



Universidad Nacional Autónoma de México
Facultad de Ingeniería



Estructuras Discretas

Grupo 6

Profesor: Orlando Zaldívar Zamorateguí

Equipo 4

Proyecto: Página Web

Tema: Semigrupos, Monoides y Grupos

Alumnos:

Navarro Rodriguez Angel Efren

Feria Ambriz Héctor Eduardo

Paz Rosas Jesús Eduardo

Toledo Durán Jesús Rodrigo

Semestre 2024-1

Temario

1. Objetivo
2. Introducción
3. Definiciones y conceptos
 - 3.1 Algebra básica
 - 3.2 Sistemas algebraicos
4. Semigrupos, Monoides y Grupos
 - 4.1 Operaciones binarias
 - 4.2 Grupo
 - 4.2.1 Grupos abelianos
 - 4.2.2 Grupos permutables
 - 4.2.3 Grupos diedrales
 - 4.2.4 Grupos cíclicos
 - 4.3 Semigrupos
 - 4.4 Monoides
 - 4.4.1 Monoide conmutativo
5. Ejemplos
6. Video
7. Cuestionario
8. Software
9. Bibliografía
10. Opinión del Usuario

1. Objetivo

El estudiante adquirirá conocimientos sobre cómo aplicar los conceptos de grupos, semigrupos y monoides en operaciones binarias, con el propósito de fomentar su habilidad para el pensamiento abstracto y lógico, además, de poder aplicar los conocimientos adquiridos y mejorar su comprensión de las estructuras matemáticas esenciales.



Imagen obtenida de: <https://foro.rinconmatematico.com/index.php?topic=103169.0>

Este tutorial tiene como objetivo abordar la comprensión del enfoque algebraico, junto con sus propiedades que hacen que su aplicación sea más efectiva y accesible para el estudiante en las situaciones que lo requiera.

2. Introducción

En el campo de la ingeniería informática, los grupos, semigrupos y monoides son conceptos matemáticos fundamentales que se emplean de manera extensa para resolver problemas en diversas disciplinas. Estos conceptos desempeñan un papel crucial en la solución de desafíos complejos en una amplia gama de aplicaciones informáticas, que incluyen la teoría de la computación, la criptografía, la teoría de lenguajes formales, la inteligencia artificial y otros campos.

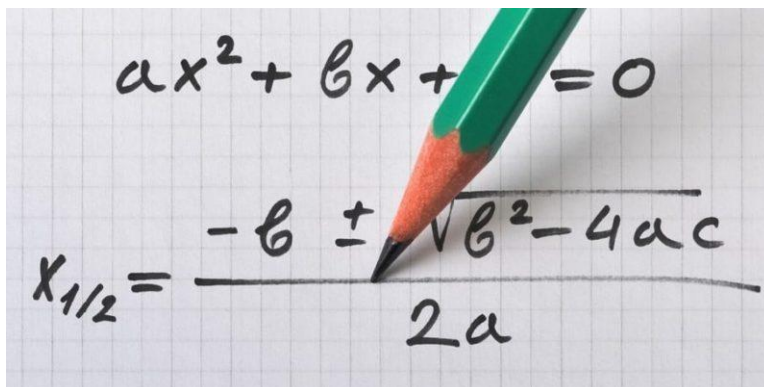


imagen obtenida de: <https://www.euroinnova.edu.es/cursos/ingenieria-informatica>

3. Definiciones y Conceptos

3.1 Álgebra básica

El álgebra es una disciplina matemática la cual se enfoca en investigar las relaciones existentes entre variables y las operaciones que se les aplican. Su objetivo principal es analizar las propiedades y operaciones relacionadas con números y expresiones utilizadas para la solución de ecuaciones.



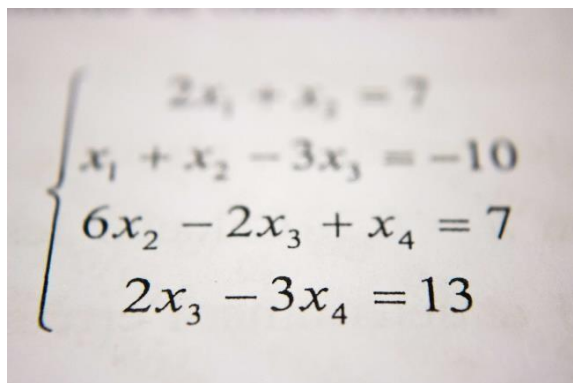
A photograph of a green pencil pointing to a handwritten quadratic equation and its solution formula on graph paper. The equation is $ax^2 + bx + c = 0$. Below it, the solution formula is written as $x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Imagen obtenida de: <https://concepto.de/algebra/>

En resumen, el álgebra nos capacita para abordar cuestiones abstractas relacionadas con grupos, semigrupos y monoides, y nos permite aplicar la lógica en el estudio de otras disciplinas como lo es en la asignatura de "Estructuras Discretas".

3.2 Sistemas algebraicos

Un sistema algebraico, en el contexto de las matemáticas, se convierte en una estructura que tiene aplicaciones en el análisis de las relaciones que existen entre dos o más variables. Estos sistemas pueden abarcar desde conjuntos finitos hasta infinitos, además, de ser una herramienta valiosa para resolver una amplia variedad de problemas matemáticos y científicos.



A photograph of a system of four linear equations in four variables, written as a set within a large left curly brace. The equations are: $2x_1 + x_2 = 7$, $x_1 + x_2 - 3x_3 = -10$, $6x_2 - 2x_3 + x_4 = 7$, and $2x_3 - 3x_4 = 13$.

Imagen obtenida de: <https://xn--deepinenespaol-1nb.org/wiki/sistema-algebraico-computacional/>

4. Semigrupos, Monoides y Grupos

4.1 Operaciones Binarias

Esta operación de importancia fundamental en el álgebra, implica tomar un par de números naturales y producir un resultado general. Esta característica es esencial para su aplicación en una amplia variedad de problemas y teorías en campos como las matemáticas y la informática. La operación binaria satisface dos condiciones básicas que son de gran relevancia en el estudio de estas estructuras matemáticas. Las cuales son:

- Aplicar un par de elementos con una naturaleza determinada.
- Asociar a dicho par con otro elemento con sus mismas características.

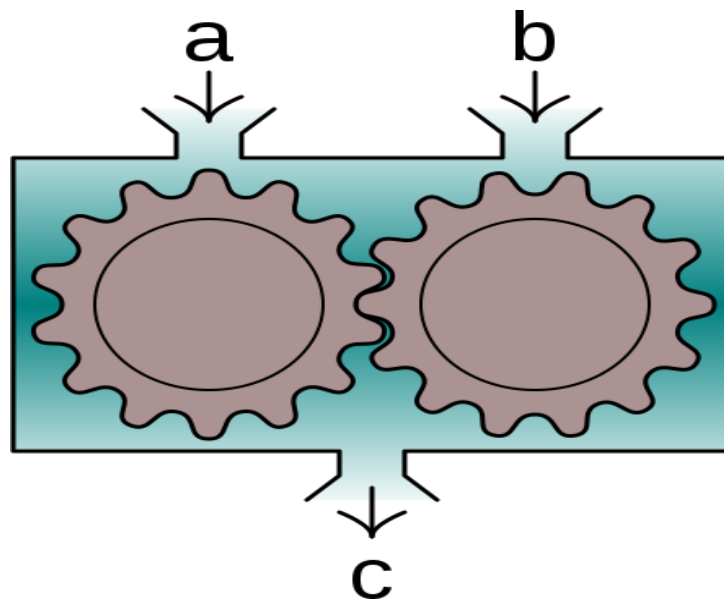


Imagen obtenida de:

https://es.m.wikipedia.org/wiki/Archivo:Operaci%C3%B3n_binaria_1.svg

4.2 Grupos

En matemáticas, un grupo es una estructura algebraica que consiste en un conjunto no vacío (denominado A) junto con una operación interna, representada por el símbolo '*'. Un grupo cumple con cuatro propiedades esenciales:

- 1. Propiedad de Clausura: Para cada par de elementos (x) e y de A, la composición $x*y$ debe resultar en un elemento de A. Esto se conoce como la propiedad de clausura.

- 2. Asociatividad: La operación '*' en el grupo debe ser asociativa, lo que significa que para cualquier terna de elementos x, y, z , se cumple que (yz) es igual a $(xy)*z$.
- 3. Elemento Neutro: Un grupo debe contener un elemento neutro 'e' para la operación '*', lo que significa que para cualquier elemento x de A , (xe) es igual a (x) y $(e*x)$ es igual a (x) . Este elemento neutro es único en la operación interna.
- 4. Elemento Inverso: Para cada elemento x en el grupo, debe existir un elemento 'y' (denominado elemento simétrico) tal que (xy) es igual a 'e' (el elemento neutro) y (yx) es igual a 'e'. Este elemento inverso es único en la operación.

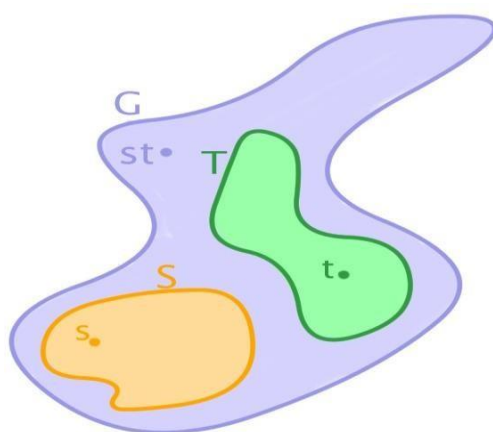


Imagen obtenida de: <https://blog.nekomath.com/algebra-moderna-i-producto-de-subconjuntos-y-clases-laterales/>

4.2.1 Grupos Abelianos

Un grupo abeliano, también conocido como grupo conmutativo, es un tipo especial de grupo en el que la propiedad de conmutatividad es fundamental. Esto significa que en un grupo abeliano, el orden de las operaciones no afecta el resultado. Para un grupo abeliano, se cumplen varias propiedades clave, como lo son:

- 1.- Conmutatividad: Para cualquier par de elementos a y b en el grupo, se cumple que: $ab = ba$.
- 2.- Asociatividad: Para cualesquiera tres elementos a, b , y c en el grupo, se cumple que $(ab)c = a(bc)$.
- 3.- Identidad: Hay un elemento en el grupo, denotado como 'e', que no cambia el valor de otro elemento cuando se multiplica por él. Es decir, para cualquier elemento a en el grupo se cumple que: $'ae' = 'ea' = 'a'$.

4.- Operación binaria: La operación que combina dos elementos del grupo para producir un tercer elemento también es un elemento del grupo.

5.- Distributividad: En un grupo abeliano, se satisface la propiedad de distributividad. La multiplicación de un elemento a por la suma de dos elementos b y c es igual a la suma de las multiplicaciones de a por b y a por c , es decir: $a \cdot (b + c) = ab + ac$.

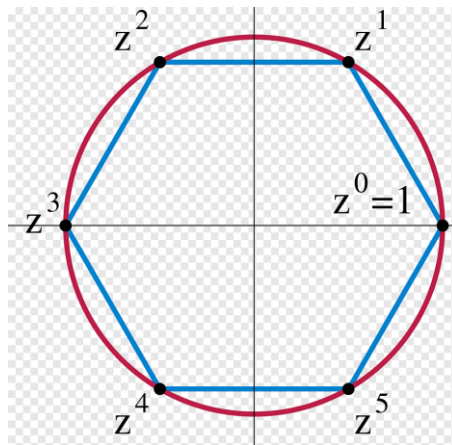


Imagen obtenida de: <https://www.pngegg.com/es/png-idcex>

4.2.2 Grupos Permutables

En el contexto de las matemáticas discretas, un punto de interés relevante es el estudio de las permutaciones dentro de los grupos. Esto se define como el conjunto de todas las permutaciones en un conjunto no vacío S bajo la operación binaria $*$. Este conjunto y su operación se denominan el grupo de permutaciones $(A, *)$.

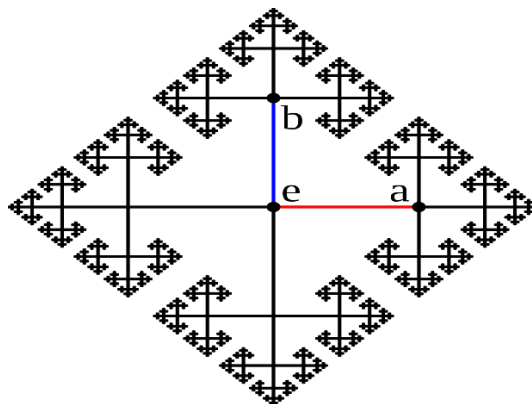


Imagen obtenida de: https://es.wikipedia.org/wiki/Teor%C3%ADa_de_grupos

4.2.3 Grupos Diedrales

Un grupo diedral se comprende como las transformaciones debidas a todos los movimientos rígidos de un polígono regular de ' n ' lados que resultan en polígonos idénticos, pero con vértices nombrados de manera diferente. Este grupo opera bajo la operación binaria de composición derecha '*', y se denomina el grupo diedral, representado por $(D_n, *)$. Los elementos de este grupo representan las simetrías y rotaciones de un polígono regular de ' n ' lados, y es un concepto fundamental en la geometría y la teoría de grupos. El grupo diedral ' D_n ' tiene ' $2n$ ' elementos, que corresponden a las diferentes simetrías y rotaciones posibles de un polígono regular de ' n ' lados.

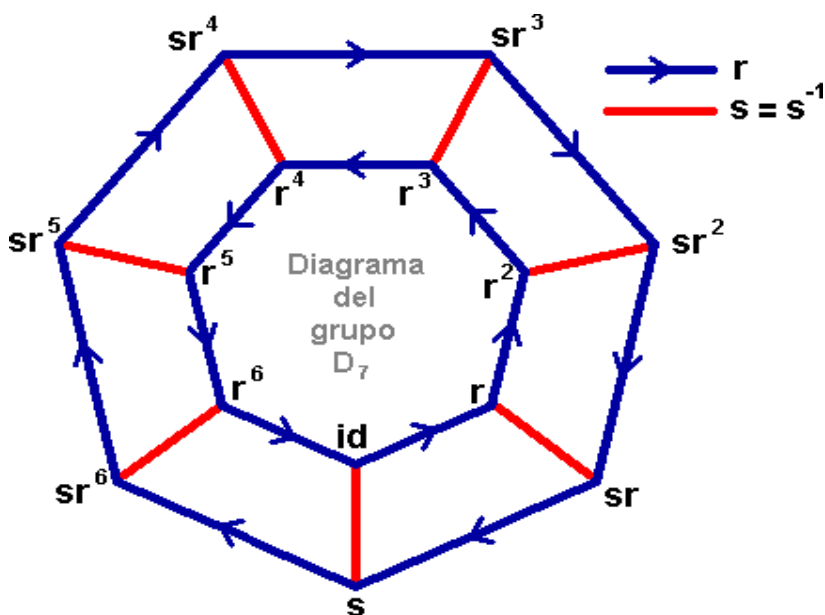


Imagen obtenida de: http://enciclopedia.us.es/index.php/Grupo_di%C3%A9drico

El grupo diédrico se puede representar como un conjunto de elementos cada uno de los cuales es una combinación de una reflexión y una rotación de un polígono o un poliedro regular. Por ejemplo, el grupo diédrico ' D_4 ' se puede representar como el conjunto de las siguientes operaciones:

- Identidad: *No se realiza ninguna operación.*
- Rotación: Giro de 90 grados en el sentido de las agujas del reloj.
- Reflexión: Giro en diagonal (*que refleja el objeto a lo largo de una línea que conecta dos vértices opuestos*).

4.2.4 Grupos Cíclicos

Un grupo se clasifica como cíclico si contiene un elemento especial, llamado generador, que tiene la propiedad de que todos los demás elementos del grupo se pueden representar como múltiplos de ese generador. Es decir, si se toma el generador 'a' y se eleva a diferentes potencias enteras, se obtendrán todos los elementos del grupo. A este grupo cíclico se le puede referir también por el símbolo $\langle a \rangle$, donde 'a' representa su generador.

$$\mathbb{Z}_3 = \{1, a, a^2\} = \\ = \langle a \mid a^3 = 1 \rangle$$

\cdot	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

Imagen obtenida de: https://www.ecured.cu/Grupo_c%C3%ADclico

En un grupo cíclico 'G' generado por un elemento 'a', todos los elementos de 'G' pueden expresarse como a elevado 'a' una potencia 'k', donde 'k' es un número entero. Cuando se multiplican elementos en este grupo, simplemente se suman los exponentes de 'a': $a^k * a^j = a^{(k+j)}$. Además, se ha establecido que todos los grupos cíclicos finitos tienen una estructura isomorfa a \mathbb{Z}'_n , el grupo de enteros módulo 'n'.

4.3 Semigrupos

Los semigrupos son estructuras matemáticas básicas que incluyen un conjunto y una operación binaria, y tienen diversas aplicaciones importantes. En esencia, si tomamos cualquier conjunto 'S' y una operación binaria '*' y esta operación cumple con la propiedad de asociatividad, entonces podemos considerar $(S, *)$ como un semigrupo.

En otras palabras, dado cualquier conjunto 'S' y una operación binaria '*' en 'S', si '*' satisface la propiedad asociativa, entonces $(S, *)$ es un semigrupo. Por ejemplo, el conjunto de números naturales con la operación de multiplicación forma un semigrupo, ya que la multiplicación es una operación binaria que es asociativa.

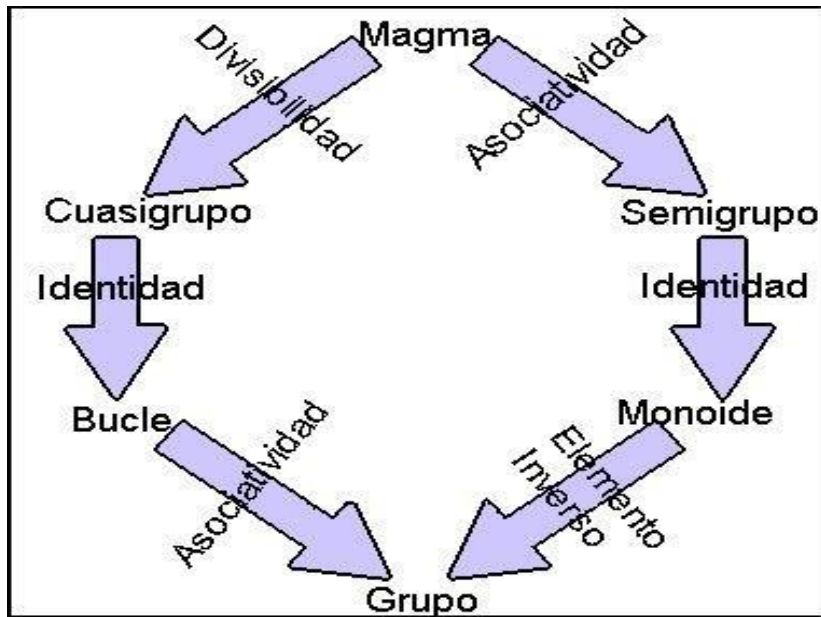


Imagen obtenida de: https://es.wikipedia.org/wiki/Magma_%28C3%A1lgebra%29

La propiedad *asociativa* es la única propiedad que se requiere para un semigrupo. Por lo tanto, un semigrupo no necesita tener elementos identidad ni elementos inversos. Si un semigrupo tiene un elemento identidad y todos sus elementos tienen inversos, entonces se le llama "grupo".

4.4 Monoides

Un monoide es una estructura matemática relacionada con los semigrupos. En términos sencillos, un monoide es una estructura algebraica que implica una operación binaria que es asociativa y que tiene un elemento neutro. Esto lo convierte en un tipo de semigrupo que incluye un elemento de identidad

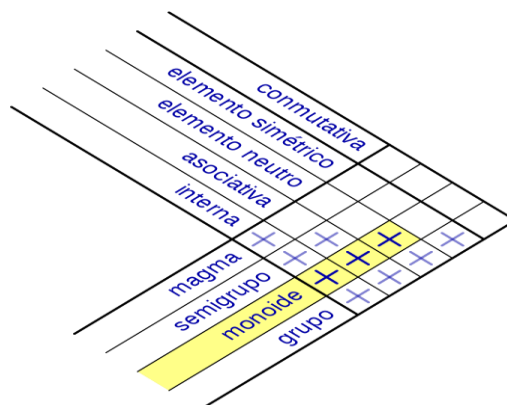


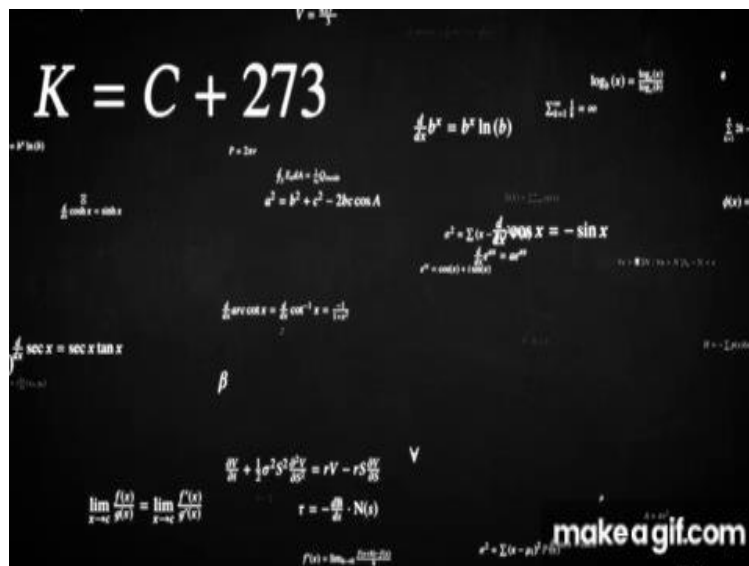
Imagen obtenida de: <https://en.wikipedia.org/wiki/Monoid>

Un conjunto 'S' en una operación binaria 'S x S' es un monoide si cumple los siguientes dos axiomas:

1. Tiene elementos idénticos: Por lo que existe un elemento 'e' dentro 'S' tal que por cada elemento 'a' dentro de 'S', las iguales $e \circ a = a$ y $a \circ e = a$.
2. Es asociativa: Para todo 'a', 'b' y 'c' dentro de 'S', la ecuación $(a.b)c \circ a.b.c$.

4.4.1 Monoide Conmutativo

En este conjunto, se define un orden algebraico en el cual se establece que $x' \leq y$ si existe un elemento 'z' que hace que la suma de 'x' y 'z' sea igual a 'y'. Una característica particular de este conjunto es la llamada "identidad conmutativa", que involucra la existencia de un elemento especial 'M'. Esta propiedad asegura que, para cualquier elemento 'z' perteneciente al conjunto, siempre se encontrará un elemento 'v' en el mismo conjunto que cumple con la relación $(w)x \leq v$.



Gif obtenido de: <https://makeagif.com//i>>

5. Ejemplos

1. Demostrar que si 'l' y 'd' son dos elementos neutros a izquierda y derecha respectivamente de un semigrupo (S,.), entonces (S,.) es un monoide, deducir que sí (S,.) tiene dos elementos neutros a izquierda distintos, entonces no existe ningún elemento de 'S' que sea elemento neutro a derecha.

Para este ejercicio se tiene que:

Paso 1

Cómo 'l' es neutro a izquierda , entonces:

$l \circ s = s$, Δs pertenece S, y como de es neutro a derecha

entonces $s' \circ d = s'$, $\Delta s'$ pertenece a S.

Paso 2

Ahora tomando en $l \circ s = d$, se obtiene:

$$l \circ d = d$$

Y tomando en $s' \circ d = l$, se obtiene:

$l \circ d = l$, por lo tanto de 3 y 4 deducimos:

$$s = l \circ d = l$$

Como los elementos neutro a la derecha e izquierda coinciden y, por tanto, existen en 'S' un elemento neutro, además, (S,..) es un semigrupo, entonces (S,..) es un semigrupo con elemento neutro, por lo tanto es un monoide.

Paso 3

Para ver la segunda parte supongamos por reducción que existe un elemento neutro a la derecha d1, entonces si l e l' son elementos neutros a izquierda distintos que existen en la primera parte del ejercicio, nos permite deducir que:

$$L = d1 \text{ y que } l' = d1$$

Paso 4

Luego $l=l'$ es una contradicción. Por lo tanto, no existe d1 elemento neutro a la derecha si hay dos elementos neutros e izquierda distintos.

Sea $S = \{(a_{ij}) \in \text{Mat}_{m \times m}(R) \mid a_{ij} = 1, 0 \text{ i,j} = 1, \dots, m\}$ y en S consideremos el producto usual de matrices.

Por lo tanto 'l' y 'd' son dos elementos neutros a izquierda y derecha respectivamente del semigrupo (S,.).

2. (a) Hallar un ejemplo de un grupo G infinito en el cual existe exactamente un elemento de orden 2.
 (b) Dar un ejemplo de un grupo G infinito en el cual todo elemento, salvo el neutro, tiene orden 2.

La resolución para este ejercicio es la siguiente:

Paso 1

(a) Sea $G = \mathbb{Z} \oplus \mathbb{Z}_2$, suponiendo las operaciones aditivas habituales en \mathbb{Z} y \mathbb{Z}_2

Se puede comprobar fácilmente que: $a = (0, 1)$ es el único elemento en G de orden 2; por ejemplo, todo elemento $(a, 1)$ con $a \neq 0$ tiene orden infinito.

Paso 2

(b) Sea G el conjunto de todas las sucesiones de números ± 1 :

$$G = \{x = (x_n)_{n=1}^{\infty} : x_n = -1 \text{ o } 1, \text{ para todo } n \in \mathbb{N}\}$$

Con la operación de multiplicación definida por coordenadas:

$$x \cdot y = (x_n \cdot y_n)_{n=1}^{\infty}$$

Paso 3

Es por ello que ' G ' es cerrado respecto a la operación definida, ya que $(\pm 1) \times (\pm 1) = (\pm 1)$

la multiplicación es asociativa y la sucesión estacionaria $1 = (1, 1, 1, \dots)$

actúa como neutro y cada elemento de ' G ' es su propio inverso, ya que: s

$$x \cdot x = ((\pm 1)^2)_{n=1}^{\infty} = 1$$

3. Dado el conjunto X y una aplicación T de X en X (es decir, t pertenece $M(X)$) se definen las potencias de exponente natural de T en la forma:

$$T^0 = 1_X$$

$$T^{n+1} = T^n \circ T, (n \text{ que pertenece a } \mathbb{N})$$

Demuestre la existencia de un monoide.

Para resolver este ejercicio los pasos son los siguientes:

Paso 1

De modo que $T^0 = 1_X$

$$T^1 = T^0 \circ T = 1_X \circ T = T$$

Paso 2

$$T^2 = T^1 \circ T = T \circ T$$

$$T^3 = T^2 \circ T = (T \circ T) \circ T = T \circ T \circ T$$

Paso 3

Por inducción se prueba que:

$$T^n \circ T^m = T^{n+m}$$

para todo n, m pertenece a N

Pongamos $(T) = (T^n \text{ y } n \text{ pertenece } N)$

.

Por lo que el par $((T), o)$ es un monoide; elemental unidad es $1x = T^0$

4. Si G es un grupo de orden par, demostrar que el número de sus elementos de orden 2 es impar.

Los pasos para resolver el ejercicio son los siguientes:

Paso 1

Los elementos de G pueden dividirse en dos clases disjuntas:

$$Q = \{x \in G : x^2 = e\} \text{ y } G \setminus Q. \text{ Si } x \in Q, \text{ entonces } x = x^{-1} \text{ y o } (x^{-1})^2 = e.$$

Paso 2

Por lo tanto, los elementos de Q van emparejados: cada x con su inverso x^{-1} es decir, hay un número par de ellos. Se sigue que el número de elementos en:

$$x \in G \setminus Q \text{ (para los cuales } x^2 = e) \text{ también es par.}$$

Paso 3

De todos ellos, solamente $x = e$ no es de orden 2.

Conclusión: G contiene un número impar de elementos de orden 2

5. Sea (S, \cdot) un monoide y $GS = \{s \in S \mid s \text{ es invertible}\}$. Probar que GS es un conjunto no vacío y que (GS, \cdot) es un grupo.

Este ejercicio se resuelve de la siguiente manera:

Paso 1

Empecemos por entender que GS es un conjunto no vacío porque el elemento neutro, que denotaremos por 1 , pertenece a GS ya que el elemento neutro es invertible.

Paso 2

Por otro lado, $GS \subseteq S$ y para todo $x, y \in GS$ (por tanto, x e y tienen elemento inverso en S , que denotamos por x^{-1} y y^{-1} , respectivamente).

A base de esto se cumple que $xy \in GS$ ya que el elemento xy tiene por inverso $y^{-1}x^{-1}$, que también pertenece a S .

Paso 3

Por tanto, el producto de S restringido a GS es una operación interna. Además, (GS, \cdot) es un semigrupo (por verificar la operación \cdot la propiedad asociativa en S), tiene elemento neutro, ya que 1 también pertenece a GS y por construcción cada elemento de GS tiene inverso, luego GS es un grupo.

Por lo que concluimos que GS es un GRUPO

6. Sea G un grupo un grupo abeliano; resolver en él la siguiente ecuación:

$$a \cdot b \cdot x^2 \cdot c = c \cdot x \cdot a$$

Por otro lado, si todos los elementos de G , excepto el elemento unidad, son de orden 3, demostrar que se verifica:

$$a \cdot (x^{-1} \cdot a \cdot x) = (x^{-1} \cdot a \cdot x) \cdot a$$

Siendo a un elemento de G y para todo x perteneciente a G .

Para resolver este ejercicio se aplican los siguientes pasos:

Paso 1

Como ya se indica que el grupo es conmutativo podemos escribir:

$$x \cdot c = c \cdot x; x \cdot a = a \cdot x$$

Paso 2

Además se comprueba que el conjunto es cerrado observando la tabla y para la propiedad conmutativa tenemos:

$$a \cdot b \cdot x^2 \cdot c = c \cdot x \cdot a \rightarrow a \cdot b \cdot x \cdot c \cdot x = \bullet = c \cdot a \cdot x \rightarrow a \cdot b \cdot x \cdot c = c \cdot a$$

O lo que es igual:

$$A \cdot b \cdot x \cdot c = a \cdot c \rightarrow a \cdot b \cdot x = a \rightarrow b \cdot x = e \rightarrow x = b^{-1}$$

Paso 3

Para demostrar la segunda parte del ejercicio, operamos a la derecha con $(x^{-1}ax)^2$, con lo cual:

$$A \cdot (x^{-1} \cdot a \cdot x)^3 = (x^{-1} \cdot a \cdot x) \cdot a (x^{-1}ax)(x^{-1}ax)$$

Y haciendo uso de la propiedad indicada en el enunciado:

$$A \cdot e = a = x^{-1} \cdot a \cdot x \cdot a \cdot x^{-1} \cdot a (x \cdot x^{-1}) a \cdot x = \bullet = x^{-1} (a \cdot x \cdot a) x^{-1} \cdot a^2 \cdot x$$

Paso 4

Pero por la misma propiedad indicada se tiene que:

$$x^3 = e \rightarrow x^{-1} = x^2; a^3 = e \rightarrow a^{-1} = a^2$$

Y, por lo tanto:

$$\begin{aligned} &= x \cdot x (a \cdot x \cdot a) x x \cdot a \cdot a \cdot x = x (x \cdot a)^2 x^2 a^2 x = \\ &x (x \cdot a)^{-1} x^2 a^2 x = x \cdot a^{-1} x^{-1} x \cdot a^2 \cdot x = x \cdot a^{-1} \cdot x \cdot a^2 \cdot x \end{aligned}$$

Con lo que, podemos concluir que:

$$A = x \cdot a^{-1} \cdot x \cdot a^{-1} \cdot x = (x \cdot a^{-1})^2 x = \bullet = (x \cdot a^{-1})^{-1} x = (a^{-1})^{-1} x^{-1} x = a$$

7. Demostrar que si 'l' y 'd' son dos elementos neutros a izquierda y derecha, respectivamente, de un semigrupo (S, \cdot) , entonces (S, \cdot) es un monoide. Deducir que si (S, \cdot) tiene dos elementos neutros a izquierda distintos, entonces no existe ningun elemento de S que sea elemento neutro a derecha.

La resolución de este ejercicio es la siguiente:

Paso 1

Como 'l' es neutro a izquierda, entonces:

$$l \cdot s = s, \forall s \in S$$

y como 'd' es neutro a derecha, entonces:

$$s \cdot d = s, \forall s \in S$$

Paso 2

Ahora, tomado en $(l) s = d$, se obtiene:

$$l \cdot d = d$$

y tomando en $s = l$, se obtiene:

$$l \cdot d = l$$

Paso 3

Por lo tanto: $s = l \cdot d = l$

Los elementos neutros a derecha e izquierda coinciden y es por ello que existe en 'S' un elemento neutro. Como además (S, \cdot) es un semigrupo, entonces (S, \cdot) es un semigrupo con elemento neutro, así que, el resultado es un monoide.

Paso 4

Para la segunda parte, por reducción existe un elemento neutro a derecha $d1$. Entonces, si l y l son los elementos neutros a izquierda distintos que existen, la primera parte del ejercicio nos permite deducir que:

$$l = d1$$

luego $l \neq l$, una contradicción.

Por lo tanto, no existe $d1$ elemento neutro a derecha si hay dos elementos neutros a izquierda distintos.

8. $A = (1, -1, i, -i)$ entonces (G, X) es un grupo cíclico con el generador i , para:

$$1 = i^4, -1 = i = i^1 \text{ y } i^{-1} = i^3$$

Para este grupo cíclico, $-i$ es también un generador

Determinar que el grupo cíclico es un abeliano

Para este ejemplo los pasos son los siguientes:

Paso 1

Podemos demostrar la existencia del grupo cíclico abeliano con lo siguiente:

$(A, *)$ es un grupo cíclico y pertenece a 'A' como generador, sea b, c pertenece a A, Entonces $b = a^m$ y $c = a^n$, donde m y n son enteros.

Paso 2

$$\begin{aligned} \text{En este caso } b * c &= a^m * a^n = a^{m+n} \\ &= a^{n+m} \end{aligned}$$

$$= a^n * a^m$$

$$= c * b$$

Por lo tanto, se demuestra la existencia del grupo cíclico abeliano en la operación algebraica.

9. Sea G un grupo y $H, K \leq G$ tales que $|H| = 38$ y $|K| = 55$. Demostrar que $H \cap K = \{e\}$

Los pasos para resolver este ejercicio son:

Paso 1

$H \cap K$ es un subgrupo tanto de H como de K . Por el Teorema de Lagrange deducimos que $|H \cap K|$ tiene que dividir tanto a $|H| = 38$ como a $|K| = 55$.

Paso 2

Pero $38 = 2 \times 19$ y $55 = 5 \times 11$ son coprimos.

asi que la única posibilidad es:

$$|H \cap K| = 1, \text{ es decir } H \cap K = \{e\}.$$

Por lo tanto, se demuestra que: $H \cap K = \{e\}$

10. Si $H \triangleleft G$ y el grupo G/H es cíclico, ¿es G necesariamente abeliano?

Para este ejercicio se tiene que:

Paso 1

Sea G el grupo diédrico de orden 6, en la notación de clase.

$$D_3 = \{I, A, A^2, B, AB, A^2B\} \text{ donde } A^3 = I = B^2 \text{ y } BA = A^{-1}B.$$

Paso 2

Sea $H = \{I, A, A^2\}$, el subgrupo cíclico generado por A . Siendo H un subgrupo de índice 2 en G , por un teorema visto en clase, es un subgrupo normal de G .

El grupo cociente G/H de orden 2 es obviamente cíclico. Sin embargo, el grupo G no es abeliano.

7. Cuestionario

A continuación, se presentan 50 preguntas, las cuáles la primera respuesta en **negritas** es la respuesta correcta.

- 1 ¿Qué es un grupo?
 - **"Un conjunto con una operación binaria y elementos neutros."**
 - "Un conjunto con una operación unaria y elementos neutros"
 - "Un conjunto con una operación ternaria y elementos neutros"
 - "Un conjunto con una operación binaria y elementos inversos"

- 2 ¿Cuál es la propiedad que define a un grupo?
 - **"Asociatividad"**
 - "Conmutatividad"
 - "Distributividad"
 - "Inversión"

- 3 ¿Cuál es la propiedad que define a un semigrupo?
 - **"Asociatividad"**
 - "Conmutatividad"
 - "Distributividad"
 - "Inversión".

- 4 ¿Cuál es la diferencia entre un grupo y un semigrupo?
 - **"Un grupo tiene elementos inversos y un semigrupo no"**
 - "Un semigrupo tiene elementos inversos y un grupo no"
 - "Un grupo es conmutativo y un semigrupo no"
 - "Un semigrupo es conmutativo y un grupo no"

- 5 ¿Qué es un monoide?
 - **" Un semigrupo con un elemento neutro"**
 - "Un grupo con un elemento neutro"
 - "Un semigrupo con elementos inversos"
 - "Un grupo con elementos inversos"

- 6 ¿Cuál es la propiedad que define a un monoide?
 - **"Asociatividad"**
 - "Conmutatividad"
 - "Distributividad"
 - "Inversión"

- 7 ¿Cuál es la relación entre grupos y semigrupos?
- **“Un grupo es un semigrupo con elementos inversos”**
 - “Un semigrupo es un grupo con elementos inversos”
 - “No hay relación entre grupos y semigrupos”
 - “Los grupos y semigrupos son lo mismo”
- 8 ¿Cuál es la relación entre grupos y monoides?
- **“Un grupo es un monoide con elementos inversos”**
 - “Un monoide es un grupo con elementos inversos”
 - “No hay relación entre grupos y monoides”
 - “Los grupos y monoides son lo mismo”
- 9 ¿Qué es un homomorfismo?
- **“Una función que preserva la estructura de grupo”**
 - “Una función que intercambia elementos del grupo”
 - “Una función que agrega elementos al grupo”
 - “Una función que elimina elementos del grupo”
- 10 ¿Qué es un isomorfismo?
- **“Un homomorfismo biyectivo”**
 - “Un homomorfismo inyectivo”
 - “Un homomorfismo sobreyectivo”
 - “Un homomorfismo que no es biyectivo”
- 11 ¿Cuál es la definición de subgrupo?
- **“Un subconjunto que es un grupo en sí mismo”**
 - “Un subconjunto que es un semigrupo en sí mismo”
 - “Un subconjunto que es un monoide en sí mismo”
 - “Un subconjunto que es un homomorfismo en sí mismo”
- 12 ¿Qué es un grupo abeliano?
- **“Un grupo conmutativo”**
 - “Un grupo no conmutativo”
 - “Un grupo con elementos inversos”
 - “Un grupo sin elementos inversos”

- 13 ¿Qué es un grupo simple?
- **“Un grupo que no tiene subgrupos propios”**
 - “Un grupo que tiene subgrupos propios”
 - “Un grupo abeliano”
 - “Un grupo conmutativo”
- 14 ¿Cuál es la definición de un semigrupo matemático?
- **“Un conjunto no vacío G con una operación binaria $*$ que satisface la cerradura y la asociatividad.”**
 - “Un conjunto vacío G con una operación binaria $*$ que satisface la cerradura y la asociatividad.”
 - “Un conjunto no vacío G con una operación binaria $+$ que satisface la cerradura y la asociatividad.”
 - “Un conjunto no vacío G con una operación binaria $*$ que satisface la cerradura, la asociatividad y la existencia del elemento neutro.”
- 15 ¿Cuál es la definición de un monoide matemático?
- **“Un conjunto no vacío G con una operación binaria $*$ que satisface la cerradura, la asociatividad y la existencia del elemento neutro.”**
 - “Un conjunto no vacío G con una operación binaria $*$ que satisface la cerradura, la asociatividad y la existencia del elemento inverso.”
 - “Un conjunto vacío G con una operación binaria $*$ que satisface la cerradura, la asociatividad y la existencia del elemento neutro.”
 - “Un conjunto no vacío G con una operación binaria $+$ que satisface la cerradura, la asociatividad y la existencia del elemento neutro.”
- 16 ¿Cuál es la propiedad asociativa en matemáticas?
- **“La propiedad de que el resultado de una operación binaria no depende del orden en que se realizan las operaciones.”**
 - “La propiedad de que el resultado de una operación binaria es el mismo independientemente de los operandos.”
 - “La propiedad de que el resultado de una operación binaria es el mismo que el operando neutro.”
 - “La propiedad de que el resultado de una operación binaria es el mismo que el inverso aditivo del operando.”

- 17 ¿Qué es el elemento neutro en un grupo matemático?
- **"Un elemento en el conjunto que, cuando se opera con cualquier otro elemento del conjunto, no cambia el valor de ese elemento."**
 - "Un elemento en el conjunto que es igual a su propio inverso aditivo."
 - "Un elemento en el conjunto que siempre produce un valor de 0 cuando se opera con cualquier otro elemento del conjunto."
 - "Un elemento en el conjunto que siempre produce un valor de 1 cuando se opera con cualquier otro elemento del conjunto."
- 18 ¿Qué es el inverso multiplicativo de un elemento en un grupo matemático?
- **"El elemento en el conjunto que, cuando se opera con el elemento original, produce el elemento neutro."**
 - "El elemento en el conjunto que es igual a su propio inverso aditivo."
 - "El elemento en el conjunto que siempre produce un valor de 0 cuando se opera con cualquier otro elemento del conjunto."
 - "El elemento en el conjunto que siempre produce un valor de 1 cuando se opera con cualquier otro elemento del conjunto."
- 19 ¿Qué es el orden de un elemento en un grupo matemático?
- **"El número más pequeño n tal que $a^n = e$, donde a es el elemento y e es el elemento neutro."**
 - "El número más grande n tal que $a^n = e$, donde a es el elemento y e es el elemento neutro."
 - "El número más pequeño n tal que $a^n = a$, donde a es el elemento y e es el elemento neutro."
 - "El número más grande n tal que $a^n = a$, donde a es el elemento y e es el elemento neutro."
- 20 "¿Qué es un subgrupo en un grupo matemático?
- **"Un subconjunto no vacío de un grupo que es cerrado bajo la operación y contiene el elemento inverso de cada elemento en el subconjunto."**
 - "Un subconjunto vacío de un grupo que es cerrado bajo la operación y contiene el elemento inverso de cada elemento en el subconjunto."
 - "Un subconjunto no vacío de un grupo que es cerrado bajo la operación y contiene el elemento neutro de cada elemento en el subconjunto."
 - "Un subconjunto no vacío de un grupo que es cerrado bajo la operación y no contiene el elemento neutro."

- 21 ¿Qué es un grupo abeliano o conmutativo?
- **"Un grupo en el que la operación es conmutativa, es decir, $a * b = b * a$ para cualquier a y b en el grupo."**
 - "Un grupo en el que la operación no es conmutativa, es decir, $a * b \neq b * a$ para algunos a y b en el grupo."
 - "Un grupo en el que todos los elementos tienen el mismo orden."
 - "Un grupo en el que todos los elementos tienen el mismo elemento inverso."
- 22 ¿Qué es un homomorfismo en un grupo matemático?
- **"Una función f que preserva la estructura del grupo, es decir, $f(a * b) = f(a) * f(b)$ para cualquier a y b en el grupo."**
 - "Una función f que transforma cada elemento del grupo en su inverso aditivo."
 - "Una función f que transforma cada elemento del grupo en su elemento neutro."
 - "Una función f que transforma cada elemento del grupo en su inverso multiplicativo."
- 23 ¿Qué es un isomorfismo en un grupo matemático?
- **"Un homomorfismo biyectivo, es decir, una función f que preserva la estructura del grupo y es uno a uno y sobre."**
 - "Un homomorfismo que no es biyectivo."
 - "Una función f que transforma cada elemento del grupo en su inverso aditivo."
 - "Una función f que transforma cada elemento del grupo en su elemento neutro."
- 24 ¿Qué es un grupo finito?
- **"Un grupo con un número finito de elementos."**
 - "Un grupo con un número infinito de elementos."
 - "Un grupo en el que todos los elementos tienen el mismo orden."
 - "Un grupo en el que todos los elementos tienen el mismo elemento inverso."
- 25 ¿Qué es un subgrupo generado por un conjunto en un grupo matemático?
- **"El subgrupo más pequeño que contiene el conjunto dado, es decir, el conjunto de todas las combinaciones lineales con coeficientes enteros de los elementos del conjunto dado."**
 - "El subgrupo más grande que contiene el conjunto dado, es decir, el conjunto de todas las combinaciones lineales con coeficientes enteros de los elementos del conjunto dado."
 - "El subgrupo generado por los elementos del conjunto dado y su inverso multiplicativo."
 - "El subgrupo generado por los elementos del conjunto dado y su inverso aditivo."

26 ¿Qué es un subgrupo normal en un grupo matemático?

- **"Un subgrupo que es cerrado bajo la operación y que satisface la propiedad de que si a es un elemento del subgrupo y g es cualquier elemento del grupo, entonces $g * a * g^{-1}$ está en el subgrupo."**
- "Un subgrupo que no es cerrado bajo la operación y que satisface la propiedad de que si a es un elemento del subgrupo y g es cualquier elemento del grupo, entonces $g * a * g^{-1}$ está en el subgrupo."
- "Un subgrupo que es cerrado bajo la operación y que satisface la propiedad de que si a es un elemento del subgrupo y g es cualquier elemento del grupo, entonces $g * a$ está en el subgrupo."
- "Un subgrupo que es cerrado bajo la operación y que satisface la propiedad de que si a y b son elementos del subgrupo, entonces $a * b$ está en el subgrupo."

27 ¿Qué es un grupo cociente en un grupo matemático?

- **"Un grupo que se forma al tomar un subgrupo normal de un grupo y considerar los cosets de ese subgrupo."**
- "Un grupo que se forma al tomar un subgrupo de un grupo y considerar los cosets de ese subgrupo."
- "Un grupo que se forma al tomar el conjunto de todos los elementos de un grupo que son iguales a su inverso multiplicativo."
- "Un grupo que se forma al tomar el conjunto de todos los elementos de un grupo que son iguales a su inverso aditivo."

28 ¿Qué es una clase lateral en un grupo matemático?

- **"El conjunto de elementos que se obtienen al multiplicar un elemento del grupo por un elemento dado de un subgrupo."**
- "El conjunto de elementos que se obtienen al multiplicar un elemento del grupo por un elemento dado que no está en el subgrupo."
- "El conjunto de elementos que se obtienen al multiplicar un elemento del subgrupo por un elemento dado del grupo."
- "El conjunto de elementos que se obtienen al multiplicar un elemento del subgrupo por un elemento dado que no está en el grupo."

- 29 ¿Qué es un conjunto generador en un grupo matemático?
- **"Un conjunto de elementos que puede generar todos los elementos del grupo mediante operaciones de la operación del grupo."**
 - "Un conjunto de elementos que puede generar algunos de los elementos del grupo mediante operaciones de la operación del grupo."
 - "Un conjunto de elementos que puede generar todos los subgrupos del grupo mediante operaciones de la operación del grupo."
 - "Un conjunto de elementos que puede generar algunos de los subgrupos del grupo mediante operaciones de la operación del grupo."
- 30 ¿Qué es un grupo libre en un grupo matemático?
- **"Un grupo en el que cualquier elemento se puede escribir de forma única como una combinación lineal de los elementos de un conjunto dado, sin restricciones adicionales."**
 - "Un grupo en el que cualquier elemento se puede escribir de forma única como una combinación lineal de los elementos de un conjunto dado, sujeto a restricciones adicionales."
 - "Un grupo en el que no se pueden escribir todos los elementos de forma única como una combinación lineal de los elementos de un conjunto dado."
 - "Un grupo en el que cualquier elemento se puede escribir como una combinación lineal."
- 31 ¿Qué es un homomorfismo en un grupo matemático?
- **"Una función entre dos grupos que preserva la estructura de grupo"**
 - "Una función entre dos grupos que cambia la estructura de grupo."
 - "Una función entre dos grupos que conserva algunos elementos del grupo, pero no otros." "Una función entre dos grupos que intercambia los elementos del grupo."
- 32 ¿Qué es un isomorfismo en un grupo matemático?
- **"Un homomorfismo entre dos grupos que es biyectivo."**
 - "Un homomorfismo entre dos grupos que no es biyectivo."
 - "Una función entre dos grupos que no preserva la estructura de grupo."
 - "Una función entre dos grupos que intercambia los elementos del grupo."
- 33 ¿Qué es un endomorfismo en un grupo matemático?
- **"Un homomorfismo de un grupo en sí mismo."**
 - "Un homomorfismo de un grupo en otro grupo."
 - "Una función que conserva algunos elementos del grupo pero no otros."
 - "Una función que intercambia los elementos del grupo."

- 34 ¿Qué es un auto morfismo en un grupo matemático?
- **"Un isomorfismo de un grupo en sí mismo."**
 - "Un isomorfismo de un grupo en otro grupo."
 - "Una función que conserva algunos elementos del grupo pero no otros."
 - "Una función que intercambia los elementos del grupo."
- 35 ¿Qué es un grupo abeliano?
- **"Un grupo en el que la operación binaria es conmutativa."**
 - "Un grupo en el que la operación binaria no es conmutativa."
 - "Un grupo en el que todos los elementos tienen un inverso."
 - "Un grupo en el que algunos elementos no tienen un inverso."
- 36 ¿Qué es un semigrupo?
- **"Un conjunto no vacío con una operación binaria asociativa."**
 - "Un conjunto no vacío con una operación binaria no asociativa."
 - "Un conjunto vacío con una operación binaria asociativa."
 - "Un conjunto vacío con una operación binaria no asociativa."
- 37 ¿Qué es un monoide?
- **"Un semigrupo con un elemento identidad."**
 - "Un semigrupo sin elemento identidad."
 - "Un grupo con un elemento identidad."
 - "Un grupo sin elemento identidad."
- 38 ¿Qué es un conjunto finito?
- **"Un conjunto con un número finito de elementos."**
 - "Un conjunto con un número infinito de elementos."
 - "Un conjunto vacío."
 - "Un conjunto con un número negativo de elementos."
- 39 ¿Qué es un conjunto infinito?
- **"Un conjunto con un número infinito de elementos."**
 - "Un conjunto con un número finito de elementos."
 - "Un conjunto vacío."
 - "Un conjunto con un número negativo de elementos."

- 40 ¿Qué es un conjunto no numerable?
- **"Un conjunto que no se puede poner en correspondencia uno a uno con los números naturales."**
 - "Un conjunto que se puede poner en correspondencia uno a uno con los números naturales."
 - "Un conjunto vacío."
 - "Un conjunto con un número negativo de elementos."
- 41 ¿Cuál es el orden del grupo de simetrías de un triángulo equilátero?
- **"6"**
 - "4"
 - "3"
 - "2"
- 42 ¿Cuál es el orden del grupo de permutaciones de un conjunto de n elementos?
- **" $n!$ "**
 - " n "
 - " $2n$ "
 - " 2^n "
- 43 ¿Qué es un subgrupo de un grupo?
- **"Un subconjunto no vacío de un grupo que es cerrado bajo la operación del grupo y que contiene el inverso de cada uno de sus elementos."**
 - "Un subconjunto no vacío de un grupo que no es cerrado bajo la operación del grupo y que no contiene el inverso de cada uno de sus elementos."
 - "Un subconjunto vacío de un grupo."
 - "Un subconjunto que no es un grupo."
- 44 ¿Qué es un submonoid de un monoide?
- **"Un subconjunto no vacío de un monoide que es cerrado bajo la operación del monoide y que contiene el elemento identidad."**
 - "Un subconjunto no vacío de un monoide que no es cerrado bajo la operación del monoide y que no contiene el elemento identidad."
 - "Un subconjunto vacío de un monoide."
 - "Un subconjunto que no es un monoide."

- 45 ¿Qué es un subsemigrupo de un semigrupo?
- **"Un subconjunto no vacío de un semigrupo que es cerrado bajo la operación del semigrupo."**
 - "Un subconjunto no vacío de un semigrupo que no es cerrado bajo la operación del semigrupo."
 - "Un subconjunto vacío de un semigrupo."
 - "Un subconjunto que no es un semigrupo."
- 46 ¿Cuál es la definición formal de un grupo?
- **"Un conjunto cerrado bajo una operación binaria, con la existencia de un elemento neutro y la existencia de inversos para cada elemento."**
 - "Un conjunto cerrado bajo una operación binaria, conmutativa y asociativa."
 - "Un conjunto cerrado bajo una operación binaria, conmutativa y distributiva."
 - "Un conjunto cerrado bajo una operación binaria, asociativa y distributiva."
- 47 ¿Cuál de las siguientes opciones es un ejemplo de monoide?
- **"El conjunto de números naturales con la operación de suma."**
 - "El conjunto de números enteros con la operación de multiplicación."
 - "El conjunto de números racionales con la operación de división."
 - "El conjunto de números reales con la operación de resta."
- 48 ¿Cuál de las siguientes opciones NO es un grupo?
- **"El conjunto de números enteros con la operación de multiplicación."**
 - "El conjunto de números racionales con la operación de división."
 - "El conjunto de números reales con la operación de suma."
 - "El conjunto de números complejos con la operación de suma."
- 49 ¿Cuál es la definición formal de un monoide?
- **"Un semigrupo con la existencia de un elemento neutro."**
 - "Un grupo con la existencia de un elemento neutro."
 - "Un conjunto cerrado bajo una operación binaria y conmutativa."
 - "Un conjunto cerrado bajo una operación binaria y distributiva."
- 50 ¿Cuál de las siguientes opciones es un ejemplo de semigrupo?
- **"El conjunto de números enteros con la operación de multiplicación."**
 - "El conjunto de números enteros con la operación de suma"
 - "El conjunto de números racionales con la operación de división."
 - "El conjunto de números naturales con la operación de resta."

8. Software

Bibliografía

- 1.- Martínez. C (2003). Curso de algebra lineal. Facultad de Ciencias. UNAM.

Es muy común denotar las operaciones binarias con el símbolo $*$, en lugar de f , y para denotar el elemento asignado a (a, b) se usa $a * b$ [en lugar de $f(a, b)$]. Se deberá recalcar que, si a y b son elementos en A , entonces, $a * b \in A$; y esta propiedad a menudo se describe diciendo que A es **cerrada** bajo la operación $*$.

Ejemplo 1 Sea $A = \mathbb{Z}$. Definase $a * b$ como $a + b$. Entonces, $*$ es una operación binaria en \mathbb{Z} .

Ejemplo 2 Sea $A = \mathbb{R}$. Se define $a * b$ como a/b . Entonces, $*$ no es una operación binaria, ya que no está definida para todo par ordenado de elementos de A . Por ejemplo, $3 * 0$ no está definida, pues no es posible dividir entre cero.

Ejemplo 3 Sea $A = \mathbb{Z}^+$. Se define $a * b$ como $a - b$. Entonces $*$ no es una operación binaria ya que no asigna un elemento de A a todo par ordenado de elementos de A ; por ejemplo, $2 * 5 \notin A$.

Ejemplo 4 Sea $A = \mathbb{Z}$. Se define $a * b$ como un número menor que a y b . Entonces, $*$ no es una operación binaria ya que no asigna un elemento **único** de A a cada par ordenado de elementos de A ; por ejemplo, $8 * 6$ podría ser 5, 4, 3, 1, etcétera. Por lo tanto, en este caso $*$ sería una relación de $A \times A$ a A pero no una función.

Ejemplo 5 Sea $A = \mathbb{Z}$. Se define $a * b$ como máximo $\{a, b\}$. Entonces, $*$ es una operación binaria; por ejemplo, $2 * 4 = 4$, $-3 * (-5) = -3$.

Ejemplo 6 Sea $A = P(S)$, para algún conjunto S . Si V y W son subconjuntos de S , se define $V * W$ como $V \cup W$. Entonces, $*$ es una operación binaria en A . Además, si se define $V * W$ como $V \cap W$, entonces, $*$ es otra operación binaria en A .

Como el ejemplo 6 indica, es posible definir muchas operaciones binarias en un mismo conjunto.

Ejemplo 7 Sea M el conjunto de todas las matrices booleanas. Se define $A * B$ (véase la sección 1.8) como $A \vee B$. Entonces, $*$ es una operación binaria. Esto también es verdadero para $A \wedge B$.

Ejemplo 8† Sea L una láttice. Se define $a * b$ como $a \wedge b$ (la máxima cota inferior de a y b). Entonces, $*$ es una operación binaria en L . Esto también es verdadero para $a \vee b$ (la mínima cota superior de a y b).

† Se usa material del capítulo 4.

•2.- Johnsonbaugh (1997). Matemáticas para la computación. JEAN.

11.7 Sea $(A, *)$ un semigrupo. Demuestre que para a, b, c en A , si $a * c = c * a$ y $b * c = c * b$, entonces $(a * b) * c = c * (a * b)$.

11.8 Sea $(\{a, b\}, *)$ semigrupo donde Demuestre $a * a = b$. que:

a) $a * b = b * a$

b) $b * b = b$

11.9 Sea $(A, *)$ un semigrupo conmutativo. Demuestre que si

$a * a = a$ y $b * b = b$, entonces

$(a * b) * (a * b) = a * b$.

11.10 Sea $(A, *)$ un semigrupo. Demuestre que si A es un conjunto finito, existe un a en A tal que

$a * a = a$.

11.11 Sea $(A, *)$ un semigrupo. Además, existe un elemento a en A tal que para todo x en A existen u y v en A que satisfacen la relación

$$a * u = v * a = x$$

Demuestre que existe un elemento identidad en A .

11.12 Sea $(A, *)$ un semigrupo y e una identidad izquierda. Además, para todo x en A existe un x en A tal que $\hat{x} * x = e$.

a) Demuestre que para todo a, b, c en A , si $a * b = a * c$, entonces $b = c$.

b) Demuestre que $(A, *)$ es un grupo, al demostrar que e es un elemento identidad.

Sugerencia: observe que $\hat{x} * x * \hat{x} * x = e$.

•3.- Rio, M. (2012). Matemáticas Discretas en la Ingeniería Aplicada. ECUARED

Sea (A, \star) un sistema algebraico con una identidad e . Sea a un elemento en A . Diremos que un elemento b es un *inverso por la izquierda* de a si $b \star a = e$. Diremos que un elemento b es un *inverso por la derecha* de a si $a \star b = e$. Por ejemplo, para el sistema algebraico de la figura 1.5, a es una identidad, así β es un inverso por la izquierda de γ , y δ es un inverso por la derecha de γ . Diremos que un elemento b es un *inverso* de a si éste es tanto un inverso por la izquierda como un inverso por la derecha de a . Es evidente que si b es un inverso de a , a también es un inverso de b . Por intuición afirmamos que un inverso de un elemento "cancela" el efecto del elemento cuando éstos se "combinan". Por ejemplo, sea (A, \star) un sistema algebraico, donde A es un conjunto de sustancias químicas: ácidos, bases y agua, y \star es una operación binaria dada como el producto de la combinación de dos sustancias químicas. En este caso, el agua puede considerarse como una sustancia química neutra, y el inverso de un ácido es una base, si su combinación produce agua.

Sea (A, \star) un sistema algebraico, donde \star es una operación binaria. Decimos que (A, \star) es un *grupo* si se satisfacen las siguientes condiciones:

1. \star es una operación cerrada.
2. \star es una operación asociativa.
3. Existe una identidad.
4. Todo elemento de A tiene un inverso por la izquierda.

Observemos que *debido a la asociatividad, un inverso por la izquierda de un elemento también es un inverso por la derecha del elemento en un grupo*. Sea b el inverso por la izquierda de a y c el inverso por la izquierda de b . Sea e la identidad. Dado que

$$(b \star a) \star b = e \star b = b$$

tenemos que

$$c \star ((b \star a) \star b) = c \star b = e$$

y a partir de

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

•4.- Skiba. Y. N (2012). Fundamentos de los métodos de computación en álgebra lineal. UNAM.

que, si x es cualquier elemento en S , entonces $x * x' = 0$).

5. Demuestre que la intersección de dos relaciones de congruencia en un semigrupo es una relación de congruencia.
6. Demuestre que la composición de dos relaciones de congruencia en un semigrupo no necesariamente es una relación de congruencia.
7. Examine el semigrupo $S = \{a, b, c, d\}$ con la siguiente tabla de multiplicación.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Examine la relación de congruencia $R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}$ en S .

- (a) Determine la tabla de multiplicación del semigrupo cociente S/R .
- (b) Determine el homomorfismo natural $f_R: S \rightarrow S/R$.
18. Examine el monoide $S = \{e, a, b, c\}$ con la siguiente tabla de multiplicación.

*	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	c	b	c
c	c	b	b	c

Examine la relación de congruencia $R = \{(e, e), (e, a), (a, e), (a, a), (b, b), (b, c), (c, b), (c, c)\}$ en S .

- (a) Determine la tabla de multiplicación del monoide cociente S/R .
- (b) Determine el homomorfismo natural $f_R: S \rightarrow S/R$.
19. Sea $A = \{0, 1\}$ examine el semigrupo libre A^* generado por A bajo la operación de concatenación. Sea N el semigrupo de todos los enteros no negativos bajo la operación de adición ordinaria.
 - (a) Verifique que la función $f: A^* \rightarrow N$, definida por $f(\alpha) =$ el número de dígitos en α , sea un homomorfismo.
 - (b) Sea R la siguiente relación en $A^*: \alpha R \beta$ si y sólo si $f(\alpha) = f(\beta)$. Demuestre que R es una relación de congruencia en A^* .
 - (c) Demuestre que A^*/R y N son isomorfos.

6.4 Grupos

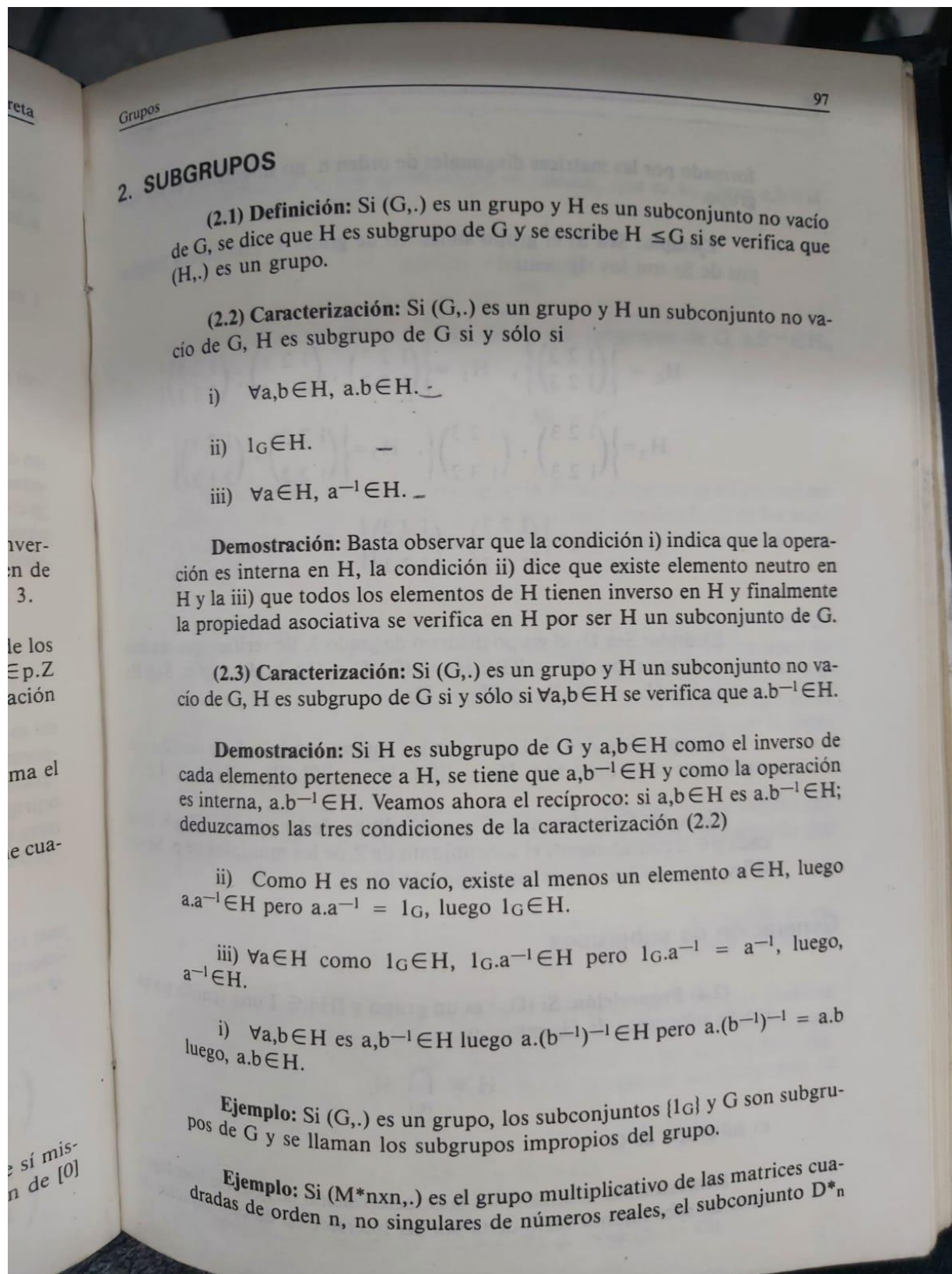
En esta sección se examinará un tipo especial de monoide, que se llama grupo, que tiene aplicaciones en todas las áreas donde ocurre la simetría. Las aplicaciones de los grupos pueden encontrarse en las matemáticas, la física y la química, así como en disciplinas menos exactas como la sociología. Muy recientemente las aplicaciones de la teoría de grupos surgieron en los quarks (astrofísica) y en la solución de acertijos tales como el cubo de Rubik. En este libro, se presentará una aplicación importante de la teoría de grupos en los códigos binarios de la sección 8.2.

Un **grupo** $(G, *)$ es un monoide, con idéntico e , que tiene la propiedad adicional de que, para cualquier elemento $a \in G$, existe un elemento $a' \in G$ tal que $a * a' = a' * a = e$. Por consiguiente, un grupo es un conjunto G con una operación binaria $*$ en G tal que

1. $(a * b) * c = a * (b * c)$ para elementos cualquiera $a, b, y c$ en G .
2. Existe un elemento único e en G tal que

$$a * e = e * a \quad \text{para cualquier } a \in G$$

5.- Busby. Ross (1997). Estructuras de Matemáticas Discretas para la Computación. Facultad de ingeniería. UNAM.



2. SUBGRUPOS

(2.1) Definición: Si (G, \cdot) es un grupo y H es un subconjunto no vacío de G , se dice que H es subgrupo de G y se escribe $H \leq G$ si se verifica que (H, \cdot) es un grupo.

(2.2) Caracterización: Si (G, \cdot) es un grupo y H un subconjunto no vacío de G , H es subgrupo de G si y sólo si

i) $\forall a, b \in H, a \cdot b \in H.$

ii) $1_G \in H.$

iii) $\forall a \in H, a^{-1} \in H.$

Demostración: Basta observar que la condición i) indica que la operación es interna en H , la condición ii) dice que existe elemento neutro en H y la iii) que todos los elementos de H tienen inverso en H y finalmente la propiedad asociativa se verifica en H por ser H un subconjunto de G .

(2.3) Caracterización: Si (G, \cdot) es un grupo y H un subconjunto no vacío de G , H es subgrupo de G si y sólo si $\forall a, b \in H$ se verifica que $a \cdot b^{-1} \in H$.

Demostración: Si H es subgrupo de G y $a, b \in H$ como el inverso de cada elemento pertenece a H , se tiene que $a \cdot b^{-1} \in H$ y como la operación es interna, $a \cdot b^{-1} \in H$. Veamos ahora el recíproco: si $a, b \in H$ es $a \cdot b^{-1} \in H$; deduzcamos las tres condiciones de la caracterización (2.2)

ii) Como H es no vacío, existe al menos un elemento $a \in H$, luego $a \cdot a^{-1} \in H$ pero $a \cdot a^{-1} = 1_G$, luego $1_G \in H$.

iii) $\forall a \in H$ como $1_G \in H$, $1_G \cdot a^{-1} \in H$ pero $1_G \cdot a^{-1} = a^{-1}$, luego, $a^{-1} \in H$.

i) $\forall a, b \in H$ es $a \cdot b^{-1} \in H$ luego $a \cdot (b^{-1})^{-1} \in H$ pero $a \cdot (b^{-1})^{-1} = a \cdot b$ luego, $a \cdot b \in H$.

Ejemplo: Si (G, \cdot) es un grupo, los subconjuntos $\{1_G\}$ y G son subgrupos de G y se llaman los subgrupos impropios del grupo.

Ejemplo: Si $(M^*_{n \times n}, \cdot)$ es el grupo multiplicativo de las matrices cuadradas de orden n , no singulares de números reales, el subconjunto D^*_n

•6.- Tremblay, J.P. & Manohar R. (2000). Matemáticas Discretas con aplicación a las Ciencias de la Computación. CECSA.

11.3 SUBGRUPOS

Sea (A, \star) un sistema algebraico y B un subconjunto de A . Diremos que el sistema algebraico (B, \star) es un subsistema de (A, \star) . La noción de subsistema es una muy natural. Supongamos que (A, \star) es un sistema algebraico que describe la interacción de un conjunto de partículas atómicas. Si estamos interesados en la interacción de algunas de las partículas, sólo podemos considerar un subsistema de (A, \star) . Sea $(N, +)$, un sistema algebraico que describe la adición

de números naturales. $(E, +)$ es un subsistema de $(N, +)$ si E es el conjunto de todos los números pares. De modo similar, consideremos el ejemplo de la rotación de figuras geométricas en un plano. Observemos que $(\{0^\circ, 120^\circ, 240^\circ\}, \star)$ es un subsistema del sistema algebraico $(\{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}, \star)$. Al igual que lo es $(\{0^\circ, 180^\circ\}, \star)$.

Sea (A, \star) un grupo, y B un subconjunto de A . Diremos que (B, \star) es un *subgrupo* de A si (B, \star) es a su vez un grupo. Supongamos que queremos verificar si (B, \star) es un subgrupo para un subconjunto B de A . Observemos que:

1. Debemos verificar si \star es una operación cerrada sobre B .
2. Se sabe que \star es una operación asociativa.
3. Debido a que sólo existe un elemento e en A tal que $e \star x = x \star e = x$ para todo x en A , debemos verificar que e está en B . En otras palabras, la identidad de (A, \star) debe estar en B como la identidad de (B, \star) .
4. Puesto que el inverso de cualquier elemento en A es único, para cualquier elemento b en B , debemos verificar que su inverso también está en B .

Por ejemplo, sea $(I, +)$ un sistema algebraico, donde I es el conjunto de todos los enteros y $+$ es la operación ordinaria de adición de enteros. Resulta claro que $(I, +)$ es un grupo. Además, $(E, +)$ es un subgrupo, donde E es el conjunto de todos los enteros pares. De igual

•7.- Zaldivar. F (2008). Introducción a la Teoría de Grupos. UNAM.

12.2 HOMOMORFISMOS, ISOMORFISMOS Y GRUPOS CICLICOS

De nuevo se considerarán las funciones que preservan estructura.

EJEMPLO 12.9 Sea $G = (\mathbb{Z}, +)$ y $H = (\mathbb{Z}_4, +)$. Defínase $f: G \rightarrow H$ por

$$f(x) = [x] = \{x + 4k | k \in \mathbb{Z}\}.$$

Para cualquier $x, y \in G$,

$$\begin{array}{ccccccc} f(x + y) & = & [x + y] & = & [x] + [y] & = & f(x) + f(y). \\ & & \uparrow & & & & \uparrow \\ & & \text{La operación en } G & & & & \text{La operación en } H \end{array}$$

Aquí f preserva las operaciones del grupo y es un ejemplo de homomorfismo de grupo. \square

Definición 12.4 \blacktriangleright Si (G, \circ) y $(H, *)$ son grupos y $f: G \rightarrow H$, f se denomina *homomorfismo de grupo* si para todo $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

Cuando se sabe que las estructuras dadas son grupos, la función f se denomina simplemente homomorfismo.

A continuación, se muestran algunas propiedades de los homomorfismos.

TEOREMA 12.5 \blacktriangleright Sean (G, \circ) , $(H, *)$ grupos con sus respectivas identidades e_G, e_H . Si $f: G \rightarrow H$ es un homomorfismo, entonces

- $f(e_G) = e_H$;
- $f(a^{-1}) = [f(a)]^{-1}$ para cualquier $a \in G$ y
- $f(S)$ es un subgrupo de H para cualquier subgrupo S de G .

Demostración

- $e_H * f(e_G) = f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$ de modo que, por el teorema 12.1.d), $f(e_G) = e_H$.
- La demostración de este apartado se deja al lector.
- Si S es un subgrupo de G , entonces $S \neq \emptyset$, de modo que $f(S) \neq \emptyset$. Sean $x, y \in f(S)$. Entonces, $x = f(a)$, $y = f(b)$ para $a, b \in S$. Como S es un subgrupo de G , $a \circ b \in S$ y $x * y = f(a) * f(b) = f(a \circ b) \in f(S)$. Por último, $x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S)$, pues $a^{-1} \in S$ cuando $a \in S$. En consecuencia, por el teorema 12.2, $f(S)$ es un subgrupo de H . \blacksquare

Definición 12.5 \blacktriangleright Si $f: (G, \circ) \rightarrow (H, *)$ es un homomorfismo, f se denomina *isomorfismo* si es uno a uno y suprayectiva. En este caso se dice que G y H son grupos isomorfos.

EJEMPLO 12.10 Sea $f: (\mathbb{R}^+, \cdot) \rightarrow (\mathbb{R}, +)$, donde $f(x) = \log_{10}(x)$. Esta función es uno a uno y suprayectiva. (Verifíquense estas propiedades.) Para $a, b \in \mathbb{R}^+$, $f(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = f(a) + f(b)$. Por tanto, f es un isomorfismo y el grupo de números reales positivos bajo la multiplicación es, en teoría, el mismo que el de todos los números reales bajo la suma. En este caso, la función f convierte un problema de multiplicación de

•8.- Briand.E (2007). Introducción a las Matemáticas Discretas. Universidad de Sevilla.

Sea \star una operación binaria sobre el conjunto A . Diremos que la operación \star es *asociativa* si

$$(a \star b) \star c = a \star (b \star c)$$

para todo a, b y c en A .[†] Sean A un conjunto de personas y \star una operación binaria tal que $a \star b$ es igual al más alto de a y b (supongamos que no hay dos personas de la misma estatura en A). Observemos que \star es una operación asociativa. Por otro lado, sean N el conjunto de todos los números naturales y $+$ una operación tal que $a + b$ es igual al valor de $a^2 + b$. El lector verificará que la operación $+$ no es asociativa. Afirmamos por intuición que cuando se tiene que llevar a cabo un cierto número de veces una operación asociativa, el orden en el cual se lleven a cabo las operaciones no es importante.

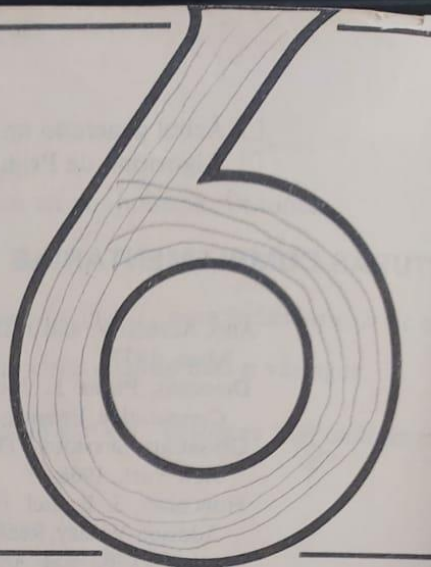
Sea (A, \star) un sistema algebraico donde \star es una operación binaria sobre A . Diremos que (A, \star) es un *semigrupo* si se satisfacen las siguientes condiciones:

1. \star es una operación cerrada.
2. \star es una operación asociativa.

Sea A el conjunto de todos los enteros pares positivos $\{2, 4, 6, \dots\}$ y $+$ la operación ordinaria de adición de enteros. Puesto que $+$ es una operación cerrada sobre A y también es una operación asociativa, entonces $(A, +)$ es un semigrupo. Sea S un alfabeto finito.

- 9.- Grimaldi, R. P. (1998) Matemáticas Discretas y Combinatoria: Una introducción con aplicaciones, México: Addison-Wesley Iberoamericana

Semigrupos y grupos



Requisitos previos: Capítulos 1, 2 y 3.

La idea de operación binaria en un conjunto de elementos se conoce ya desde el álgebra que se enseña en la educación media; por ejemplo, la suma y la multiplicación en el conjunto de todos los enteros. En este capítulo se tratarán las operaciones binarias desde un punto de vista más abstracto. Esto ayudará a desarrollar la noción de semigrupo, que se utilizará en el estudio de las máquinas de estado finito en el capítulo 7. Además se expondrán las ideas básicas de la teoría de los grupos, que se aplicarán en la teoría de la codificación en el capítulo 8.

6.1 Operaciones binarias

A pesar de que todos hemos trabajado durante años con operaciones binarias, será importante para el trabajo en este capítulo dar una definición precisa de esta idea fundamental.

Una **operación binaria** en un conjunto A es una función $f: A \times A \rightarrow A$. Obsérvense las siguientes propiedades que una operación binaria deberá satisfacer:

1. Puesto que $\text{Dom}(f) = A \times A$, f asigna un elemento $f(a, b)$ de A a cada par ordenado (a, b) de elementos de A . O sea la operación binaria deberá ser definida para cada par ordenado de elementos de A .
2. Como una operación binaria es una función, sólo un elemento de A se asigna a cada par ordenado (a, b) .

Por tanto, se puede decir que una operación binaria es una regla que a cada par ordenado de los elementos de A asigna un único elemento de A . A continuación se darán algunos ejemplos.

*Y obtener los teoremas
Para los Semigrupos*

- 10.- Liu, C.L. (1995). Elementos de Matemáticas Discretas. McGraw-Hill. P(296,297)

11. En \mathbb{R} , donde $a * b$ es $a \times |b|$.
12. En el conjunto de los números reales sin cero, donde $a * b$ es a/b .
13. En \mathbb{R} , donde $a * b$ es el mínimo de a y b .
14. En el conjunto de todas las matrices booleanas de $n \times n$, donde $A * B$ es $A \odot B$ (véase la sección 1.8).
15. En \mathbb{R} , donde $a * b$ es $ab/3$.
16. En \mathbb{R} , donde $a * b$ es $ab + 2b$.
17. En una látice A , donde $a * b$ es $a \vee b$.
18. En una látice A , donde $a * b$ es $a \wedge b$.
19. Complete la siguiente tabla de manera que la operación binaria $*$ sea conmutativa.

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

20. Examine la operación binaria $*$ definida en el conjunto $A = \{a, b, c, d\}$ por la siguiente tabla.

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

Calcule

- (a) $c * d$ y $d * c$
- (b) $b * d$ y $d * b$
- (c) $a * (b * c)$ y $(a * b) * c$
- (d) ¿ $*$ Es conmutativa?; ¿asociativa?

En los ejercicios 21 y 22, complete la tabla dada, de modo que la operación binaria $*$ sea asociativa.

21.

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

22.

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

23. Sea A un conjunto con n elementos.
 - (a) ¿Cuántas operaciones binarias pueden definirse en A ?
 - (b) ¿Cuántas operaciones binarias conmutativas pueden definirse en A ?
24. Sea $A = \{a, b\}$.
 - (a) Determine las tablas para cada una de las 16 operaciones binarias que pueden ser definidas en A .
 - (b) Determine las operaciones binarias en A que son conmutativas.
 - (c) Determine las operaciones binarias en A que son asociativas.
25. Sea $*$ una operación binaria en un conjunto A y suponga que $*$ satisface las propiedades de idempotencia, asociatividad y conmutatividad, como se explicó en el ejemplo 16. Defina una relación \leq en A por: $a \leq b$ si y sólo si $b = a * b$. Demuestre que (A, \leq) es un conjunto parcialmente ordenado y que para todas las a y b MCS (LUB) $(a, b) = a * b$.

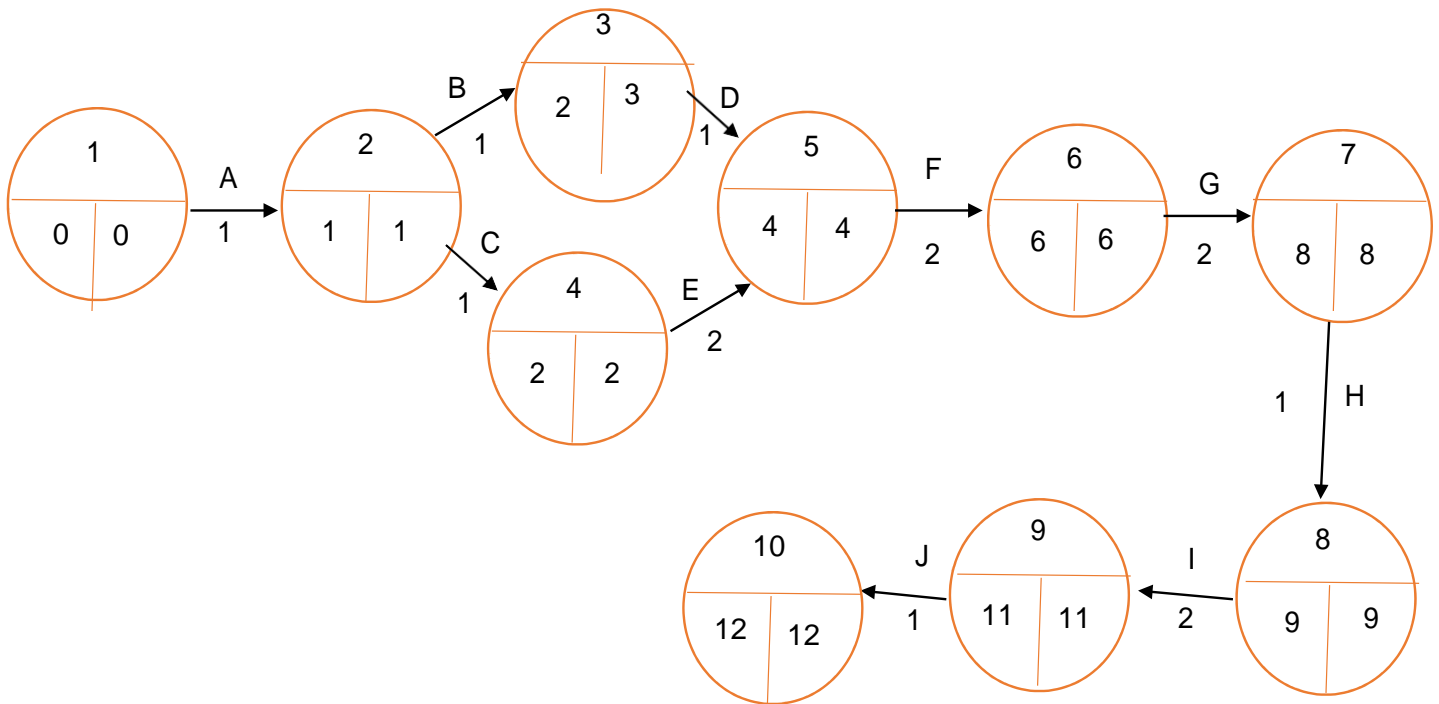
6.2 Semigrupos

En esta sección se definirá un sistema algebraico simple que consta de un conjunto y una operación binaria, y que tiene muchas aplicaciones importantes.

Un **semigrupo** es un conjunto no vacío S junto a una operación binaria asociativa $*$ definida en S . Se denotará el semigrupo por $(S, *)$ o cuando sea claro que la operación $*$ existe, sólo como S . También se llamará a $a * b$ **producto** de a y b . Se dice que el semigrupo $(S, *)$ es conmutativo si $*$ es una operación conmutativa.

Tarea

- A** Revisión de temas a investigar
- B** Recolección de información y fuentes de investigación el libros
- C** Planteamiento del objetivo y elaboración de la introducción
- D** Obtener y redactar las definiciones de conceptos para el tema
- E** Analizar y elaborar ejemplos prácticos sobre el tema
- F** Realizar las preguntas para el cuestionario en el tutorial
- G** Comenzar a realizar el tutorial con base a ejemplos de la plataforma
- H** Elaboración del software para implementarlo al tutorial
- I** Con toda la información lista, elaborar el documento formal donde se exponga el proyecto
- J** Un integrante del equipo realizará el video explicando paso a paso un ejemplo sobre el tema



Tarea	Tiempo optimista (O)	Tiempo probable (M)	Tiempo Pesimista (P)
1A	1 día	1 día	2 días
2B	1 día	2 días	3 días
3C	1 día	2 días	3 días
4D	1 día	2 días	3 días
5E	2 días	3 días	4 días
6F	2 días	3 días	4 días
7G	2 días	3 días	4 días
8H	1 día	2 días	3 días
9I	2 días	3 días	4 días