Luis Manuel Hernández Ramos

Caracas
12 de junio de 2024

Índice

1. LEYES DE COMPOSICIÓN INTERNA (L.C.I.)

1.1. Operaciones Binarias

En una operación binaria operan dos elementos para producir un resultado. Si en la operación binaria operan dos elementos de un conjunto X para producir un resultado en el mismo conjunto X, se está hablando de operación binaria externa. En esta guía trataremos fundamentalmente con operaciones binarias internas. Si queremos dar una definición más formal y precisa del término Operación Binaria Interna, debemos definir las operaciones binarias como funciones.

Definición 1.1: Operación Binaria (Interna)

Una función $f : X \times X \mapsto X$, se denomina *Operación Binaria (o Composición)* Interna definida en X, si su dominio es todo el producto $X \times X$.

Esta definición quiere decir que la operación binaria interna f, asigna a cada par de elementos $x, y \in X$ un único valor $f(x, y) \in X$. Seguramente, el lector se encuentra relacionado con muchos tipos de operaciones binarias internas diferentes, por ejemplo, la suma de números naturales, enteros, racionales, reales y complejos son operaciones binarias internas. También la multiplicación de números naturales, enteros, racionales, reales y complejos son operaciones binarias internas. Dichas operaciones, se representan como una función en los siguientes ejemplos.

Ejemplo 1.1

Los siguientes son ejemplos de operaciones binarias internas:

- La función $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$ dada por $f(x, y) = x + y$ es una operación binaria interna en el conjunto de los números enteros.
- La función $f : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ definida por $f(x, y) = x + y$ es una operación binaria interna en el conjunto de los números naturales.
- La función $g : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$, definida por $g(x, y) = x - y$ no es una operación binaria interna, puesto que la resta de dos números naturales no siempre es un número natural. Si definiésemos la función $g : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{Z}$, por $g(x, y) = x - y$, estaríamos hablando de una operación binaria externa.
- Si definimos $g : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$ dada por $g(x, y) = x - y$, si es una operación binaria interna puesto que la resta es cerrada en los enteros.

En esta guía, para simplificar, como vamos a trabajar siempre con operaciones binarias internas, al referirnos a operaciones binarias, estaríamos hablando de operaciones binarias

internas.

La representación de una operación binaria como una función puede no ser muy práctica y por eso el lector probablemente no está acostumbrado a utilizarla. En cambio, la regla general es utilizar la llamada notación infija.

Notación 1.1: Notación Infija

Para simplificar la notación, sea una operación binaria $\circ : X \times X \mapsto X$, se puede denotar al valor de la función $\circ$ en el punto (a, b), es decir $\circ(a, b)$, como $a \circ b$.

El ejemplo a continuación muestra el uso de la notación infija para representar la suma de dos números naturales.

Ejemplo 1.2: $a + b$ (Notación infija)

La notación $a+b$ (suma de números naturales), es el valor de la función $+ : \mathbb{N}\times\mathbb{N} \mapsto \mathbb{N}$ en el punto (a, b). Es decir, $+(a, b) \equiv a + b$.

Como funciones, las relaciones binarias también son relaciones y también conjuntos. Eso significa que podemos definir una relación binaria por comprensión o por extensión.

Observación 1.1

Cuando el conjunto X tiene cardinalidad finita, es posible definir la operación binaria por extensión. Por ejemplo, si la operación binaria es $\circ : X \times X \mapsto X$, es posible definirla dando los resultados de $x \circ y$ para todos los pares ordenados $x, y \in X$. Esto puede hacerse mediante una tabla.

El ejemplo a continuación muestra la definición de una operación binaria por extensión mediante una tabla.

Ejemplo 1.3

Se define una operación binaria $*$ en el conjunto $X = \{a, b, c\}$, por extensión, mediante la siguiente tabla:

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

Aquí, los elementos del lado izquierdo de la operación binaria $*$ se muestran en la primera columna de la tabla, y los elementos del lado derecho en la primera fila. De esta tabla puede desprenderse, por ejemplo: $a * a = b$, $a * b = c$, $b * a = a$.

1.2. Definición de Leyes de Composición Interna (L.C.I)

Una Ley de Composición Interna (L.C.I.) es la asociación de una operación binaria interna a un conjunto. Las L.C.I son unas de las estructuras algebraicas más sencillas.

Definición 1.2: Ley de Composición Interna

Sea X un conjunto cualquiera y sea $\circ$ una operación binaria interna definida en X. Entonces a la Estructura Algebraica $[X, \circ]$ se le denomina *Ley de Composición Interna (L.C.I.)*.

El que la asociación de una operación binaria a un conjunto constituya una ley de composición interna, depende tanto de la operación como del conjunto con el que se le está asociando. Para que dicha asociación $[X, \circ]$ sea una ley de composición interna, la operación $\circ$ debe ser cerrada en el conjunto X. A esta propiedad se le conoce también como *Propiedad de Clausura*.

Ejemplo 1.4

A continuación, unos ejemplos de Leyes de Composición Internas y otros ejemplos que no lo son.

- $[\mathbb{Z}, +]$ es una Ley de Composición Interna,
- $[\mathbb{Z}, .]$ es una Ley de Composición Interna,
- $[\mathbb{N}, +]$ es una Ley de Composición Interna,
- $[\mathbb{N}, -]$ *no* es una Ley de Composición Interna,
- $[\mathbb{Z}, -]$ es una Ley de Composición Interna,
- $[\mathbb{Z}, /]$ *no* es una Ley de Composición Interna.

1.3. Elementos Distinguidos

Algunos elementos de las leyes de composición interna son distinguidos en el sentido que presentan propiedades relevantes. La presencia de algunos de estos elementos y de algunas propiedades serán utilizados para definir posteriormente otros tipos de estructuras algebraicas tales como: semigrupos, monoides o grupos. Otros elementos son simplemente elementos destacados que una L.C.I. podría poseer o no. Este es, por ejemplo el caso del elemento cero o nulo que definiremos a continuación.

Definición 1.3: Elemento Nulo

En una Ley de Composición Interna $[X, \circ]$, se dice que un elemento $z \in X$ es un *Elemento Nulo* si cumple que:

$$\forall x \in X : z \circ x = x \circ z = z$$

Veremos algunos ejemplos de la presencia o no de elemento nulo en algunas L.C.I.

Ejemplo 1.5

En $[\mathbb{Z}, .]$ el 0 es un elemento nulo. En cambio, en $[\mathbb{Z}, +]$ no existe elemento nulo.

Ejemplo 1.6

En la operación binaria $*$ definida en $X \times X$ con $X = \{a, b, c\}$ mediante la siguiente tabla:

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

el elemento nulo es a.

Ejemplo 1.7

En la operación binaria $*$ definida en $X \times X$ con $X = \{a, b, c\}$ mediante la siguiente tabla:

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

no hay el elemento nulo. Note que a es un elemento nulo a la izquierda, pero no a la derecha.

Es importante tomar en cuenta la siguiente observación.

Observación 1.2

En la bibliografía, puede encontrarse al elemento nulo bajo la denominación de Elemento Cero. Hay que tener cuidado con esta denominación, ya que el elemento $0 \in \mathbb{Z}$ no siempre es el elemento nulo de la estructura planteada. Por ejemplo, en $[\mathbb{Z}, +]$, como ya dijimos, se tiene que $0 \in \mathbb{Z}$, sin embargo no existe un elemento nulo en dicha estructura. También pudiera darse el caso de un elemento nulo que no sea el 0, como es el caso del ejemplo 1.6.

Un elemento distinguido importante es el Elemento Neutro, que no debe confundirse con el Nulo. La presencia de un Elemento Neutro en una L.C.I. es de mucha relevancia, al punto que muchas de las estructuras algebraicas más importantes tienen la presencia de este.

Definición 1.4: Elemento Neutro

En una Ley de Composición Interna $[X, \circ]$, se dice que un elemento $e \in X$ es un *Elemento Neutro (o Identidad)* si cumple que:

$$\forall x \in X : e \circ x = x \circ e = x$$

- Si se cumple que $\forall x \in X : e \circ x = x$, se dice que e es un *neutro a la izquierda.*
- Si se cumple que $\forall x \in X : x \circ e = x$, se dice que e es un *neutro a la derecha.*
- Un elemento neutro es al mismo tiempo un neutro a la izquierda y un neutro a la derecha.

A continuación se darán varios ejemplos en donde hay o no presencia de un elemento neutro.

Ejemplo 1.8

En $[\mathbb{Z}, .]$ el elemento neutro es el 1. En cambio, en $[\mathbb{Z}, +]$ el elemento neutro es el 0.

Ejemplo 1.9

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

el elemento neutro es b.

Ejemplo 1.10

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

no hay elemento neutro. El elemento b es neutro por la izquierda, pero no por la derecha.

Ejemplo 1.11

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

no hay elemento neutro. El elemento b es neutro por la izquierda, pero no por la derecha.

Un hecho relevante es que en una L.C.I. puede haber a lo sumo un elemento neutro (si existe, es único). Esto queda enunciado en el siguiente lema.

Lema 1.1: Unicidad del neutro

Sea $[X, \circ]$ una Ley de Composición Interna. Entonces hay a lo sumo un elemento neutro $e \in X$.

Demostración 1.1

Por reducción al absurdo, supongamos que existen dos elementos neutros $e_1 \in X$ y $e_2 \in X$, $e_1 \neq e_2$. Entonces,

$$e_1 * e_2 = e_2,$$

por ser e_1 un elemento neutro a la izquierda. Igualmente,

$$e_1 * e_2 = e_1,$$

por ser e_2 un elemento neutro a la derecha. Por lo tanto $e_1 * e_2 = e_1 = e_2$, lo que contradice la suposición inicial $e_1 \neq e_2$. En consecuencia el elemento neutro es único.

Observación 1.3

En realidad esta argumentación prueba algo más, prueba que no puede existir un neutro a la izquierda y un neutro a la derecha diferentes.

Cada elemento de una L.C.I. podría o no tener un elemento simétrico (o inverso).

Definición 1.5: Elemento Simétrico o Inverso

Sea una $[X, \circ]$ una Ley de Composición Interna con elemento neutro e. Sea $x \in X$ un elemento cualquiera. Se dice que el elemento $x^{-1} \in X$ es el *Elemento Simétrico o Inverso* de x, si cumple que:

$$x \circ x^{-1} = x^{-1} \circ x = e$$

Si además, para todo elemento $x \in X$ existe un elemento simétrico (inverso) x^{-1}, entonces se dice que $[X, \circ]$ tiene la propiedad de simétrico (inverso).

- Si para un elemento $y \in X$, se cumple que $y \circ x = e$, se dice que este es un *simétrico (inverso) a la izquierda.*
- Si se cumple que $x \circ y = e$, entonces se dice que y es un *simétrico (inverso) a la derecha.*
- Un elemento simétrico (inverso) es un simétrico (inverso) a la izquierda y a la derecha simultáneamente.

Nota 1.1

Hay que tomar en cuenta los siguientes hechos:

- La existencia del elemento simétrico está ligada a que en la estructura algebraica haya un elemento neutro. Estructuras algebraicas sin elemento neutro no pueden tener elementos simétricos.
- Hay que notar que en la definición anterior no se habla de un simétrico de toda la estructura algebraica $[X, \circ]$, sino que se habla del simétrico de elementos x de X en particular. En un estructura algebraica pudiera haber elementos sin elemento inverso (o simétrico).

La presencia de elementos simétricos para todos los elementos del conjunto en donde se define la L.C.I. es una propiedad importante que de ocurrir permitiría deducir aseveraciones relevantes respecto a la estructura algebraica. Por esta razón se hace una definición especial para este caso.

Definición 1.6: Inverso o Simétrico de una Estructura Algebraica

Cuando en una estructura algebraica $[X, \circ]$ todo elemento $x \in X$ tiene elemento simétrico $x^{-1} \in X$, se dice que la estructura $[X, \circ]$ tiene *Elemento Simétrico*.

A continuación, unos ejemplos sobre la presencia o no de elementos simétricos (o inversos) en una L.C.I.

Ejemplo 1.12

En $[\mathbb{Z}, .]$ el elemento simétrico (o inverso) de un elemento $x \in \mathbb{Z}, x \neq 0$, cualquiera es $1/x$. Como el elemento 0 no tiene elemento simétrico, entonces se dice que en la estructura $[\mathbb{Z}, .]$ no tiene la propiedad del elemento simétrico.

Ejemplo 1.13

En $[\mathbb{Z}, +]$ todo elemento $x \in \mathbb{Z}$ tiene un único elemento simétrico. En efecto, el simétrico de un elemento $x \in \mathbb{Z}$, es el elemento $-x$. Es decir, $x^{-1} = -x$ en la notación utilizada. En consecuencia, la estructura $[\mathbb{Z}, +]$ tiene la propiedad del elemento simétrico.

Ejemplo 1.14

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

el elemento neutro es b. También $a^{-1} = c$, $b^{-1} = b$ y $c^{-1} = a$.

Ejemplo 1.15

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

el elemento neutro es b. Aquí se tiene que $b^{-1} = b$, y los elementos a y c no tienen elemento simétrico.

Otros elementos que pudieran ser relevantes en una estructura algebraica, en caso de existir, serían los elementos idempotentes.

Definición 1.7: Elementos Idempotentes

Sea $[X, \circ]$ una Ley de Composición Interna. Un elemento $a \in X$ se dice *Idempotente* si $a \circ a = a$.

Ejemplo 1.16

En la operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

Los elementos a y b son idempotentes. En cambio, el elemento c no es idempotente.

1.4. Propiedades de las Leyes de Composición Internas

Es posible que estemos acostumbrados a escuchar que una operación dada cumpla con la propiedad conmutativa, o que cumpla con la propiedad asociativa. Casos célebres son los de la suma de naturales, enteros, racionales y reales, o el de la multiplicación definida en esos mismos conjuntos. Estas estructuras son conmutativas, asociativas, etc. Sin embargo, hay L.C.I. que no cumplen con estas propiedades. Las propiedades que cumplen las L.C.I. permiten clasificarlas.

La primera de estas propiedades es tal vez la más famosa. Desde la escuela primaria hemos escuchado decir, por ejemplo, que "el orden de los factores no altera el producto". Esto quiere decir simplemente que las estructuras que tienen como operación a la multiplicación son conmutativas. Definamos lo que es una L.C.I. conmutativa:

Definición 1.8: L.C.I. Conmutativa

Una Ley de Composición Interna, $[X, \circ]$ se dice *Conmutativa* si,

$$\forall a, b \in X : x \circ y = y \circ x;$$

He aquí algunos ejemplos de lyes de composición internas sobre conjuntos finitos, con operaciones definidas por extensión:

Ejemplo 1.17

La operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

es conmutativa.

Ejemplo 1.18

La operación binaria $*$ definida en $X = \{a, b, c\}$ mediante la siguiente tabla:

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

no es conmutativa. En efecto, $a * b = b$ y $b * a = a$.

Note que en las L.C.I. Conmutativas, la tabla que define la operación es simétrica

respecto a su diagonal.

Otros ejemplos de L.C.I sobre conjuntos infinitos son los siguientes:

Ejemplo 1.19

Algunos ejemplos de L.C.I. conmutativas y no conmutativas son:

- $[\mathbb{Z}, +]$ es una Ley de Composición Interna Conmutativa,
- $[\mathbb{Z}, .]$ es una Ley de Composición Interna Conmutativa,
- $[\mathbb{N}, +]$ es una Ley de Composición Interna Conmutativa,
- $[\mathbb{Z}, -]$ es una Ley de Composición Interna *no* Conmutativa,

Otra de las propiedades importantes que puede tener una L.C.I. es la Asociatividad.

Definición 1.9: L.C.I Asociativa

Una Ley de Composición Interna (L.C.I), $[X, \circ]$ se dice que es *Asociativa* si para todo $x, y, z \in X$ cumple:

$$(x \circ y) \circ z = x \circ (y \circ z);$$

Quizás, la asociatividad no es suficientemente valorada como propiedad para el no conocedor. Pero cuando uno reflexiona que en una L.C.I no asociativa, la manera como se efectúan las operaciones influye en el resultado, cae en cuenta de su importancia. El que una estructura algebraica sea asociativa permite definir la operación de muchos términos sin recurrir a paréntesis, como por ejemplo,

$$a \circ b \circ c \circ d,$$

sin importar como uno coloque los paréntesis para realizar las operaciones binarias, el resultado es el mismo.

Ejemplo 1.20

Ejemplos de L.C.I asociativas son los siguientes:

- $[\mathbb{Z}, +]$ es una Ley de Composición Interna Asociativa.
- $[\mathbb{Z}, .]$ es una Ley de Composición Interna Asociativa.
- $[\mathbb{N}, +]$ es una Ley de Composición Interna Asociativa.
- $[\mathbb{Z}, -]$ es una Ley de Composición Interna *no* Asociativa.

Nota 1.2: La aritmética de punto flotante no es asociativa

En la aritmética de punto flotante, la suma y la multiplicación de números representables no son operaciones asociativas. Entonces, a la hora de realizar cálculos con dicha aritmética, los resultados pueden cambiar según se coloquen los paréntesis. Este es un hecho importante para los cálculos numéricos en el computador.

Es muy probable también, que en nuestra formación hayamos tenido que "despejar variables"para obtener resultados de ecuaciones. Podemos despejar, sólo los elementos cancelables.

Definición 1.10: Elementos Cancelables

Sea $[X, \circ]$ una Ley de Composición Interna. Un elemento $x \in X$ se dice *Cancelable* respecto a la operación $\circ$ si,

$$\forall y_1, y_2 \in X : (x \circ y_1 = x \circ y_2) \vee (y_1 \circ x = y_2 \circ x) \Rightarrow (y_1 = y_2)$$

Y si una estructura algebraica posee la Propiedad de Cancelación, quiere decir que siempre podemos despejar.

Definición 1.11: Propiedad de Cancelación

Sea una estructura algebraica $[X, \circ]$. Si todos los elementos $x \in X$ son cancelables se dice que la estructura tiene la propiedad de cancelación.

Ejemplo 1.21

- En la estructura multiplicativa $[\mathbb{R}, .]$ todos los elementos son cancelables excepto el cero. Al no tener la propiedad de cancelación siempre se debe tomar precaución a la hora de despejar.
- La estructura $[\mathbb{R}, +]$ si tiene la propiedad de cancelación.

Una relación entre elementos de una L.C.I. se dice de Congruencia, si la relación se mantiene a través de la operación. Más precisamente,

Definición 1.12: Relaciones de Congruencia

Sea $[X, \circ]$ una Ley de Composición Interna. Sea R una relación de equivalencia definida en X. Se dice que R es una *Congruencia* en $[X, \circ]$ si,

$$\forall x_1, x_2, y_1, y_2 \in X : (x_1 R x_2) \wedge (y_1 R y_2) \Rightarrow (x_1 \circ y_1) R (x_2 \circ y_2)$$

Un ejemplo clásico es la relación de congruencia módulo n en los números enteros.

Ejercicio 1.1

Demostrar que la relación de congruencia módulo n definida en los números enteros es una relación de congruencia en $[\mathbb{Z}, +]$

Esta relación de congruencia permite definir la operación suma entre clases de equivalencia de la relación.

1.5. Ejercicios adicionales sobre Leyes de Composición Internas

He aquí algunos ejercicios sobre L.C.I.

Ejercicio 1.2

Sea X el conjunto de proposiciones lógicas, simples o compuestas. Determine si $[X, \wedge]$ y $[X, \vee]$ son leyes de composición internas. Determine presencia de elementos distinguidos y propiedades que cumplen.

Ejercicio 1.3

Dado un conjunto no vacío X. Determine si $[P(X), \cap]$ y $[P(X), \cup]$ son leyes de composición internas. Determine presencia de elementos distinguidos y propiedades que cumplen.

Ejercicio 1.4

Dado un valor $n \in \mathbb{Z}$. Para $a, b \in \mathbb{Z}$, se define la operación $*$ como:

$$a * b = a + b - n.$$

¿Es $[\mathbb{Z}, *]$ una L.C.I?. Si es así, determine sus elementos distinguidos y propiedades.

Ejercicio 1.5

Para $a, b \in \mathbb{Z}^+$, se define la operación $*$ como:

$$a * b = \text{máx}\{a, b\}.$$

¿Es $[\mathbb{Z}^+, *]$ una L.C.I?. Si es así, determine sus elementos distinguidos y propiedades.

Ejercicio 1.6

Para $a, b \in \mathbb{Z}^+$, se define la operación $\circ$ como:

$$a \circ b = M.C.D\{a, b\}. \text{ Máximo Común Divisor}$$

y la operación $*$ se define como:

$$a * b = m.c.m\{a, b\}. \text{ Mínimo Común Múltiplo}$$

¿Es $[\mathbb{Z}^+, \circ]$ una L.C.I?. Si es así, determine sus elementos distinguidos y propiedades. ¿Es $[\mathbb{Z}^+, *]$ una L.C.I?. Si es así, determine sus elementos distinguidos y propiedades.

Ejercicio 1.7

Sea la estructura $[P, +]$, donde $P = \{x \mid x = 2k,\ k \in \mathbb{Z}\}$ (Números Pares). Verifique si es una L.C.I., presencia de elementos distinguidos y propiedades.

Ejercicio 1.8

Sea la estructura $[I, +]$, donde $I = \{x \mid x = 2k + 1,\ k \in \mathbb{Z}\}$ (Números Impares). Verifique si es una L.C.I., presencia de elementos distinguidos y propiedades.

Ejercicio 1.9

Sea la estructura $[X, .]$, donde $X = \{x \in \mathbb{Q} \mid x = 2^k,\ k \in \mathbb{Z}\}$ (Potencias de dos) y la operación . la multiplicación de números racionales. Verifique si es una L.C.I., presencia de elementos distinguidos y propiedades.

Ejercicio 1.10

Sea X=$\{f \mid f : \mathbb{R} \mapsto \mathbb{R}\}$ el conjunto de las funciones reales. ¿La estructura $[X, \circ]$ es una L.C.I.? Aquí la operación $\circ$ es la composición de funciones. Determine presencia de elementos distinguidos y propiedades.

2. SEMIGRUPOS

La propiedad asociativa es de tal importancia, que una L.C.I. asociativa pasa a una nueva categoría llamada Semigrupo.

Definición 2.1: Semigrupo

Sea X un conjunto cualquiera, y sea $[X, \circ]$ una Ley de Composición Interna Asociativa. Entonces se dice que $[X, \circ]$ es un *Semigrupo*.

Es probable que conozcamos muchos ejemplos de semigrupos, como los que enumeraremos en el ejemplo a continuación:

Ejemplo 2.1

Algunas de las siguientes estructuras son semigrupos, otras no lo son:

- $[\mathbb{Z}, +]$ es un Semigrupo,
- $[\mathbb{Z}, .]$ es un Semigrupo,
- $[\mathbb{N}, +]$ es un Semigrupo,
- $[\mathbb{Z}, -]$ *no* es un Semigrupo (no es asociativa).

Los semigrupos de cadenas de caracteres son muy importantes en computación, en particular en teoría de compiladores. A continuación se ejemplificará el llamado Semigrupo Libre Asociado.

Ejemplo 2.2

Sea X un conjunto finito arbitrario. Sea X^+ el conjunto de todas las secuencias finitas no vacías de elementos de X. Sea $\|$ la operación de concatenación definida en X^+ como:
Si $a = x_1x_2 \dots x_n \in X^+$, y $b = y_1y_2 \dots y_m \in X^+$ entonces:

$$a\|b = x_1x_2 \dots x_nb = x_1x_2 \dots x_ny_1y_2 \dots y_m.$$

La estructura $[X^+, \|]$, es un semigrupo denominado: el *Semigrupo Libre* generado por X.

Ejercicio 2.1

Demostrar que el Semigrupo Libre generado por un conjunto X es siempre asociativo.

2.1. Ejercicios adicionales de semigrupos

Ejercicio 2.2

Verificar cuales de los ejercicios y ejemplos sobre L.C.I. corresponden efectivamente a semigrupos y cuales no.

Ejercicio 2.3

Sea $[S, *]$ un semigrupo y sea T un subconjunto no vacío de S. ¿Será $[T, *]$ también un semigrupo?. En caso negativo ¿Qué propiedad debe cumplirse para que $[T, *]$ sea un semigrupo?

Ejercicio 2.4

Sea $[S, *]$ un Semigrupo.

1. ¿Pueden existir en $[S, *]$ dos elementos neutros a la izquierda distintos, $l_1 \neq l_2$? Demuéstrelo.
2. Demuestre que de existir en $[S, *]$ dos elementos neutros a la izquierda l_1 y l_2, con $l_1 \neq l_2$, entonces no puede existir un elemento r neutro a la derecha.
3. ¿Se puede demostrar lo anterior sin la necesidad de la propiedad asociativa?

3. MONOIDES

En álgebra abstracta, un monoide es una estructura algebraica con una operación binaria que es asociativa y tiene elemento neutro. Los monoides no sólo son de interés para el álgebra abstracta, sino que tienen aplicaciones en la computación en temas tales como: lenguajes formales y máquinas de estado finito.

Definición 3.1: Monoide

Sea $[M, \circ]$ un Semigrupo. Si existe un elemento neutro $e \in M$ se dice que $[M, \circ]$ es un *Monoide*.

Notación 3.1

A la hora de representar monoides, tengamos en cuenta algunos aspectos de la notación:

- En esta guía, salvo que se indique otra cosa, se denotará al elemento neutro con la letra e.
- En ocasiones, para hacer distinción del elemento neutro e, se le agregará a la notación de la estructura. Por ejemplo, al monoide $[M, \circ]$ se le podrá denotar como $[M, \circ, e]$.
- Es frecuente que se diga que el conjunto M es un monoide, cuando en realidad el monoide es la estructura que incluye la operación. Esto se realiza a veces para simplificar. Sin embargo, hay que tomar en cuenta que en una estructura algebraica, el conjunto va siempre ligado a por lo menos una operación.

Ejemplo 3.1

A continuación, algunos ejemplos de monoides:

- $[\mathbb{Z}, +, 0]$ es un Monoide,
- $[\mathbb{Z}, ., 1]$ es un Monoide,
- $[\mathbb{N}, +, 0]$ es un Monoide.

Si a los semigrupos libres asociados definidos anteriormente, les permitimos la posibilidad de una cadena o secuencia vacía, esta puede servir como elemento neutro de la operación de concatenación. En ese caso, la estructura obtenida se convierte en un monoide, llamado Monoide Libre Asociado. Los Monoides Libres Asociados son importante en el estudiuo de los lenguajes formales.

Ejemplo 3.2: Monoide Libre Asociado

Sea X un conjunto finito arbitrario. Sea X^+ el conjunto de todas las secuencias finitas vacías o no vacías de elementos de X. Sea Λ la secuencia vacía. Sea $\|$ la operación de concatenación, definida en X^+ como: si $a = x_1x_2\ldots x_n \in X^+$ y $b = y_1y_2\ldots y_m \in X^+$, entonces:

$$a\|b = x_1x_2\ldots x_nb = x_1x_2\ldots x_ny_1y_2\ldots y_m.$$

La estructura algebraica $[X^+, \|, \Lambda]$, es un monoide denominado: el *Monoide Libre* generado por X.

Los elementos de un monoide no tienen porqué tener un elemento inverso, pero en caso de tenerlo, este es único.

Lema 3.1: Unicidad del Inverso en un Monoide

En un Monoide $[M, \circ]$, un elemento $x \in M$ tiene a lo sumo un elemento inverso x^{-1}.

Demostración 3.1

Supongamos que para un elemento $x \in M$ existen dos elementos simétricos distintos x_1^{-1} y x_2^{-1}, $x_1^{-1} \neq x_2^{-1}$. Entonces,

$$x_1^{-1} = x_1^{-1} \circ e = x_1^{-1} \circ (x \circ x_2^{-1}) = (x_1^{-1} \circ x) \circ x_2^{-1} = e \circ x_2^{-1} = x_2^{-1},$$

lo que contradice la hipótesis $x_1^{-1} \neq x_2^{-1}$ y por lo tanto el elemento simétrico de x es único.

3.1. Homomorfismo entre Monoides

Una de las ideas más importantes en las matemáticas modernas tienen que ver con aplicaciones que conservan la estructura de un álgebra en otra. Estas aplicaciones, pueden o no ser biyectivas. En ocasiones, se requiere que dos estructuras algebraicas sean "similares", en el sentido que que lo sean sus operaciones y propiedades. También, pudiera requerirse que una estructura simule a otra estructura, exhibiendo el mismo o parte de su comportamiento. También pudiera requerirse que una estructura algebraica sea capaz de hacer lo que hace la otra. Todo esto es importante, por ejemplo, en el estudio de las máquinas de estado finito. Las aplicaciones de las que hablamos se denominan homomorfismos.

Definición 3.2: Homomorfismo entre Monoides

Sean $[A, \circ, e_A]$ y $[B, *, e_B]$ monoides. Sea $\phi : A \mapsto B$ una aplicación. Se dice que ϕ es un *Homomorfismo* entre los monoides $[A, \circ, e_A]$ y $[B, *, e_B]$ si cumple:

1. $\forall x, y \in A : \phi(x \circ y) = \phi(x) * \phi(y)$.
2. $\phi(e_A) = e_B$.

Si además ϕ es biyectiva, se dice que ϕ es un *Isomorfismo*.

Una aplicación que ejemplifica muy bien el significado de los homomorfismos son los logaritmos. Una de las primeras aplicaciones de los logaritmos fueron las de poder realizar multiplicaciones y divisiones de números grandes, realizando sumas y restas. Esto era una necesidad real antes de la aparición de las máquinas calculadoras o de los computadores. El logaritmo es un homomorfismo (isomorfismo) que permite hacer operaciones en el monoide $[\mathbb{R}^+, ., 1]$ mediante cálculos en el monoide $[\mathbb{R}, +, 0]$. Antes de la invención de las máquinas calculadoras, los cálculos los logaritmos y de sus inversas se hacían mediante tablas.

Ejemplo 3.3

Sean los monoides $[\mathbb{R}^+, ., 1]$ y $[\mathbb{R}, +, 0]$. Sea $\phi(x) : \mathbb{R}^+ \mapsto \mathbb{R}$ la función definida como $\phi(x) = \ln(x)$. Se tiene que

1. $\ln(x.y) = \ln(x) + \ln(y)$.
2. $\ln(1) = 0$.

entonces esta función es un homomorfismo entre $[\mathbb{R}^+, ., 1]$ y $[\mathbb{R}, +, 0]$. Además, como ϕ es biyectiva se trata de un isomorfismo.

Ejercicio 3.1

Sean $A = \{a, b, c\}$ y $B = \{x, y, z\}$. Se definen las operaciones $\circ : A \times A \mapsto A$ y $* : B \times B \mapsto B$, mediante las tablas siguientes:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Sea la operación $\phi : A \mapsto B$ definida por:

$$\phi(a) = y, \quad \phi(b) = x, \quad \phi(c) = z.$$

Demuestre que ϕ es un isomorfismo entre $[A, \circ, a]$ y $[B, *, y]$.

3.2. Monoides de Transformación

Existe una amplia variedad de monoides. Incluso, uno podría definir un monoide cuyos elementos sean funciones que van de un conjunto en sí mismo. Estas funciones son denominadas transformaciones. Un monoide de transformación es una estructura algebraica que formaliza la noción de aplicar secuencias de transformaciones a un valor.

Definición 3.3: Transformación

Sea S cualquier conjunto. Una transformación de S es una aplicación $T : S \mapsto S$.

Definición 3.4: Monoide de Transformación

Sea $\mathbb{T} = \{T_\alpha\}$, una colección de transformaciones $T_\alpha : S \mapsto S$, la cual contiene a la aplicación identidad I_S y es cerrada respecto a la composición de aplicaciones. Esto es,

$$T_\alpha \in \mathbb{T} \text{ y } T_\beta \in \mathbb{T} \Longrightarrow T_\alpha \circ T_\beta \in \mathbb{T}.$$

Entonces, a la estructura algebraica $[\mathbb{T}, \circ, I_S]$ se le conoce con el nombre de *Monoide de Transformación*.

Los elementos de un monoide de transformación son transformaciones (aplicaciones de un conjunto en si mismo) y la operación binaria $\circ$ es la composición de funciones.

Lema 3.2

$[T, \circ, I_S]$ verifica los axiomas:

1. $T_\alpha \circ \left(T_\beta \circ T_\gamma\right) = \left(T_\alpha \circ T_\beta\right) \circ T_\gamma$ (Asociatividad)
2. $T_\alpha \circ I_S = I_S \circ T_\alpha = T_\alpha$ (Elemento Neutro)

y es, por lo tanto, un Monoide.

Ejercicio 3.2

Demostrar el lema anterior.

Ejercicio 3.3

Sea |S|=n. ¿Cuantas transformaciones posibles hay $T_\alpha : S \mapsto S$.

3.3. Teorema de Cayley (Monoides)

El teorema de Cayley, enunciado por el matemático británico Arthur Cayley, es un resultado fundamental que establece un isomorfismo entre cualquier monoide y un monoide de transformación. Esto quiere decir que podemos estudiar a los monoides estudiando a los monoides de transformación, facilitando la comprensión de su estructura y funcionamiento. También facilita la clasificación de los monoides.

Teorema 3.1: Teorema de Cayley (Monoides)

Todo monoide es isomorfo a un monoide de transformación.

Demostración 3.2

Sea $[M, *]$ un monoide y sea $T_M = \{T_g : g \in M\}$ una colección de transformaciones $T_g : M \mapsto M$ definidas por,

$$T_g(x) = x * g, \qquad \forall x \in M.$$

Probaremos primero que la aplicación $\phi : M \mapsto T_M$, definida como: $\phi(g) = T_g$ es un homomorfismo entre $[M, *]$ y $[T_M, \circ]$. En efecto, para todo $x \in M$,

$$\phi(g * h)(x) = T_{g*h}(x) = x * (g * h) = (x * g) * h = T_h(T_g(x)) = (T_g \circ T_h)(x),$$

por lo que,

$$\phi(g * h) = \phi(g) \circ \phi(h).$$

La aplicación $\phi(g) : g \mapsto T_g$ es además biyectiva. Probaremos que es inyectiva y sobreyectiva.,

1. Sobreyectividad: Por construcción de la aplicación ϕ, toda transformación $T_g \in T_M$ tiene su pre-imagen $g \in M$.
2. Inyectividad:

$$\begin{aligned} \phi(g) = \phi(h) &\Rightarrow T_g(x) = T_h(x), \quad \forall x \in M \\ &\Rightarrow x * g = x * h, \quad \forall x \in M \\ &\Rightarrow g = h \text{ Tomando } x = e. \end{aligned}$$

Entonces ϕ es un isomorfismo entre el monoide $[M, *]$ y el monoide $[T_M, \circ]$.

3.4. Ejercicios adicionales de Monoides

Ejercicio 3.4

Sea la estructura $[\mathbb{N}, *]$ donde la operación $*$ se define de la siguiente manera,

$$a * b = \text{máx}\{a, b\}.$$

Demuestre que $[\mathbb{N}, *]$ es un monoide.

Ejercicio 3.5

Sea $\mathbb{Z}^+$ el conjunto de los números enteros positivos. Sean las operaciones,

$$\begin{aligned} a * b &= MCD(a,b) \quad \text{Máximo Común Divisor} \\ a \circ b &= mcm(a,b) \quad \text{Mínimo Común Múltiplo.} \end{aligned}$$

Determine si $[\mathbb{Z}^+, *]$ y $[\mathbb{Z}^+, \circ]$ son monoides. ¿Cómo tendría que ser al conjunto A, para que ambas $[A, *]$ y $[A, \circ]$ sean monoides.

Ejercicio 3.6

Sea la estructura $[F, \circ]$, donde $F = \{f \mid f : \mathbb{R} \mapsto \mathbb{R}\}$ es el conjunto de funciones reales y la operación $\circ$ es la composición de funciones. Demuestre que $[F, \circ]$ es un Monoide. ¿Qué le faltaría para que cada elemento tuviera un Elemento Simétrico o Inverso?.

Ejercicio 3.7

Sea $[M, \circ]$ un monoide con la siguiente propiedad,

$$\forall x, y \in M : x \circ y \circ x = y \circ x \circ y.$$

Demuestre que en $[M, \circ]$ se cumple:

1. $\forall x \in M : x \circ x = x$. (Idempotencia).
2. $\forall x, y \in M : x \circ y = y \circ x$. (Conmutatividad).

Ejercicio 3.8

Sea $[M, *]$ un monoide conmutativo. Se define el conjunto

$$S = \{T \mid [T, *] \text{ es un submonoide de } [M, *]\}.$$

Para todo $A, B \in S$, se define la operación $\#$ de la siguiente manera,

$$A \# B = \{x \mid x = a * b,\ a \in A, b \in B\}.$$

Demuestre que la estructura $[S, \#]$ es un monoide conmutativo.

4. GRUPOS

El lector, quizás se encuentre familiarizado con la resolución de ecuaciones algebraicas lineales y cuadráticas mediante resolventes. Existen también fórmulas resolventes para ecuaciones de grados tres y cuatro. Durante siglos, se buscaron infructuosamente fórmulas resolventes generales para ecuaciones algebraicas de grado 5 o más. En el siglo XIX, dos jóvenes, Niels Abel de Noruega y Evariste Galois de Francia, fueron pioneros en la determinación de las condiciones bajo las cuales estos resolventes pueden existir. La teoría desarrollada, especialmente por Evariste Galois, involucra el desarrollo de la Teoría de Grupos. Un grupo es esencialmente un monoide $[G, \circ]$ en el que existe solución única para todas las ecuaciones del tipo $a \circ x = b$, con $a, b \in G$. La existencia de una única solución para tales ecuaciones depende de la existencia de un único elemento inverso a^{-1} para todo $a \in G$. Entonces, la solución al sistema $a \circ x = b$ vendría siendo

$$x = e \circ x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ b.$$

Entonces, un grupo $[G, \circ]$ vendría siendo una L.C.I., asociativa, con elemento neutro y donde cada elemento $a \in G$ tiene un único elemento inverso.

Definición 4.1: Grupo

Sea $[G, \circ]$ un Monoide. Si $[G, \circ]$ tiene la propiedad de inverso, se dice que $[G, \circ]$ es un *Grupo*.

Notación 4.1

Algunos usos de la notación a tomar en cuenta son:

- Para distinguir al elemento neutro e de un grupo $[G, \circ]$, se suele denotar este como $[G, \circ, e]$. El elemento inverso también se suele distinguir en la estructura, por ejemplo de la siguiente manera, $[G, \circ, e, (.)^{-1}]$.
- En esta guía, salvo que se indique otra cosa al simétrico (o inverso) de un elemento $x \in G$ se le denotará como x^{-1}. El elemento inverso de un grupo no es siempre $x^{-1} = \frac{1}{x}$. En un grupo aditivo, por ejemplo, $x^{-1} = -x$.
- En ocasiones, para simplificar, se habla de que un conjunto G es un grupo, cuando en realidad el grupo es la estructura que incluye la operación.

El orden de un grupo $[G, \circ]$ es la cantidad de elementos del conjunto G.

Definición 4.2: Orden de un Grupo

El *Orden* de un Grupo $[G, \circ]$ es la cardinalidad del conjunto G

Existen grupos de orden finito y grupos de orden infinito.
A continuación algunos ejercicios.

Ejercicio 4.1

Sea la estructura $[\mathbb{C}, \circ]$, donde $\mathbb{C} = \{1, i, -1, -i\}$, y la operación $\circ$ es el producto de números complejos. Demuestre que $[\mathbb{C}, \circ]$ es un grupo.

Ejercicio 4.2

Sean $A = \{a, b, c\}$ y $B = \{x, y, z\}$. Se definen las operaciones $\circ : A \times A \mapsto A$ y $* : B \times B \mapsto B$, mediante las tablas siguientes:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Las estructuras $[A, \circ, a]$ y $[B, *, y]$ son ejemplos de grupos. Demuéstrelo.

Lema 4.1

Sea $[G, \circ]$ un grupo. Demuestre que $e^{-1} = e$.

Ejercicio 4.3

Demuestre el lema anterior.

Lema 4.2

Sea $[G, \circ]$ un grupo. Sea $x \in G$. Se cumple,

$$(x^{-1})^{-1} = x.$$

Ejercicio 4.4

Demuestre el lema anterior.

Lema 4.3

Sea $[G, \circ]$ un grupo. Sean $x, y \in G$. Entonces,

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

Demostración 4.1

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

Lema 4.4: Propiedad de Cancelación en los Grupos

Sea $[G, \circ]$ un Grupo. Entonces, todo $x \in G$ es cancelable. Los grupos tienen la propiedad de cancelación.

Observación 4.1

La propiedad de cancelación de un grupo es la que permite despejar variables.

Ejercicio 4.5

Demuestre la propiedad de cancelación en los grupos.

4.1. Subgrupos

Un subgrupo es un subconjunto de un grupo que también es un grupo bajo la misma operación del grupo original. El análisis de los subgrupos de un grupo permite descomponer grupos complejos en grupos más pequeños y manejables, facilitando su análisis y comprensión. Los subgrupos juegan un papel crucial en la teoría de la simetría, donde se utilizan para describir las diferentes formas en que un objeto o patrón puede ser transformado sin cambiar su apariencia fundamental. Específicamente, en Química, los subgrupos de simetría molecular se utilizan para clasificar y estudiar las propiedades de las moléculas. En Física, los subgrupos tienen aplicaciones en áreas como la mecánica cuántica y la teoría de la relatividad.

Definición 4.3: Subgrupo

Sea $[G, \circ]$ un Grupo. Sea $S \subseteq G$. Si $[S, \circ]$ es también un grupo, se dice que es un *Subgrupo de* $[G, \circ]$.

Ejemplo 4.1

Sea $[G, \circ]$ un grupo con elemento neutro e, entonces el conjunto $[\{e\}, \circ]$ es siempre un subgrupo de $[G, \circ]$.

Ejemplo 4.2

$[\mathbb{Z}, +]$ es un subgrupo de $[\mathbb{R}, +]$

Una ventaja que presenta el estudio de los subgrupos es que hereda propiedades del grupo original. En consecuencia, para probar que una estructura es un subgrupo de otra, no hace falta verificar todas las propiedades. El siguiente teorema permite caracterizar subgrupos mediante unas pocas propiedades.

Teorema 4.1: Caracterización de Subgrupos

Sea $[G, \circ]$ un Grupo. Sea $S \subseteq G$ un conjunto no vacío. Entonces $[S, \circ]$ será un Subgrupo de $[G, \circ]$ si cumple,

$$\forall x, y \in S : x \circ y^{-1} \in S. \tag{1}$$

Demostración 4.2

1. **Asociatividad:** Como G es un grupo

   $$\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z).$$

   Como $S \subseteq G$, entonces la propiedad se cumple para todo elemento en S.

2. **Elemento Neutro:** Dado que S es no vacío, existe un elemento $x \in S$. Por la propiedad 1, tomando $y = x$ se tiene:

   $$x \circ y^{-1} = x \circ x^{-1} = e \in S.$$

   Por lo que el elemento neutro de G pertenece a S, y es por supuesto el elemento neutro de $[S, \circ]$.

3. **Elemento Simétrico o Inverso**: De nuevo, por la propiedad 1 y tomando $x = e$ se tiene:

   $$\forall y \in S : e \circ y^{-1} = y^{-1} \in S.$$

   lo que demuestra que para todo elemento $y \in S$ su simétrico o inverso $y^{-1} \in S$.

Lema 4.5

Demuestre que $[S, \circ]$ es un subgrupo de $[G, \circ]$ si y sólo si se cumplen estas tres condiciones:

1. $S \neq \emptyset$, $S \subseteq G$.
2. $\forall x \in S : x^{-1} \in S$.
3. $\forall x, y \in S : x \circ y \in S$.

Ejercicio 4.6

Demuestre la equivalencia del lema anterior con la caracterización de subgrupos demostrada en esta guía.

4.2. Teorema de Lagrange

El Teorema de Lagrange es fundamental en la teoría de grupos, ya que permite establecer una conexión crucial entre el orden de un grupo finito y el orden de sus subgrupos. Este teorema, fue enunciado por el matemático italiano de origen francés Joseph Louis Lagrange en el siglo XVIII.

Antes de enunciar el Teorema de Lagrange, vamos a definir dos relaciones de equivalencia sobre los elementos de un grupo llamadas Relaciones de Equivalencia a la Izquierda y Relaciones de Equivalencia a la Derecha. Cada subgrupo de un grupo genera ambas relaciones definidas como sigue.

Definición 4.4: Equivalencia a la Derecha y de Equivalencia a la Izquierda

Cada subgrupo S de un grupo G permite definir dos relaciones de equivalencia sobre el conjunto G: la equivalencia a la izquierda (denotada $\equiv_S$) y la equivalencia a la derecha (denotada ${}_S\equiv$). Estas relaciones se definen de la siguiente manera para todo $x, y \in G$:

$$x \equiv_S y \iff \exists a \in S : y = x \circ a.$$
$$x {}_S\equiv y \iff \exists a \in S : y = a \circ x.$$

Como es bien sabido, las relaciones de equivalencia definen las llamadas clases de equivalencia que conforman una partición del conjunto en el que se define la relación. En este caso, las clases definidas son llamadas clases laterales.

Definición 4.5: Clases Laterales

Las llamadas *Clases Laterales* son las clases de equivalencia definidas por estas relaciones. Se denotan como xS en el caso de la equivalencia a la izquierda y Sx en el caso de la equivalencia a la derecha.

Notación 4.2

Como es bien sabido, las clases de equivalencia forman una partición del conjunto G. Las particiones formadas por las relaciones de equivalencia a la derecha y de equivalencia a la izquierda son denotadas por:

$$G : S = G/\equiv_S$$
$$S : G = G/_S\equiv$$

Ejercicio 4.7

Demuestre que las relaciones de equivalencia a la izquierda y de equivalencia a la derecha son efectivamente relaciones de equivalencia.

El índice de un subgrupo en un grupo es el número de clases de equivalencia de la partición inducida las relaciones de equivalencia a la derecha y a la izquierda, es decir, el índice de un subgrupo en un grupo es el número de clases laterales de dichas relaciones de equivalencia.

Definición 4.6: Índice de un Subgrupo en un Grupo

Se define como el *Índice del Subgrupo S en el Grupo G*, denotado $i(S, G)$, a la cardinalidad del conjunto cociente $G : S$. Es decir,

$$i(S, G) = |S : G| = |G : S|.$$

Resulta que todas las clases laterales tienen la misma cardinalidad, y esa cardinalidad es igual al orden del subgrupo que define la relación de equivalencia a la derecha (y a la izquierda). De este hecho se desprende inmediatamente el Teorema de Lagrange.

Ejercicio 4.8

Demostrar que todas las clases laterales tienen la misma cardinalidad, y esa cardinalidad es igual al orden del subgrupo que define la relación de equivalencia a la derecha (y a la izquierda).

Teorema 4.2: Teorema de Lagrange

Sea $[S, \circ]$ un subgrupo de un grupo de orden finito $[G, \circ]$. Entonces,

$$|G| = |S||G : S|.$$

Demostración 4.3

Para la demostración del Teorema de Lagrange se demuestra que todas las clases laterales tienen la misma cardinalidad y que esta cardinalidad coincide con la cardinalidad del subgrupo S. Para esto, se prueba que existe una biyección entre las clases laterales y S. Para esta demostración, vamos a trabajar con clases laterales izquierdas. La demostración con las clases laterales derechas es similar y lleva al mismo resultado.
Dado un x cualquiera, se define la función $f : G \mapsto [x]$, que a cada elemento de G le asigna un elemento de la clase lateral de x, de la siguiente manera:

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

Ahora, se probará que la función f es biyectiva. Empecemos por la sobreyectividad. Dado $y \in [x]$, esto significa que $y = h \circ x$, para algún $h \in S$. Por lo que existe un elemento $h \in S$ tal que $f(h) = y$. Entonces, todo elemento en $[x]$ tiene una pre-imagen $h \in G$. La función f es sobreyectiva, en consecuencia.
Ahora, se probará que la función f es inyectiva. Suponemos que $f(h_1) = f(h_2)$, por lo que $h_1 \circ x = h_2 \circ x$. Como G es un grupo, el elemento x es cancelable por la derecha y en consecuencia $h_1 = h_2$. Hemos demostrado entonces que f es inyectiva y por ende biyectiva.
Como existe una biyección entre cualquier clase lateral $[x]$ y el conjunto S, quiere decir que ambos conjuntos tienen la misma cardinalidad, es decir, $|[x]| = |S|$. Esto es válido para todas las clases laterales. En consecuencia, la cardinalidad de todas las clases laterales es la misma cardinalidad de S y también se tiene que,

$$|G| = |S||S : G|$$

□

Corolario 4.1

Sea $[S, \circ]$ un subgrupo de un grupo de orden finito $[G, \circ]$. Entonces, el orden de S divide al orden de G.

4.3. Homomorfismos de Grupos

En el álgebra abstracta, los homomorfismos de grupo desempeñan un papel fundamental para comprender las relaciones entre distintas estructuras algebraicas conocidas como grupos. Los homomorfismos de grupo son importantes en áreas tales como: criptografía, teoría de la codificación (códigos correctores de errores), etc.

Definición 4.7: Homomorfismo de Grupo

Sean $[A, \circ]$ y $[B, *]$ Grupos. Entonces, una función $\phi : A \mapsto B$ se dice que es un *Homomorfismo* de $[A, \circ, e_A]$ a $[B, *, e_B]$ si,

$$\forall x, y \in X : \phi(x \circ y) = \phi(x) * \phi(y)$$

Al igual que en monoides, cuando el homomorfismo es biyectivo, se habla de Isomorfismo. Un Isomorfismo es una "correspondencia perfecta.^{en}tre dos grupos que conserva la forma en que se combinan sus elementos. Es como si re-etiquetáramos los elementos de un grupo sin alterar su estructura interna.

Definición 4.8: Isomorfismo de Grupo

Sea ϕ un Homomorfismo de los Grupos $[A, \circ, e_A]$ a $[B, *, e_B]$. Se dice que ϕ es además un *Isomorfismo de Grupos* si es una aplicación biyectiva.

Al identificar dos grupos isomorfos, podemos estudiar uno y aplicar los resultados al otro. A veces, podemos trabajar con un grupo isomorfo más simple para resolver un problema y luego traducir la solución al problema original. Los isomorfismos nos ayudan a comprender la esencia de un grupo, independientemente de su representación específica.

Cuando verificamos si una función es un homomorfismo de grupo, a diferencia de los homomorfismos de monoides, no es necesario verificar la condición de que la imagen a través del homomorfismo del neutro del grupo de partida es el neutro del grupo de llegada. Esta condición se verifica automáticamente gracias a la propiedad del inverso que tienen los grupos.

Lema 4.6

Si ϕ es un homomorfismo del grupo $[A, \circ, e_A]$ al grupo $[B, *, e_B]$, entonces la condición,

$$\phi(e_A) = e_B$$

se verifica automáticamente.

Demostración 4.4

$$e_A = e_A \circ e_A \implies \phi(e_A) = \phi(e_A \circ e_A) = \phi(e_A) * \phi(e_A).$$

Ahora, como $[B, *, e_B]$ es un grupo, existe $\phi(e_A)^{-1}$, por lo que sustituyendo y por asociatividad, se tiene,

$$e_B = \phi(e_A) * \phi(e_A)^{-1} = \phi(e_A) * (\phi(e_A) * \phi(e_A)^{-1}) = \phi(e_A) * e_b = \phi(e_A).$$

Gracias a la existencia del inverso tanto en el grupo de partida, como en el de llegada, es posible el lema siguiente:

Lema 4.7

Sea ϕ un homomorfismo del grupo $[A, \circ, e_A]$ al grupo $[B, *, e_B]$, entonces, para todo $x \in A$,

$$\phi(x^{-1}) = \phi(x)^{-1}.$$

Demostración 4.5

$$e_B = \phi(e_A) = \phi(x \circ x^{-1}) = \phi(x) * \phi(x^{-1})$$
$$e_B = \phi(e_A) = \phi(x^{-1} \circ x) = \phi(x^{-1}) * \phi(x)$$

es decir, que $\phi(x^{-1})$ verifica las propiedades del inverso de $\phi(x)$, y como el inverso en $[B, *, e_B]$ es único, entonces necesariamente $\phi(x)^{-1} = \phi(x^{-1})$.

4.3.1. Imagen y Núcleo de un Homomorfismo

Dos subgrupos que juegan un papel fundamental en la teoría de grupos son la Imagen de un Homomorfismo y el Núcleo (o Kernel) de un Homomorfismo.

Definición 4.9: Imagen de un Homomorfismo

Sea $\phi : A \mapsto B$ un homomorfismo del grupo $[A, \circ, e_A]$ al grupo $[B, *, e_B]$. La *Imagen* de ϕ (a veces llamada Imagen de A) se define como,

$$Im(\phi) = \{y \in B \mid \exists x \in A : y = \phi(x)\}$$

Lema 4.8

$[Im(\phi), *, e_B]$ es un subgrupo de $[B, *, e_B]$.

Demostración 4.6

1. $\phi(e_A) = e_B$, por lo que $Im(\phi) \neq \emptyset$.
2. Sean $x, y \in Im(\phi)$, entonces,
   a) $\exists a \in A : x = \phi(a)$,
   b) $\exists b \in A : y = \phi(b)$.

   Entonces,
   $$x * y^{-1} = \phi(a) * \phi(b^{-1}) = \phi(a \circ b^{-1}).$$
   Como A es un grupo, entonces $c = a \circ b^{-1} \in A$ y en consecuencia,
   $$x * y^{-1} = \phi(c) \in Im(\phi).$$

Definición 4.10: Núcleo de un Homomorfismo

Sea $\phi : A \mapsto B$ un homomorfismo del grupo $[A, \circ, e_A]$ al grupo $[B, *, e_B]$. El *Núcleo (o Kernel)* de ϕ se define como
$$\ker(\phi) = \{x \in A \mid \phi(x) = e_B\}.$$

Lema 4.9

$[\ker(\phi), \circ, e_A]$ es un subgrupo de $[A, \circ, e_A]$

Demostración 4.7

1. $\phi(e_A) = e_B$, por lo que $\ker(\phi) \neq \emptyset$.
2. Sean $x, y \in \ker(\phi)$,
   $$\phi(x \circ y^{-1}) = \phi(x) * \phi(y)^{-1} = e_B * e_B^{-1} = e_B^{-1} = e_B.$$
   por lo tanto $x \circ y^{-1} \in \ker(\phi)$.

Un homomorfismo es inyectivo si y sólo si su núcleo contiene sólo al elemento neutro deñ grupo de partida.

Lema 4.10

Sean $[G_1, *, e_1]$, $[G_2, \circ, e_2]$ grupos. Sea $\phi : G_1 \mapsto G_2$ un homomorfismo. Entonces,
$$\phi \text{ es inyectiva } \iff \ker(\phi) = \{e_1\}.$$

Demostración 4.8

1. La demostración ϕ es inyectiva $\implies \ker(\phi) = \{e_1\}$. es inmediata por reducción al absurdo, puesto que si existe una $x \neq e_1$, $x \in \ker(\phi)$ por inyectividad $x = e_1$.

2. Por otra parte, supongamos que para $x, y \in G_1$ se tiene que $\phi(x) = \phi(y)$. Entonces,

$$\begin{aligned} \phi(x * y^{-1}) &= \phi(x) \circ \phi(y^{-1}) \\ &= \phi(x) \circ \phi(y)^{-1} \\ &= \phi(x) \circ \phi(x)^{-1} \\ &= e_2. \end{aligned}$$

   De esto y por hipótesis deducimos que $x * y^{-1} = e_1$, en consecuencia $x = y$. Por lo tanto $\ker(\phi) = \{e_1\} \implies \phi$ es inyectiva.

4.4. Grupos de Permutación

Probablemente, el lector esté familiarizado con el concepto de Permutación, viéndolo en términos generales como una disposición de los miembros de un conjunto en un orden diferente al inicial. Una definición más formal de uan permutación sería la siguiente:

Definición 4.11: Permutación

Una *Permutación* de un conjunto X es una función biyectiva $f : X \mapsto X$.

Es decir, que una permutación es una transformación biyectiva. Al decir biyectiva, significa que hay una correspondencia biunívoca entre el conjunto X y su imagen a través de f. Si por ejemplo, se reordenaran los alumnos de un salón, eso sería una permutación y la función f asignaría a cada estudiante al estudiante que ubicaría su mismo lugar después del reordenamiento. Esta sería una permutación de un conjunto finito, porque el número de estudiantes del salón es un conjunto finito. Al conjunto de todas las permutaciones finitas de un conjunto X de n elementos se le llama $S_n(X)$ y su definición es la siguiente.

Definición 4.12: Conjunto de Permutaciones de un Conjunto Finito

Sea $X \neq \emptyset$, con $|X| = n$ (Conjunto finito no vacío). Se define,

$$S_n(X) = \{f \mid f : X \mapsto X, \text{ f biyectiva }\}.$$

S_n es el conjunto de las permutaciones de los n elementos de X.

Ejercicio 4.9: D

termine La cardinalidad de $S_n(X)$

El conjunto $S_n(X)$ con la operación de composición constituye un grupo muy importante, llamado Grupo de Permutación.

Lema 4.11: Grupo de Permutación

$[S_n(X), \circ, I_X]$ es un grupo, llamado *Grupo de Permutación*

Demostración 4.9

1. **L.C.I:** La composición de funciones biyectivas es una función biyectiva, por tanto una permutación. Por lo tanto, si $f, g \in S_n(X)$ entonces $f \circ g \in S_n(X)$.
2. **Asociativa:** La composición de funciones es asociativa.
3. **Elemento Neutro:** La función I_X es una permutación perteneciente a $S_n(X)$ y verifica,
$$I_X \circ f = f \circ I_X = f, \quad \forall f \in S_n(X).$$
4. **Elemento Simétrico o Inverso:** Si $f \in S_n(X)$, como la inversa de una función biyectiva es también una función biyectiva, entonces $f^{-1} \in S_n(X)$.

4.5. Teorema de Cayley (Grupos)

El teorema de Cayley de grupos, es un resultado fundamental en la teoría de grupos, que establece que todo grupo finito puede ser representado como un grupo de permutaciones. En otras palabras, cualquier grupo puede ser "visualizado" como un conjunto de reordenamientos de elementos.

Teorema 4.3: Teorema de Cayley

Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.

Demostración 4.10

Según el Teorema de Cayley para Monoides, todo Monoide es isomorfo a un Monoide de Transformación. En ese caso, el isomorfismo viene dado por la aplicación,

$$T_g(x) = x * g.$$

En el caso de que el monoide sea un grupo $[G, *]$, cada transformación T_g es una función biyectiva, y por lo tanto una permutación de los elementos de G. En efecto, para cada $g \in G$,

$$T_g(x) = T_g(y) \implies x * g = y * g,$$

y por la propiedad de cancelación se tiene que $x = y$, por lo que T_g es inyectiva. Además, para cualquier $y \in G$, se tiene que $y = T_g(x)$, con $x = y * g^{-1}$, por lo que la transformación es también sobreyectiva.

4.6. Grupos Abelianos

Muchos de los grupos con los que estamos familiarizados son conmutativos, en particular, los grupos aditivos y los grupos multiplicativos. A los grupos conmutativos se les denomina Abelianos en honor al matemático noruego Niels Abel, uno de los precursores de la teoría de grupos y quien fue el primero en demostrar que no existen soluciones algebraicas generales para las raíces de una ecuación polinómica de grado mayor a 4.

Definición 4.13: Grupo Abeliano

Si un grupo $[X, \circ]$ es Conmutativo, se dice que $[X, \circ]$ es un *Grupo Abeliano*.

Ejemplo 4.3

Algunos ejemplos de grupos abelianos son:

- $[\mathbb{R}, +, 0]$ es un grupo Abeliano.
- $[\mathbb{Z}, +, 0]$ es también un grupo Abeliano.
- $[\mathbb{R}, ., 0]$ ni siquiera es un grupo (el elemento 0 no tiene elemento simétrico)

Ejercicio 4.10

Dar un ejemplo de grupo no Abeliano.

4.6.1. Grupos Cíclicos

Uno de los tipos de grupos más simples son los Grupos Cíclicos. Los grupos cíclicos son generados por un sólo elemento y todas sus potencias. Las potencias de un elemento

se definen como:

Definición 4.14: Potencias de un elemento

De manera recursiva, se pueden definir las potencias de un elemento en un grupo de la siguiente manera: Para $n \in \mathbb{Z}^+$, se tiene,

$$a^0 = e,\ a^n = a \circ a^{n-1}$$

También se pueden definir las potencias negativas como, $a^{-n} = (a^n)^{-1}$.

Ejercicio 4.11

Probar que para todo $n \in \mathbb{Z}^+$ se verifica,

$$(a^{-n}) = (a^{-1})^n$$

Ahora que hemos definido lo que son las potencias de un elemento, incluyendo las potencias negativas y algunas de sus propiedades, definamos lo que es un grupo cíclico.

Definición 4.15: Grupo Cíclico

Un grupo $[G, *]$ se dice *Cíclico* si puede ser generado por un sólo elemento $a \in G$. Es decir si,

$$G = \langle a \rangle \ = \{a^k : k \in \mathbb{Z}\}$$

Los grupos generados por un elemento de un grupo G son subgrupos de G.

Lema 4.12

Sea $[G, *]$ un grupo. Sea $a \in G$. Entonces $\langle a \rangle$ es un subgrupo de G.

Demostración 4.11

1. $\langle a \rangle$ es subconjunto de G. Si no lo fuera, la operación $*$ en G no fuera cerrada.
2. Como $e = a^0$ entonces $\langle a \rangle \neq \emptyset$. Esto implica que el subconjunto $\langle a \rangle$ es no vacío.
3. Sean $x = a^n$ y $y = a^m$, entonces $x * y^{-1} = a^n * a^{-m} = a^{n-m} \in \langle a \rangle$.

Todo esto demuestra que $\langle a \rangle$ es un subgrupo de G.

Y no sólo el grupo generado por un elemento a es un subgrupo, sino que es el menor subgrupo de G que contiene al elemento a.

Lema 4.13

El grupo generado por el elemento a, $\langle a \rangle$, es el menor subgrupo de G que contiene a a.

Demostración 4.12

Por la propiedad de clausura, si S es un subgrupo de G que contiene a a, entonces debe contener a todas las potencias de a. Por lo tanto $\langle a \rangle \subseteq S$.

Definición 4.16: Orden de un elemento

El *Orden (Período)* de un elemento a de un grupo, es el entero positivo m más pequeño tal que $a^m = e$. Si no existe tal m se dice que a tiene *orden infinito*.

Los grupos cíclicos son abelianos, es decir conmutativos.

Lema 4.14

Todo grupo cíclico G es un grupo Abeliano.

Demostración 4.13: S

an $x = a^n$ y $y = a^m$, entonces,

$$x * y = a^n * a^m = a^{n+m} = a^{m+n} = a^m * a^n = y * x.$$

Salvo isomorfismos, existe exactamente un grupo cíclico para cada cantidad finita de elementos, y exactamente un grupo cíclico infinito. Por esta razón, los grupos cíclicos son considerados los más simples y han sido completamente clasificados.

Ejercicio 4.12

1. Dado el conjunto $G = \{0, 1, 2, \ldots, n-1\}$ y la operación en G definida como $a * b = a + b(\mod n)$. Demuestre que $[G, *]$ es un grupo cíclico.

2. Demuestre que el grupo cíclico $G, *$ es isomorfo a todos los grupos cíclicos de la misma cardinalidad.

4.7. Ejercicios adicionales de Grupos

Ejercicio 4.13

Demostrar que si $x \circ x = x$ en un grupo, necesariamente $x = e$.

Ejercicio 4.14

Dado $n \in \mathbb{N}$. Sea $n\mathbb{Z}$ el conjunto de números enteros múltiplos de n, definido de la siguiente manera,

$$n\mathbb{Z} = \{x \mid x = nz,\ z \in \mathbb{Z}\}.$$

Demuestre que $[n\mathbb{Z}, +, 0]$ es un subgrupo Abeliano de $[\mathbb{Z}, +, 0]$.

Ejercicio 4.15

Sea $H = \{2^n : n \in \mathbb{Z}\}$. Demuestre que $[H, ., 1]$ es un subgrupo del grupo multiplicativo $[\mathbb{Q}, ., 1]$.

Ejercicio 4.16

Sea $[S, *]$ un monoide y $G_S = \{s \in S \mid s \text{ es invertible}\}$. Probar que G_S es un grupo.

Ejercicio 4.17

Sea $[G, \circ]$ un grupo. Sean a, b, c elementos fijos de G. Demostrar que la ecuación

$$x \circ a \circ x \circ b \circ a = x \circ b \circ c,$$

tiene una solución y sólo una.

Ejercicio 4.18

Sea $[G, *]$ un grupo y sea $\sim$ la relación definida en G como:

$$x \sim y, \text{ si y sólo si, } \exists w \in G : y = w^{-1} * x * w.$$

Demuestre que $\sim$ es una relación de equivalencia en G.

Ejercicio 4.19

En un grupo con un número par de elementos, demostrar que existe al menos un elemento a distinto del neutro tal que $a^{-1} = a$.

Ejercicio 4.20

Demostrar que un grupo $[G, \circ]$ con 4 o menos elementos es forzosamente Abeliano. (Sugerencia: $b \circ a$ es uno de los siguientes: e, b, a, $b \circ a$)

Ejercicio 4.21

Dado un grupo $[G, *]$, definimos la estructura $[G, \circ]$ en donde la operación $\circ$ se define como $a \circ b = b * a$ para todo $a, b \in G$.

1. Demuestre que $[G, \circ]$ es también un grupo.
2. Se define la función $f : G \mapsto G$ de la siguiente manera $f(x) = x^{-1}$, para todo $x \in G$. Demuestre que f es un isomorfismo entre $[G, *]$ y $[G, \circ]$.

Ejercicio 4.22

Sea la estructura $[F, \circ]$, donde $F = \{f \mid f : \mathbb{R} \mapsto \mathbb{R}, f \text{ biyectiva }\}$ es el conjunto de funciones reales biyectivas, y la operación $\circ$ es la composición de funciones. Demuestre que $[F, \circ]$ es un Grupo. ¿Es un grupo Abeliano? ¿Por qué?.

Ejercicio 4.23

[Producto de Grupos] Sean los grupos $[A, \circ, e_A]$ y $[B, *, e_B]$. Se define la estructura $[P, \#]$, donde $P = A \times B$ (producto cartesiano de A y B) y la operación $\#$ se define como,

$$(a, b)\#(c, d) = (a \circ c, b * d).$$

1. Demuestre que $[P, \#]$ es un grupo.
2. Se dice que un grupo $[G_1, \circ]$ realiza a otro grupo $[G_2, *]$ si existe un homomorfismo inyectivo $f : G_2 \mapsto G_1$. Demuestre que $[P, \#]$ realiza tanto a $[A, \circ, e_A]$ como a $[B, *, e_B]$.

Ejercicio 4.24

Sea la estructura $[\mathbb{Z}_n, \#]$, donde el conjunto $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ y la operación $\#$ viene definida de la siguiente manera:

$$a\#b = \begin{cases} a+b & si \quad a+b < n \\ a+b-n & si \quad a+b \geq n. \end{cases}$$

Demuestre que $[\mathbb{Z}_n, \#]$ es un grupo.

Ejercicio 4.25

Demostrar que si en un grupo $[G, \circ]$, se cumple que, $x \circ x = e$ para todo $x \in G$, entonces el grupo es Abeliano.

Ejercicio 4.26

Sea una estructura asociativa $[G, *]$, con $G \neq \emptyset$, en el cual todas las ecuaciones $x * a = b$ y $a * y = b$ tienen soluciones $x, y \in G$. Demuestre que $[G, *]$ es un grupo.

Ejercicio 4.27

Sea $[G, \circ]$ un grupo. Demostrar que $(a \circ b)^n = a^n \circ b^n$ si y sólo si $[G, \circ]$ es Abeliano.

Ejercicio 4.28

Sea A un conjunto acotado, para el cual para todo $a, b \in A$ existe,

$$a \wedge b = \text{ínf}\{a, b\},$$
$$a \vee b = \sup\{a, b\}.$$

Determine si $[A, \wedge]$ y $[A, \vee]$ son grupos abelianos.

REFERENCIAS

[1] Birkoff, Garrett and McLane, Saunders. *Álgebra Moderna.* Traducido de la 12va edición inglesa. Editorial Vicens-Vives, Barcelona, 1963.

[2] Prather, Ronald. *Discrete Mathematical Structures for Computer Science.* Houghton, Mifflin Company. Boston, 1976.