ESCUELA SUPERIOR POLITECNICA DEL LITORAL
INSTITUTO DE CIENCIAS MATEMATICAS

Matrices Cuadradas sobre el Campo de los Reales y Tres Estructuras Algebraicas Definidas Sobre Ellas

MONOGRAFIA

Previa a la Obtención del Título de:
Magister en Educación Matemática

Presentada por:

María Dolores Quiroga Montesinos

Guayaquil - Ecuador
1 9 9 4

AGRADECIMIENTO

La conclusión de un trabajo es una sensación placentera, pues atrás queda el tiempo invertido en investigación, elaboración y materialización del tema tratado.

Esta monografía no podría estar completa si no incluyera en ella mi agradecimiento especial a la Sra. Ing. ***Margarita Martínez de Jordán*** quien ha sido parte activa de este trabajo; pues, no se ha limitado a ser una fría correctora del tema tratado, sino, ha sido artífice de la forma y contenido que hoy tiene esta monografía.

Quiero también, dejar testimonio de mi agradecimiento a todos quienes forman el ***Instituto de Ciencias Matemáticas*** de la Escuela Superior Politécnica del Litoral.

DEDICADO A
MI MADRE Y HERMANO

INDICE GENERAL

INTRODUCCION

Una matriz es un arreglo rectangular de números. Estos arreglos se presentan en diversas ramas de las Matemáticas aplicadas. En muchos casos estan formados por coeficientes de transformaciones lineales o de sistemas de ecuaciones lineales que surgen, por ejemplo, en problemas relacionados con redes eléctricas, ajuste de curvas en Estadística y con el transporte. Las matrices son útiles porque permiten considerar a un arreglo de muchos números como un solo objeto, representado por medio de un solo símbolo y realizar cálculos con estos símbolos en una forma muy compacta. La "taquigrafía matemática" obtenida de este modo es muy elegante y poderosa, y resulta apropiada para diversos problemas prácticos; se introdujo a las Matemáticas aplicadas a la Ingeniería hace más de sesenta años y su importancia va en aumento en diversas ramas.

En este trabajo se presentan primero las matrices y los conceptos relativos, se definen las operaciones algebraicas para las matrices y se consideran los sistemas de ecuaciones lineales.(capítulo 1).

Luego en los capítulos dos, tres, y cuatro se presenta a las matrices con tres estructuras algebraicas definidas sobre ellas. Siendo el objetivo básico, proporcionar a los estudiantes de nivel medio un primer encuentro con el estudio del Algebra abstracta y así sembrar las semillas a partir de las cuales crecerá una actitud positiva hacia las Matemáticas.

CAPITULO 1 MATRICES CUADRADAS

1.1 INTRODUCCION

El término *matriz* , se mencionó por primera vez en la literatura matemática en un artículo de 1850 de *James Joseph Sylvester* (1814-1897). El significado usual no técnico de este término es <lugar donde algo se crea, produce o desarrolla>. Para Sylvester, entonces, una matriz, que era un <ordenamiento oblongo de términos>, era una entidad a partir de la cual uno podía formar varias porciones cuadradas para producir determinantes. Estas últimas cantidades, formadas a partir de matrices cuadradas, eran bastante bien conocidas en esa época y muy importantes.

Pero hoy las Matemáticas han cambiado y ahora son las matrtices más importante que los determinantes; por eso consideramos relevante conocer las matrices ylas operaciones entre ellas.

Este trabajo está diseñado para que los estudiantes se familiaricen con las matrices, sus operaciones y las estructuras que se forman sobre ellas.

1.2 DEFINICION DE MATRICES CUADRADAS

Sea R el conjunto de los numeros reales: una matriz n x n es un ordenamiento cuadrado, con n filas o renglones y n columnas, de números reales.

$$A=(a_{ij})=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \leftarrow \text{filas}$$

$\uparrow$ $\uparrow$

columnas

Si A es la matriz mostrada anteriormente, a los elementos a_{ij} se les llama componentes de A y a_{ij} recibe el nombre de componente ij, lo cual indica que es el elemento que se ubica en la fila i-ésima y la columna j-ésima.De suerte que (a_{ij}) será aquella matriz cuyo elemento i,j es a_{ij}

En todo lo que sigue, n será un entero fijo con la condición $n \geq 2$ y todas las matrices estarán en $M_n(R)$ donde $M_n(R)=\{(a_{ij}); a_{ij} \in R\}$,es el conjunto de todas las matrices de n x n sobre R

Es de resaltar que en general el número de filas no necesariamente es igual al número de columnas, pero para efectos de nuestro trabajo particular nos restringiremos a este caso. Dejamos al lector la inquietud de resolver cuanto de lo que aquí consta puede hacerse en el caso de matrices rectangulares.

1.3 OPERACIONES ENTRE MATRICES

Queremos introducir la noción de igualdad entre sus elementos, una operación binaria adición, una multiplicación escalar por elementos de R y otra operación binaria que es la multiplicación entre matrices, será de forma que se convierta en un álgebra sobre $M_n(R)$

A partir de aquí, no será necesario especificar que se está trabajando sobre R. Por consiguiente simplemente se hablará de matrices. La dimensión de una matriz está dada por el número de filas y columnas; en el caso de nuestras matrices cuadradas n x n, bastará con especificar n.

IGUALDAD DE MATRICES

DEFINICION 1

Sean (a_{ij}) y (b_{ij}) dos matrices de la misma dimensión; son iguales si y sólo si $a_{ij} = b_{ij}$ para toda i y para toda j. Si A y B son iguales, se escribe A=B. Si A no es igual a B se escribe A≠B

EJEMPLO 1. Las matrices A y B son iguales, pero ninguna es igual a C

$$A=\begin{bmatrix}2 & 4\\ 8 & 0\end{bmatrix}\quad B=\begin{bmatrix}2 & 4\\ 8 & 0\end{bmatrix}\quad \mathrm{C}=\begin{bmatrix}2 & 7\\ 8 & 3\end{bmatrix}$$

EJEMPLO 2 Las matrices M y N son iguales

$$M=\begin{bmatrix}x & y & 1\\ 0 & 8 & z\\ 0 & 1 & 1\end{bmatrix}=N=\begin{bmatrix}1 & 3 & 1\\ 0 & 8 & \pi\\ 0 & 1 & 1\end{bmatrix}\Leftrightarrow x=1, y=3, z=\pi$$

Una vez definida la igualdad de dos matrices se pasa al siguiente concepto, el de adición o suma de matrices.

SUMA DE MATRICES

DEFINICION 2

Sean $A = (a_{ij})$ y $B = (b_{ij})$ dos matrices.

Definimos $(a_{ij}) + (b_{ij}) = (c_{ij})$ donde $c_{ij} = a_{ij} + b_{ij}$ para toda i y para toda j

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{bmatrix}$$

Esto es, la suma de dos matrices es la matriz obtenida al sumar las entradas correspondientes. Para esto es necesario que las matrices tengan igual dimensión.

EJEMPLO 3 Hallar

$$\begin{bmatrix} 2 & 3 \\ -1 & 7 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

SOLUCION La suma es la matriz

$$\begin{bmatrix} 2+1 & 3+0 \\ -1+0 & 7+1 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ -1 & 8 \end{bmatrix}$$

EJEMPLO 4. Hallar

$$\begin{bmatrix} 3 & 5 \\ 6 & -1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

SOLUCION. La suma es la matriz

$$\begin{bmatrix} 3+0 & 5+0 \\ 6+0 & -1+0 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 6 & -1 \end{bmatrix}$$

Este ejemplo nos permite ver que si sumamos a una matriz, otra,cuyas entradas sean todas cero, el resultado será la misma matriz. Entonces definimos:

MATRIZ CERO

DEFINICION 3

Sea 0 la matriz con todos sus registros iguales a cero.

Como es evidente en el ejemplo 4

$$A+0=0+A=A$$

Como vemos esta matriz actúa como elemento neutro de la suma

¿ Y qué es un elemento neutro?

Es aquél que permite que al operar con él, el elemento original quede igual, no haya variación.

EJEMPLO 5. Hallar

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \end{bmatrix} + \begin{bmatrix} 2 & 4 & 7 \\ 3 & 5 & 8 \\ 1 & 6 & 0 \end{bmatrix}$$

SOLUCION. La suma no está definida pues las matrices no tienen la misma dimensión.

En el teorema 1 se presentan las propiedades básicas de la suma de matrices.

Las propiedades conmutativas, asociativas y del elemento identidad se siguen fácilmente de las definiciones y de las correspondientes propiedades para los números reales.

TEOREMA 1 Sean A, B y C matrices. Sea 0 la matriz cero. Entonces.

i) A+0=A (Propiedad de la existencia de la identidad aditiva).

ii) A+B=B+A (Propiedad conmutativa de la adición).

iii) A+(B+C)=(A+B)+C (Propiedad asociativa de la adición).

Demostración

i) A+0=A (identidad aditiva).

El elemento nulo, llamado en este caso la matriz cero, es la matriz cuyos registros son todos iguales a cero. Es claro, entonces, que si 0 es la matriz cero, A+0=A para todo $A \in M_n(R)$.

ii) A+B=B+A (conmutativa de la adición).

Sean $A = (a_{ij})$ y $B = (b_{ij})$

Por la definición de suma de matrices,

$$A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

Puesto que la suma de los números reales es conmutativa,

$$(a_{ij} + b_{ij}) = (b_{ij} + a_{ij})$$

Finalmente, de la definición de suma de matrices,

$$(b_{ij} + a_{ij}) = (b_{ij}) + (a_{ij}) = B + A$$

Por lo tanto A+B=B+A.

iii) A+(B+C)=(A+B)+C (asociativa de la adición).

Sean $A = (a_{ij})$, $B = (b_{ij})$ y $C = (c_{ij})$

$$A + (B + C) = (a_{ij}) + [(b_{ij}) + (c_{ij})]$$

$$= (a_{ij}) + (b_{ij} + c_{ij}), \text{ por definicion de suma de matrices}$$
$$= (a_{ij} + (b_{ij} + c_{ij})), \text{ por definicion de suma de matrices}$$
$$= ((a_{ij} + b_{ij}) + c_{ij}), \text{ por la asociatividad de los numeros reales}$$
$$= (a_{ij} + b_{ij}) + (c_{ij}), \text{ por la definicion de suma de matrices}$$
$$= [(a_{ij}) + (b_{ij})] + (c_{ij}), \text{ por definicion de suma de matrices}$$
$$= (A + B) + C$$

La suma A+A siempre está definida, puesto que A y A tienen la misma dimensión. Resulta razonable escribir A+A como 2A. Considérese el ejemplo siguiente:

EJEMPLO 6

Sea $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Entonces $A + A = \begin{bmatrix} a+a & b+b \\ c+c & d+d \end{bmatrix} = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$

Este ejemplo sugiere la definición de la multiplicación por escalar. Al trabajar con matrices, frecuentemente nos referimos a los números reales como escalares.

MULTIPLICACION POR UN ESCALAR

DEFINICION 4

Sean $A = (a_{ij})$ y r un escalar ,definimos $r(a_{ij}) = (b_{ij})$ donde $b_{ij} = ra_{ij}$ para toda i y para toda j.

EJEMPLO 7 Hallar

$$(\pi)\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 6 \\ 1 & -1 & 4 \end{bmatrix}$$

SOLUCION. Al multiplicar por(π) cada registro de la matriz obtenemos la siguiente matriz

$$\begin{bmatrix} \pi & 2\pi & 3\pi \\ 0 & \pi & 6\pi \\ \pi & -\pi & 4\pi \end{bmatrix}$$

EJEMPLO 8 Hallar

$$(-1)\begin{bmatrix} 1 & 3 \\ 8 & 2 \end{bmatrix}$$

SOLUCION. El resultado de multiplicar una matriz por el escalar (-1) es la matriz (-1)A=-A

$$\begin{bmatrix} -1 & -3 \\ -8 & -2 \end{bmatrix}$$

DIFERENCIA ENTRE MATRICES.

DEFINICION 5

Sean A y B matrices, escribimos A+(-1)B como A-B y llamaremos a esto la diferencia entre A y B.

TEOREMA 2 Sean A y B matrices y 0 la matriz cero. Sean c y d escalares arbitrarios y 0 y 1 los escalares identidad de la suma y multiplicación, respectivamente. Entonces

i) c(A+B)=cA+cB

ii) (c+d)A=cA+dA

iii) (cd)A=c(dA)

iv) 1A=A

v) $0A=0_{n\times n}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$, donde 0 es el número real nulo.

La suma y multiplicación de un escalar por una matriz nos parece naturales pero la definición del producto de matrices que vamos a dar parecerá peculiar y poco natural. La explicación típica que se da en álgebra lineal para esta definición muestra cómo las corresponden a ciertas funciones, llamadas transformaciones lineales; en consecuencia el producto de matrices corresponde a la composición de transformaciones lineales. También puede darse otra explicación en términos de sistemas de ecuaciones lineales. Dar un tratamiento siguiendo estos lineamientos nos obligaría a profundizar demasiado en el álgebra lineal, por lo que solamente daremos la regla para multiplicar matrices sin más justificación para esta operación.

MULTIPLICACION DE MATRICES

DEFINICION 6

Sean las matrices $A=(a_{ij})$ y $B=(b_{ij})$, de la misma dimensión entonces la matriz producto AB es la matriz

$C=(c_{ij})$, en donde $(c_{ij})=\sum_{k=1}^{n}a_{ik}b_{kj}=a_{i1}b_{1j}+a_{i2}b_{2j}+\ldots+a_{in}b_{nj}$

Obsérvese que el subíndice k sobre el cual se desarrolla la suma que precede es un índice ficticio (o mudo). Bien se podría denotar con cualquier otro símbolo.

Note también que AB sólo se puede definir cuando el número de columnas de A es igual al número de filas de B. Observemos también que la entrada i,j de C se obtiene usando la i-ésima fila de A y la j-ésima columna de B. Así

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nj} & \cdots & b_{nn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & c_{ij} & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

EJEMPLO 9. Calcular el producto.

$$\text{Si } A = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \text{ y } B = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}, \text{ entonces } AB = \begin{bmatrix} 1(4)+2(1) & 1(1)+2(3) \\ 3(4)+5(1) & 3(1)+5(3) \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 17 & 18 \end{bmatrix}$$

Una manera de recordar cómo se forma el producto AB es la siguiente:

El componente s,t es el "producto punto" de la s-ésima fila de A por la columna t-ésima de B.

En el caso aludido, por ejemplo, el componente 2,1 es el producto punto 3(4)+5(1) de la fila 2=(3,5) de A y (4,1) que es la columna 1 de B escrita horizontalmente.

EJEMPLO 10. Consideremos la matriz de dimensión n x n

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \qquad \text{así } I = (i_{su}) \begin{cases} 1, & s = u \\ 0, & s \neq u \end{cases}$$

Esta matriz especial se llama la *matriz identidad n x n.* Siempre que deseemos especificar su dimensión explícitamente, la denotamos I_n ,así por ejemplo:

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ y } I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Ahora consideremos A, una matriz cuadrada arbitraria de la misma dimensión que la matriz identidad. Entonces el producto AI_n está definido $(a_{ij}) = \sum_{k=1}^{n} a_{ik} i_{kj}$

Lo mismo podemos decir para el producto $I_n A$ que esta definido por $a_{ij} = \sum_{k=1}^{n} i_{ik} a_{kj}$

De esta manera $AI_n = I_n A = A$ para toda $A \in M_n(R)$.

Las matrices no satisfacen la ley conmutativa de la multiplicación ; es decir, AB no es necesariamente igual a BA.

Recuerdese, también que con las matrices es posible que AB=0 pero $A \neq 0$ y $B \neq 0$.

EJEMPLO 11 Calcular AB y BC si

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ y } \quad C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

SOLUCION. Tenemos:

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

$$BC = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

Pero lo que si satisfacen en la multiplicación de matrices es la ley asociativa y la ley distributiva respecto a la adición de matrices, es decir:

TEOREMA 3 Sean A, B y C matrices. Entonces:

i) A(BC)=(AB)C

ii) A(B+C)=AB+AC

iii) (A+B)C=AC+BC

Le sugerimos al lector que pause en cada demostración; realice ejemplos concretos y se asegure de entenderla, antes de pasar al siguiente literal.

Demostración

i) A(BC)=(AB)C

Sean

$A=(a_{ij})$, $B=(b_{ij})$, $C=(c_{ij})$, $AB=D=(d_{ij})$, $BC=E=(e_{ij})$, $(AB)C=F=(f_{ij})$ y $A(BC)=G=(g_{ij})$

Ahora bien,

$$f_{ij}=\sum_{k=1}^{n}d_{ik}c_{kj}=\sum_{k=1}^{n}\left(\sum_{r=1}^{n}a_{ir}b_{rk}\right)c_{kj}$$

y

$$g_{ij}=\sum_{r=1}^{n}a_{ir}e_{rj}=\sum_{r=1}^{n}a_{ir}\left(\sum_{k=1}^{n}b_{rk}c_{kj}\right)$$

Entonces

$$f_{ij}=\sum_{k=1}^{n}\left(a_{i1}b_{1k}+a_{12}b_{2k}+\cdots+a_{in}b_{nk}\right)c_{kj}$$

$$=a_{i1}\sum_{k=1}^{n}b_{1k}c_{kj}+a_{i2}\sum_{k=1}^{n}b_{2k}c_{kj}+\cdots+a_{in}\sum_{k=1}^{n}b_{nk}c_{kj}$$

$$=\sum_{r=1}^{n}a_{ir}\left(\sum_{k=1}^{n}b_{rk}c_{kj}\right)=g_{ij}$$

COMENTARIO Una vez que se ha estudiado detalladamente por qué es cierta la ley asociativa (AB)C=A(BC), el lector puede apreciar que equivale a mostrar que los elementos (i,j) de las matrices (AB)C=A(BC) son las sumas dobles.

$$\sum_{k=1}^{n}\sum_{r=1}^{n}(a_{ir}b_{rk})c_{kj} \quad \text{y} \quad \sum_{r=1}^{n}\sum_{k=1}^{n}a_{ir}\left(b_{rk}c_{kj}\right)$$

Estas sumas dobles son iguales porque el orden sumatorio no afecta a la suma y porque los términos $(a_{ir}b_{rk})c_{kj}$, $a_{ir}\left(b_{rk}c_{kj}\right)$ son iguales en virtud de la ley asociativa de los números.

En vista de que (AB)C=A(BC), pueden suprimirse los paréntesis en los productos de tres matrices -dado que se genera el mismo resultado con las agrupaciones- y expresar cualquiera de los productos como ABC, para A, B y C en $M_n(R)$

ii) A(B+C)=AB+AC

Se demostrará la primera de las leyes de la distribución. La demostración de la segunda es idéntica y por tanto se omite.

Supóngase que $A=\left(a_{kj}\right)$, $B=\left(b_{kj}\right)$ y $C=\left(c_{kj}\right)$.

La kj-ésima componente de B+C es $b_{kj}+c_{kj}$

La ij-ésima componente de A(B+C) es

$$\sum_{k=1}^{n}a_{ik}\left(b_{kj}+c_{kj}\right)=\sum_{k=1}^{n}a_{ik}b_{kj}+\sum_{k=1}^{n}a_{ik}c_{kj}$$

Que es igual a la ij-ésima componente de AB más la ij-ésima componente de AC y esto demuestra la parte ii)

1.4 MATRICES ESPECIALES.

En esta breve sección se desea definir otra sencilla operación sobre matrices y presentar ciertos tipos especiales de matrices que tienen importancia práctica

TRANSPUESTA DE UNA MATRIZ

DEFINICION 7

Si $A = (a_{rs}) \in M_n(R)$, entonces la transpuesta de A, denota por A', es la matriz $A' = (b_{rs})$, en donde $b_{rs} = a_{sr}$ para todo r y s.

$$\text{Si } A = (a_{rs}) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \text{ entonces } A' = (a_{sr}) = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{bmatrix}$$

En virtud de la definición, la fila r de la matrtiz transpuesta A' es la columna r de la matriz original A, y viceversa.

Se puede también obtener A' por reflexión de A con respecto a su diagonal principal, o sea la de elementos a_{ii}

EJEMPLO 12 Hallar A' si

$$A = \begin{bmatrix} 1 & 4 \\ -3 & 2 \end{bmatrix}$$

SOLUCION. Tenemos:

$$A' = \begin{bmatrix} 1 & -3 \\ 4 & 2 \end{bmatrix}$$

Obsérvese que las filas de A se convierten en las columnas de A'

EJEMPLO 13 Hallar A' si

$$A = \begin{bmatrix} 2 & 4 & 0 \\ -1 & 3 & 2 \\ -3 & 1 & 2 \end{bmatrix}$$

SOLUCION. Tenemos:

$$A' = \begin{bmatrix} 2 & -1 & -3 \\ 4 & 3 & 1 \\ 0 & 2 & 2 \end{bmatrix}$$

Debido a su trascendencia, a continuación se enumeran formalmente varias propiedades básicas de la transposición de matrices.

TEOREMA 4 Si A y B son matrices y a y b están en R, entonces

i) (A')'=A"=A;(transpuesta de la transpuesta)

ii) (aA+bB)' =aA' + bB';(transpuesta de una combinación lineal)

iii) (AB)' = B'A' (transpuesta de un producto)

Demostración. Las partes i) y ii) son muy sencillas y se dejan al lector. Se prueba la parte iii).

Sean $A = (a_{ij})$ y $B = (b_{ij})$; sea $AB = C = (c_{ij})$.

Debemos probar que c_{ij}' es la entrada (i,j) de B'A'.

Ahora bien,

$$c_{ij}' = c_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki} = \sum_{k=1}^{n} a_{kj}' b_{ik}' = \sum_{k=1}^{n} b_{ik}' a_{kj}' = \text{la entrada (i,j) de B'A'.}$$

Por consiguiente (AB)' = B'A'

MATRIZ SIMETRICA

DEFINICION 8

Se dice que una matriz A es simétrica si A' = A

EJEMPLO 14 Hallar A' si

$$A=\begin{bmatrix}1 & \pi\\ \pi & 0\end{bmatrix}$$

SOLUCION. Tenemos

$$A'=\begin{bmatrix}1 & \pi\\ \pi & 0\end{bmatrix}$$

EJEMPLO 15 Hallar A' si

$$A=\begin{bmatrix}-3 & 1 & 5\\ 1 & 0 & -2\\ 5 & -2 & 4\end{bmatrix}$$

SOLUCION. Tenemos

$$A'=\begin{bmatrix}-3 & 1 & 5\\ 1 & 0 & -2\\ 5 & -2 & 4\end{bmatrix}$$

MATRIZ ANTISIMETRICA

DEFINICION 9

Se dice que una matriz A es antisimétrica si A'=-A

EJEMPLO 16

$$Si\ \ A=\begin{bmatrix}0 & \pi\\ -\pi & 0\end{bmatrix}\ \text{entonces}\ A'=\begin{bmatrix}0 & -\pi\\ \pi & 0\end{bmatrix}$$

EJEMPLO 17

$$Si\ \ A=\begin{bmatrix}0 & -4 & 1\\ 4 & 0 & -5\\ -1 & 5 & 0\end{bmatrix}\ \text{entonces}\ A=\begin{bmatrix}0 & 4 & -1\\ -4 & 0 & 5\\ 1 & -5 & 0\end{bmatrix}$$

MATRIZ TRIANGULAR

DEFINICION 10

Una matriz cuadrada se denomina ***triangular superior*** si todas sus componentes debajo de la diagonal son cero. Es ***Triangular inferior*** si todas sus componentes por encima de la diagonal son cero. Es decir, $A = (a_{ij})$ es triangular superior si $a_{ij} = 0$ para i>j. Y es triangular inferior si $a_{ij} = 0$ cuando i<j.

EJEMPLO 18

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 3 & 0 \\ 5 & 0 & 2 \end{bmatrix} \text{ y } A_2 = \begin{bmatrix} 1 & 6 & -1 \\ 0 & 2 & 3 \\ 0 & 0 & 4 \end{bmatrix}$$

MATRIZ DIAGONAL

DEFINICION 11

Una matriz A cuyos elementos arriba y abajo de la diagonal principal son todos ceros, es decir, $a_{ij} = 0$ para todo $i \neq j$, se conoce como matriz diagonal.

EJEMPLO 19

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -4 \end{bmatrix}$$

MATRIZ ESCALAR

DEFINICION 12

Una matriz diagonal se denomina escalar si todos los componentes de la diagonal principal son iguales.

Por ende una matriz escalar tiene la forma

$$A=\begin{bmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & a_{ii} & 0 \\ 0 & 0 & 0 & a \end{bmatrix}$$

en donde a es un número.

Veamos porque este tipo de matrices reciben este nombre. Sean

$A=\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ y $B=\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$ matrices de la misma dimensión ,entonces

el producto $AB=\begin{bmatrix} ab_1+0b_3 & ab_2+0b_4 \\ 0b_1+ab_3 & 0b_2+ab_4 \end{bmatrix}=\begin{bmatrix} ab_1 & ab_2 \\ ab_3 & ab_4 \end{bmatrix}$

Pero observamos que esta matriz se puede escribir también como el producto del escalar ***a*** que está en la diagonal principal por la matriz B. Sean

$a \in R$ y una matriz $B=\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$ entonces $aB=\begin{bmatrix} ab_1 & ab_2 \\ ab_3 & ab_4 \end{bmatrix}$

Entonces, aunque son dos operaciones diferentes, en este caso, las dos operaciones nos dan como resultado la misma matriz.

Como podemos observar AB=aB por eso es que esta matriz recibe el nombre de escalar, porque actúa como escalar sin ser precisamente un escalar.

MATRIZ INVERSA

DEFINICION 13.

Una matriz B se llama inversa de una matriz cuadrada A si AB=BA=I.Dicha matriz B se denota por A^{-1}.

Decimos que una matriz A es *inversible o no singular* si tiene inversa.Sin embargo, una matriz A puede no tener inversa, en cuyo caso se llama *no inversible o singular.*

TEOREMA 5 Si una matriz A es inversible, entonces la inversa de A es única.

Demostración. Supóngase que la matriz A es inversible y que B y C son inversas de A. Entonces

BA=AB=I y CA=AC= I

Considérese ahora el producto CAB en dos formas haciendo uso de la ley asociativa de la multiplicación:

C(AB)=CI=C y (CA)B=IB=B

Puesto que C(AB)=(CA)B, se tiene que C=B, de modo que la inversa es úninca.

TEOREMA 6. Si dos matrices A y B son inversibles, entonces AB es inversible y $(AB)^{-1} = B^{-1}A^{-1}$

Demostración: Sean A^{-1} y B^{-1} las inversas de A y B, respectivamente. Puesto que

$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = (AI)A^{-1} = AA^{-1} = I$

Y

$(B^{-1}A^{-1})(AB) = (B^{-1}(A^{-1}A))B = (B^{-1}I)B = B^{-1}B = I$

$B^{-1}A^{-1}$ es la inversa de AB. Por lo tanto, $(AB)^{-1} = B^{-1}A^{-1}$ y AB es inversible

1.5 APLICACIONES

Existen al menos cinco razones de por qué las matrices son importantes en las ciencias matemáticas.

1. Surgen al resolver problemas de sistemas de ecuaciones lineales.

2. Las matrices son un buen recurso para almacenar información que viene naturalmente con índices en dos variables. Esto es especialmente cierto en los negocios, la economía y las ciencias de la computación.

3. Muchos fenómenos físicos son lineales o casi lineales en su naturaleza y las matrices aparecen en las descripciones matemáticas de esos fenómenos.

4. Las matrices son una herramienta valiosa para la teoría de las gráficas.

5. El conjunto de las matrices cuadradas tienen una estructura algebraica muy rica, que tiene interés en sí misma y es fuente de inspiración para el estudio de estructuras algebraicas más abstractas. Esto lo veremos en los capítulos siguientes de este trabajo.

Para nuestros propósitos la aplicación más importante de la multiplicación de matrices ha sido la representación de un sistema de ecuaciones lineales en la forma AX=B.

REPRESENTACION DE UNA ECUACION

Una ecuación lineal de la forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ puede representarse en la forma matricial como sigue

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = b$$

Una ecuación puede representarse empleando el producto interno. La expresión $3x_1 + 5x_2 - 4x_3$ puede representarse por medio del producto interno:

$$\begin{pmatrix} 3 & 5 & -4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

donde el vector fila contiene los coeficientes de cada variable en la expresión y el vector columna contiene las variables. Multiplíquense los dos vectores para comprobar que el producto interno dé por resultado la expresión original.

Si se desea representar la ecuación $3x_1 + 5x_2 - 4x_3 = 25$ puede igualarse el producto interno con una matriz (1 x 1) que contenga la constante del miembro derecho, o sea:

$$\begin{pmatrix} 3 & 5 & -4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 25 \end{pmatrix}$$

REPRESENTACION DE SISTEMAS DE ECUACIONES

Un sistema de ecuaciones que tenga la forma

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{array}$$

puede representarse por la ecuación matricial **AX=B**

donde **A** es una matriz que contiene los coeficientes variables en el miembro izquierdo del conjunto de ecuaciones. **X** es un vector columna de n componentes que contiene n variables y **B** es un vector columna de n componenetes que contiene las constantes del lado derecho para las ecuaciones n. Esta representación aparece como

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

A diferencia de las ecuaciones individuales que pueden representarse mediante el producto interno, un sistema de ecuaciones se representa utilizando la multiplicación de matrices. El sistema

$$\begin{aligned} 5x_1 + 3x_2 &= 15 \\ 4x_1 - 2x_2 &= 12 \end{aligned}$$

Puede representarse así $\begin{pmatrix} 5 & 3 \\ 4 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 15 \\ 12 \end{pmatrix}$

Si se efectúa la multiplicación de matrices en el miembro izquierdo de la ecuación matricial, el resultado será

$$\begin{pmatrix} 5x_1 + 3x_2 \\ 4x_1 - 2x_2 \end{pmatrix} = \begin{pmatrix} 15 \\ 12 \end{pmatrix}$$

EJEMPLO 20 El sistema de ecuaciones

$$\begin{aligned} 2x_1 + 3x_2 + 6x_3 &= 6 \\ 4x_2 + 5x_3 &= 5 \\ 6x_3 &= 6 \end{aligned}$$

puede representarse en la forma matricial AX=B como

$$\begin{pmatrix} 2 & 3 & 6 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 6 \\ 5 \\ 6 \end{pmatrix}$$

Note que los ceros deben incluirse en la matriz A cuando una variable no aparece en determinada ecuación.

Si tenemos una matriz A n x n y una matriz B n x 1, entonces las siguientes proposiciones son equivalentes:

1. La forma escalonada reducida por filas de A es I.

2. A es inversible (A^{-1}=R(I)), donde R es cualquier sucesión de operaciones elementales de fila tal que R(A)=I

3. AX=B tiene soluciónñ única para (la matriz de variables n x 1) X.

Un sistema homogéneo de n ecuaciones lineales en n incógnitas tiene precisamente una solución (la trivial) o bien infinidad de soluciones.

Si la matriz A se puede reducir por filas a I, entonces el sistema dado AX=0 tiene solución única. Si no se la puede reducir por filas a I, entonces el sistema homogéneo de ecuaciones asociado a la forma escalonada reducida por filas tiene más incógnitas que ecuaciones, entonces este sistema tiene infinitas soluciones.

SOLUCION DE UN SISTEMA MEDIANTE ELIMINACION GAUSSIANA CON PIVOTEO PARCIAL.

Resuelva el siguiente sistema mediante eliminación gaussiana con pivoteo parcial:

$$\begin{aligned} x_1 - x_2 + x_3 &= 1 \\ -3x_1 + 2x_2 - 3x_3 &= -6 \\ 2x_1 - 5x_2 + 4x_3 &= 5 \end{aligned}$$

Paso 1. El sistema se escribe en forma de matriz aumentada. De la primera columna con elementos distintos de cero (llamada columna pivote), se elige el elemento que tenga el mayor valor absoluto. A este elemento se le llama pivote:

$$\left(\begin{array}{ccc|c} 1 & -1 & 1 & 1 \\ -3 & 2 & -3 & -6 \\ 2 & -5 & 4 & 5 \end{array}\right)$$

Paso 2. Las filas se reacomodan a fin de cambiar el pivote hacia la parte superior:

$$\left(\begin{array}{ccc|c} -3 & 2 & -3 & -6 \\ 1 & -1 & 1 & 1 \\ 2 & -5 & 4 & 5 \end{array}\right)$$ se intercambiaron la primera y segunda fila

Paso 3. La primera fila se divide entre el pivote:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 1 & -1 & 1 & 1 \\ 2 & -5 & 4 & 5 \end{array}\right)$$ La primera fila se dividió entre -3

Paso 4. Se suman múltiplos de la primera fila a las demás filas con el objeto de hacer cero los otros elementos situados en la columna pivote:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & -\frac{1}{3} & 0 & -1 \\ 0 & -\frac{11}{3} & 2 & 1 \end{array}\right)$$ la primera fila se multiplicó por -1 y por -2, y los

resultados se sumaron a las filas dos y tres, respectivamente.

Paso 5. La primera fila se deja ya tal cual está, efectuándose de nuevo los pasos del uno al cuatro en la submatriz que queda:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & -\frac{1}{3} & 0 & -1 \\ 0 & -\frac{11}{3} & 2 & 1 \end{array}\right) \text{ nuevo pivote}$$

Se intercambia la primera y segunda fila de la submatriz:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & -\frac{11}{3} & 2 & 1 \\ 0 & -\frac{1}{3} & 0 & -1 \end{array}\right)$$

La nueva primera fila se divide entre el pivote:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & 1 & -\frac{6}{11} & -\frac{3}{11} \\ 0 & -\frac{1}{3} & 0 & -1 \end{array}\right)$$

La nueva primera fila se multiplica por 1/3 y se suma la nueva segunda fila:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & 1 & -\frac{6}{11} & -\frac{3}{11} \\ 0 & 0 & -\frac{2}{11} & -\frac{12}{11} \end{array}\right)$$

Paso 6. Se contínua en esta forma hasta dejar la matriz en su forma escalonada por filas:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & 1 & -\frac{6}{11} & -\frac{3}{11} \\ 0 & 0 & -\frac{2}{11} & -\frac{12}{11} \end{array}\right)$$

La nueva primera fila se divide entre el pivote:

$$\left(\begin{array}{ccc|c} 1 & -\frac{2}{3} & 1 & 2 \\ 0 & 1 & -\frac{6}{11} & -\frac{2}{11} \\ 0 & 0 & 1 & 6 \end{array}\right)$$

Paso 7. Se emplea la sustitución hacia atrás para hallar la solución (si existe) del sistema. En este ejemplo, es claro que: $x_3 = 6 \quad x_2 = 3 \quad x_1 = -2$

EJEMPLO 21. Resolver el siguiente problema:

La alacena mágica de una bruja contiene 10 onzas de hojas molidas de tréboles de cuatro hojas y 14 onzas de raíces de mandrágora en polvo. Si la bruja utiliza en forma exacta todo el contenido de su alacena, entonces ésta se resurtirá de manera automática. Para un filtro de amor se requieren 3 1/13 onzas de tréboles molidos de cuatro hojas y 2 2/13 de raíces de mandrágora en polvo. Una receta de una muy conocida cura del resfriado común requiere 5 5/13 de onzas de tréboles de cuatro hojas y 10 10/13 onzas de raíz de mandrágora. Qué cantidades del filtro de amor y del remedio para el resfriado deberá preparar la bruja a fin de utilizar exactamente el contenido de su alacena mágica?

SOLUCION. El sistema de ecuaciones:

$$3\tfrac{1}{13}x_1 + 5\tfrac{5}{13}x_2 = 10$$
$$2\tfrac{2}{13}x_1 + 10\tfrac{10}{13}x_2 = 14$$

puede representarse en la forma matricial **AX=B** como

$$\begin{pmatrix} 3\frac{1}{13} & 5\frac{5}{13} \\ 2\frac{2}{13} & 10\frac{10}{13} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 10 \\ 14 \end{pmatrix}$$

El sistema se escribe en forma de matriz aumentada

$$\left(\begin{array}{cc|c} \frac{40}{13} & \frac{70}{13} & 10 \\ \frac{28}{13} & \frac{140}{13} & 14 \end{array}\right)$$

Mediante eliminación gaussiana con pivoteo parcial, quedaría

$$\left(\begin{array}{cc|c} \frac{40}{13} & \frac{70}{13} & 10 \\ \frac{28}{13} & \frac{140}{13} & 14 \end{array}\right) \approx \left(\begin{array}{cc|c} 1 & \frac{7}{4} & \frac{13}{4} \\ 0 & 7 & 7 \end{array}\right) \approx \left(\begin{array}{cc|c} 1 & \frac{7}{4} & \frac{13}{4} \\ 0 & 1 & 1 \end{array}\right)$$

Se emplea la sustitución hacia atrás para hallar la solución del sistema. En este ejemplo es claro que $x_1 = \frac{3}{2}$ y $x_2 = 1$

EJEMPLO 22. Resolver el siguiente problema

Una compañía elabora tres productos que han de ser procesados en tres departamentos. En la tabla se resumen las horas requeridas por unidad de cada producto en cada departamento. Además las capacidades semanales se expresan para cada departamento en términos de las horas de trabajo disponibles. Se desea determinar si hay combinaciones de los tres grupos que aprovechen al máximo las capacidades semanales de los tres departamentos.

		Producto		Horas disponibles a la semana
Departamento	1	2	3	
A	2	3.5	3	1200
B	3	2.5	2	1150
C	4	3	2	1400

SOLUCION. Si x_j = *número de unidades fabricadas por semana del producto* j, las condiciones a satisfacer se expresan en el siguiente sistema de ecuaciones.

$$2x_1 + 3.5x_2 + 3x_3 = 1200 \quad \text{(departamento A)}$$
$$3x_1 + 2.5x_2 + 2x_3 = 1150 \quad \text{(departamento B)}$$
$$4x_1 + 3x_2 + 2x_2 = 1400 \quad \text{(departamento C)}$$

puede representarse en la forma matricial **AX=B** como

$$\begin{pmatrix} 2 & \frac{35}{10} & 3 \\ 3 & \frac{25}{10} & 2 \\ 4 & 3 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1200 \\ 1150 \\ 1400 \end{pmatrix}$$

el sistema se escribe en forma de matriz aumentada

$$\left(\begin{array}{ccc|c} 2 & \frac{35}{10} & 3 & 1200 \\ 3 & \frac{25}{10} & 2 & 1150 \\ 4 & 3 & 2 & 1400 \end{array}\right)$$

mediante eliminación gaussiana con pivoteo parcial, quedaría

$$\left(\begin{array}{ccc|c} 2 & \frac{35}{10} & 3 & 1200 \\ 3 & \frac{25}{10} & 2 & 1150 \\ 4 & 3 & 2 & 1400 \end{array}\right) \approx \left(\begin{array}{ccc|c} 4 & 3 & 2 & 1400 \\ 3 & \frac{25}{10} & 2 & 1150 \\ 2 & \frac{35}{10} & 3 & 1200 \end{array}\right) \approx \left(\begin{array}{ccc|c} 1 & \frac{3}{4} & \frac{1}{2} & 350 \\ 0 & \frac{1}{4} & \frac{1}{2} & 100 \\ 0 & 2 & 2 & 500 \end{array}\right) \approx \left(\begin{array}{ccc|c} 1 & \frac{3}{4} & \frac{1}{2} & 350 \\ 0 & 1 & 2 & 400 \\ 0 & 0 & -2 & -300 \end{array}\right) \approx \left(\begin{array}{ccc|c} 1 & \frac{3}{4} & \frac{1}{2} & 350 \\ 0 & 1 & 2 & 400 \\ 0 & 0 & 1 & 150 \end{array}\right)$$

De emplea la sustitución hacia atrás para hallar la solución del sistema.. La respuesta quedaría : $x_1 = 200, x_2 = 100$ y $x_3 = 150$.

CAPITULO 2 GRUPOS

2.1 INTRODUCCION

En el capítulo anterior hemos hablado del conjunto de las matrices cuadradas, digamos $M_n(R)$ y dos operaciones llamadas adición y multiplicación. Hablábamos de varias leyes -asociativa, conmutativa y distributiva- satisfechas por estas operaciones.

Pero ciertos de estos conceptos estudiados anteriormente se repiten, por ejemplo, para algunos sistemas de números, entonces esto nos lleva a pensar si sería más ventajoso estudiar las consecuencias de estas leyes sin considerar otras propiedades especiales de cada sistema en estudio, sino hacerlo en forma global.

El estudio general que estamos a punto de comenzar se llama Algebra abstracta. Tiene ejemplos y aplicaciones muy variadas, y su importancia en la Matemática moderna difícilmente puede sobrestimarse.

Para cada estructura algebraica, trabajaremos con un conjunto y una o más funciones u operaciones. Nos restringiremos a la consideración de operaciones binarias, es decir, si el conjunto es $M_n(R)$, tendremos una función, u operación, cuyo dominio es $M_n(R)$ x $M_n(R)$ y cuyo codominio es $M_n(R)$. Por el momento usaremos la notación a*b, para representar el valor f(a,b) de la función.

Si en un análisis simultáneo hay diferentes operaciones binarias, se usarán subíndices o supraíndices en * para distinguirlos. El método más importante para describir una operación binaria particular * en un conjunto dado es el de caracterizar al elemento a*b asignado a cada par (a,b) mediante alguna propiedad definida en términos de a y b.

La mayor parte de las estructuras algebraicas que estudiaremos se definen como un conjunto con una o dos operaciones binarias. Las condiciones que estas operaciones deben satisfacer se llaman los axiomas del sistema.

2.2 DEFINICION Y PROPIEDADES ELEMENTALES.

Es natural comenzar nuestro estudio de estructuras algebraicas considerando un conjunto G con una sola operación binaria que satisface algunas leyes.

El primer tipo de estructura que estudiaremos es el de *grupo*.

GRUPO

DEFINICION 1

Un grupo <G.*> es un conjunto G, junto con una operación binaria * en G, tal que se satisface los siguientes axiomas:

i) La operación binaria * es asociativa.

ii) Existe un elemento **e** en G tal que **e*x=x*e=x** para todas las **x** elemento de G.(Este elemento **e** es un elemento identidad para * en G).

iii) Para cada **a** en G existe un elemento **a'** en G con la propiedad de que **a'*a=a*a'=e** (El elemento **a'** es un inverso de **a** respecto a *)

Un *elemento identidad* para una operación binaria * en un conjunto S es cualquier elemento **e** que satisfaga **e*x=x*e=x** para todas las **x** $\in$ S.

Entre los axiomas para un grupo es frecuente que se incluya una proposición de la forma: "el conjunto es cerrado bajo la operación", que quiere decir si **a** y **b** son elementos de **G**, entonces a*b es un elemento de G. Hemos evitado la necesidad de tal expresión, porque la consideramos una consecuencia de la definición de operación binaria en G.

Obsérvese que un grupo no sólo es un conjunto G. Más bien, que un grupo <G,*>, consta de dos entidades, el conjunto **G** y la operación binaria * en G. Hay dos ingredientes. Denotar al grupo por el símbolo de conjunto G es por lo tanto lógicamente incorrecto. Sin embargo, debemos señalar en este momento, que seremos descuidados con la notación en algunas circunstancias y solo denotaremos al grupo por la letra G. Pero insistimos en que al hablar de un grupo específico G, debe aclararse cuál será la operación del grupo en G, pues un conjunto contiene gran variedad de posibles operaciones binarias definidas, constituyendo grupos diferentes.

En muchos ejemplos de grupos, se verifica la ley conmutativa, y esto nos lleva a definir un tipo especial de grupo.

GRUPO ABELIANO

DEFINICION 2

Si en un grupo <G, *> se verifica además, la propiedad:a*b=b*a, para todo a, b elementos de G (conmutativa) se dice que el grupo es abeliano o conmutativo.

Ahora, pongamos algunos ejemplos de conjuntos con operaciones binarias que dan grupos y otros que no dan grupos.

EJEMPLO 1Consideremos el conjunto de los enteros **Z** y la operación de adición.

i) La ley asociativa se verifica, es decir (a+b)+c=a+(b+c)

ii) El entero 0 es un elemento identidad,es decir,a+0=a=0+a para todo a elemento de Z

iii) El entero -**a** es un elemento inverso de **a**, es decir, a+(-a)=0=(-a)+a=0 para todo a elemento de los enteros.

Estas propiedades nos dicen que los enteros con la operación de adición forman un grupo. Este grupo se conoce como el *grupo aditivo de los enteros*

¿Formaría un grupo los enteros positivos cuya notación es Z^+?

EJEMPLO 2. El conjunto Z^+ bajo la adición no forman un grupo. La adición es una operación binaria asociativa y conmutativa, pero **NO** existe elemento identidad.

EJEMPLO 3. La multiplicación de los Z^+ es una operación binaria asociativa y conmutativa. En este caso 1 es un elemento identidad, pero no hay elemento inverso para z^+diferente de 1. Por tanto, **NO** tenemos un grupo.

Existen resultados acerca de grupos que deseamos presentar y probar, porque ya verán en seguida que son extraordinariamente útil.

El aprendizaje del alfabeto no fue probablemente la parte más interesante de nuestra educación infantil, sin embargo, una vez que lo dominamos, que panoramas más fascinantes se abrieron ante nosotros.

LEMA 1 Si G es un grupo, entonces

i) el elemento identidad de G es único;

ii) todo a elemento de G tiene inverso único en G;

iii) para todo a elemento de G, (a')' = a;

iv) para a, b elementos de G, (a.b)' = b'.a'.

PRUEBA. Antes de que comencemos propiamente con la prueba parece aconsejable que veamos qué es lo que vamos a probar. En la parte i) queremos probar que si dos elementos e y f de G gozan de la propiedad de que para todo a elemento de G, $a = a.e = e.a = a.f = f.a$, entonces $e = f$.En la parte ii) nuestro objetivo es demostrar que si $x.a = a.x = e$ y $y.a = a.y = e$,donde los tres a, x,y están en G, entonces $x = y$.

Consideremos primero la parte i). Como $e.a = a$ para todo a elemento de G, tenemos que, en particular, $e.f = f$. Pero, por otra parte, $b.f = b$ para todo b elemento de G, luego debemos tener $e.f = e$. Juntando estas dos fracciones de información obtenemos $f=e.f=e$, y, por tanto, $e=f$.

En lugar de probar la parte ii) probaremos algo más fuerte que nos traerá inmediatamente la parte ii) como consecuencia. Supongamos que para a en G, $a.x=e$ y $a.y=e$; entonces, obviamente, $a.x=a.y$. Hagamos de esto nuestro punto de partida. Es decir, supongamos que $a.x=a.y$ con a, x, y en G. Hay un elemento b en G tal que $b.a=e$ (por lo que hasta ahora sabemos puede que haya varios de tales b). Por tanto, $b.(a.x)=b.(a.y)$. Usando la ley asociativa esto nos lleva a que

$$x=e.x=(b.a).x=b.(a.x)=b.(a.y)=(b.a).y=e.y=y.$$

Hemos probado, en realidad, que en un grupo G, $a.x=a.y$ implica que $x=y$. Análogamente, podemos probar que $x.a=y.a$ implica que $x=y$. Esto quiere decir que en los grupos podemos cancelar, siempre que sea del mismo lado, en las ecuaciones. Pero debe tenerse presente que de que $a.x=y.a$ no puede concluirse que $x=y$, pues no tenemos medio alguno de saber que $a.x=x.a$.

La parte iii) se sigue de esto si observamos que $a'.(a')' = e = a'.\ a$;cancelando la a' a la izquierda nos da $(a')' = a$,Esto es, para grupos en general, lo análogo del resultado familiar, digamos por ejemplo, -(-5)=5, en los números reales respecto a la suma.

La parte iv) es la más trivial de todas, pues $(a.b).(b'\ .\ a') = a.((b.b').a') = a.(e.a')=a.a' = e$ y luego, de acuerdo con la definición de inverso, $(a.b)' = b'\ .\ a'$.

Ciertos resultados obtenidos en la prueba son de suficiente importancia para enunciarlos expresamente como hacemos ahora en el

LEMA 2.Dados a, b en el grupo G, entonces las ecuaciones $a\ .x = b$ y $y\ .a = b$ tienen soluciones únicas para x, y en G. En particular, las dos leyes de cancelación,

$$a.u = a.w \text{ implica } u = w$$

y

$$u.a = w.a \text{ implica } u = w$$

se verifican en G.

Dejemos al lector los pocos detalles necesarios para la prueba de este lema.

2.3 GRUPOS FINITOS Y TABLAS DE GRUPO.

Hasta ahora nuestros ejemplos han correspondido a grupos infinitos, esto es, de grupos donde el conjunto G tiene un número infinito de elementos.

Otra característica natural de un grupo G es el número de elementos de que consta. Este número es, desde luego, más interesante cuando es finito; en tal caso decimos que G es un *grupo finito*

ORDEN DE UN GRUPO FINITO

DEFINICION 3

Si G es un grupo finito, entonces el **orden** $|G|$ **de** G es el número de elementos en G. En general, para cualquier conjunto finito S, $|S|$ es el número de elementos en S.

Un grupo debe tener al menos un elemento a saber, la identidad, el conjunto más pequeño que puede dar lugar a un grupo es un conjunto {e} de un elemento. En cada grupo, el elemento identidad es siempre su propio inverso. Y se tiene la multiplicación trivial.

*	e
e	e

Si construímos una estructura de grupo en un conjunto de dos elementos, entonces uno de los elementos debe desempeñar el papel de identidad. El conjunto quedaría así {e,a}. Busquemos una tabla para una operación binaria * en {e,a} que dé una estructura de grupo.

Cuando demos una tabla para una operación de grupo, siempre colocaremos los elementos en la parte superior, hacia la derecha en el mismo orden en que los colocamos del lado izquierdo, hacia abajo, colocando en primer lugar la identidad, como en la tabla siguiente:

*	e	a
e		
a		

Ya que $a^2 \in G$ debe tenerse $a^2 = e$, o bien, $a^2 = a$, pero $a^2 = a$ implica que $a = e$, de donde $a^2 = e$ y se tiene

*	e	a
e	e	a
a	a	e

Sean $G = \{e,a,b\}$. Se considera ab y se observa que $ab \neq a$ porque $ab=a$ implica que $b=e$. De modo semejante, $ab \neq b$ y, de aquí que $ab=e$. Esto implica que $b=a'$ y, por tanto, $ba=e$.

De aquí se obtiene el arreglo parcialmente lleno

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

Ahora bien, se sabe, que cada una de las filas y columnas del arreglo debe contener, al menos, elementos diferentes de G, de donde finalmente se obtiene

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

Sean $G=\{e,a,b,c\}$. Se distinguen dos casos.

Caso 1. Supóngase que existe un elemento cuyo inverso no es igual a sí mismo. En beneficio del argumento, supóngase que $ab=e$. Entonces $ba=e$ y, de aquí, que $ac \neq e$, a o c. De donde, $ac=b$ y, de modo semejante, $ca=b$. De aquí que

$$b^2 = bb = b(ac) = (ba)c = ec = c.$$

Se obtiene el arreglo

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

El cual se completa para dar

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

Caso 2 Supóngase ahora que todo elemento tiene inverso igual a sí mismo. Por tanto $a^2 = b^2 = c^2 = e$. Entonces $ab \neq e, a$ o b y, por consiguiente, $ab=c$. De modo semejante, $ba=c$. Por medio de un argumento semejante, se tiene $ac=ca=b$, $ac=cb=a$, dando

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

Este último grupo se conoce como grupo cuatro de Klein (en honor de F. Klein, matemático alemán, 1849-1925)

Con base en estos ejemplos, podremos enumerar algunas condiciones que una tabla que defina una operación binaria en un conjunto finito debe satisfacer, para dotarlo de una estructura de grupo.Es necesario que algún elemento del conjunto, que siempre denotaremos por e, actúe como identidad. La condición $e*x=x$ significa que la fila de la tabla que contiene a e en el extremo izquierdo, debe contener exactamente los elementos que aparecen hasta arriba de la tabla, en el mismo orden. En forma análoga, la condición $x*e=x$ significa que la columna de la tabla bajo e, debe contener precisamente los elementos que aparecen en el extremo izquierdo, en el mismo orden. El hecho de que cada elemento a tenga un inverso derecho y un izquierdo, quiere decir que en la fila frente a a debe aparecer el elemento e y que en la columna bajo a debe aparecer e en primer lugar. Así, e debe aparecer en cada fila y en cada columna. Sin embargo, podemos mejorar esto. Las ecuaciones tratadas en los lemas anteriores tienen solución única. Por un argumento análogo, esto significa que cada elemento b del grupo debe aparecer una y sólo una vez en cada fila y en cada columna de la tabla.

2.4 SUBCONJUNTOS Y SUBGRUPOS

Habrán notado que hemos tenido a veces grupos contenidos en grupos mayores. Por ejemplo, el grupo **Z** bajo la suma está contenido en el grupo **Q** bajo la suma, el cual a su vez está contenido en el grupo **R** bajo la suma. Cuando vemos al grupo **<Z,** +> como contenido en el grupo **<R,** +> es importante notar que la operación + en los enteros n y m como elementos de **<Z,** +> produce el mismo elemento $n + m$ que resultaría si se pensara en n y m como elementos de **<R,** +>. Por tanto, no debemos considerar al grupo $< Q^+,$ +> como contenido en **<R,** +> aunque Q^+ está contenido en **R** como conjunto.

No sólo se requiere que el conjunto de un grupo esté contenido en el conjunto del otro, sino también que la operación de grupo en el conjunto menor asigne el mismo elemento a cada par ordenado de este conjunto menor que el asignado por la operación de grupo del conjunto mayor.

SUBCONJUNTO DE UN CONJUNTO

DEFINICION 4

Un conjunto B es un subconjunto de un conjunto A denotado por $B \subseteq A$ o $A \supseteq B$ si cada elemento de B es también un elemento de A. Las notaciones $B \subset A$ o $A \supset B$ se usarán para $B \subseteq A$, pero $B \neq A$.

Nótese que de acuerdo con esta definición, para cualquier conjunto A, A misma y $\varnothing$ son subconjuntos de A.

SUBGRUPOS

DEFINICION 5

Si G es un grupo y H es un subconjunto no vacío de G, se dice que H es un subgrupo de G y se escribe $H \leq G$ si se verifica que H es él mismo un grupo bajo la operación inducida de grupo de G.

+

Por lo tanto conviene tener un criterio de rutina para determinar si un subconjunto de un grupo G es un subgrupo de G. El siguiente teorema proporciona dicho criterio.

TEOREMA 1 Un subconjunto H de un grupo G es un subgrupo de G si y sólo si

i) H es cerrado bajo la operación binaria de G;

ii) la identidad *e* de G está en H;

iii) para todos los $a \in H$ es cierto que $a' \in H$ también.

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.

EJEMPLO 4 Consideramos el grupo aditivo de los enteros $\langle \mathbf{Z}, + \rangle$ Para cada $p \in Z$ consideramos el subconjunto de Z de los múltiplos de p. Se verifica que son los únicos subgrupos de $\langle \mathbf{Z}, + \rangle$.

EJEMPLO 5 Q bajo multiplicación es un subgrupo propio de bajo multiplicación.

2.5 GRUPO DE MATRICES

PROBLEMA 1

Consideremos a $M_n(R)$, que es el conjunto de todas las matrices de n x n sobre R, con la definición de suma convencional.

Probaremos que $\langle M_n(R),+\rangle$ es un grupo abeliano.

a) La operación de adición es asociativa y conmutativa. (Teorema 1, capítulo 1).

b) Existe la matriz nula que es la matriz formada por ceros solamente y que actúa como elemento neutro de la suma.(Definición 3, capítulo 1).

c) Para toda matriz (a_{ij}) existe la matriz opuesta $(-a_{ij})$tal que $(a_{ij})+(-a_{ij})$ es la matriz cero. Ejemplo:

$$A=\begin{bmatrix}1 & 3\\ 5 & 7\end{bmatrix} \text{ y } -A=\begin{bmatrix}-1 & -3\\ -5 & -7\end{bmatrix} \text{ entonces } A+(-A)=\begin{bmatrix}1+(-1) & 3+(-3)\\ 5+(-5) & 7+(-7)\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$$

Claro está, entonces, que el conjunto con la operación suma forman un grupo.Esto $\langle M_n(R)\rangle$ es un grupo abeliano.

PROBLEMA 2

Trabajemos ahora, con el mismo conjunto del problema anterior, junto con la operación producto entre matrices.

¿ Será $\langle M_n(R),\bullet\rangle$ un grupo?.

Veamos si satisface los axiomas de grupo.

a) La operación binaria definida es asociativa.(Teorema 3,capítulo 1).

b) Existe el elemento neutro que es la Identidad.(Ejemplo 10, capítulo 1).

c) Pero, lastimosamente no todos los elementos del conjunto tienen inverso, porque no toda matriz cuadrada es inversible. Ejemplo $A = \begin{bmatrix} 3 & 5 \\ 0 & 0 \end{bmatrix}$

Por lo tanto, el conjunto de todas las matrices cuadradas sobre R con la operación producto **NO** forman un grupo.

PROBLEMA 3.

Ahora probaremos que el conjunto G de matrices no singulares de 2 x 2 sobre los números racionales **Q** forma un grupo que no es conmutativo. Hallar $a,\ b \in$ G tales que $(ab)^{-1} \neq a^{-1}b^{-1}$.

Solución. No se dice cómo deben multiplicarse las matrices, pero se acostumbra suponer que se sobrentiende la multiplicación ordinaria de matrices, siendo asociativa esta multiplicación y la matriz identidad de 2 x 2 la identidad para G.

Sean $X,\ Y$ dos matrices no singulares de 2 x 2 sobre **Q**, digamos

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix},\quad Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

donde los elementos de las matrices son números racionales y donde

$$x_{11}x_{22} - x_{12}x_{21} \neq 0 \qquad y_{11}y_{22} - y_{12}y_{21} \neq 0$$

Entonces XY también es no singular porque

$$XY = \begin{pmatrix} x_{11}y_{11} + x_{12}y_{21} & x_{11}y_{12} + x_{12}y_{22} \\ x_{21}y_{11} + x_{22}y_{21} & x_{21}y_{12} + x_{22}y_{22} \end{pmatrix}$$

y

$$(x_{11}y_{11} + x_{12}y_{21})(x_{21}y_{12} + x_{22}y_{22}) - (x_{21}y_{11} + x_{22}y_{21})(x_{11}y_{12} + x_{12}y_{22}) = (x_{11}x_{22} - x_{21}x_{12})(y_{11}y_{22} - y_{21}y_{12}) \neq 0$$

.

También, si $Z \in G$, digamos

$$Z = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

entonces se deduce que $Z^{-1} \in G$ es

$$Z^{-1} = \frac{1}{z_{11}z_{22} - z_{12}z_{21}} \begin{pmatrix} z_{22} & -z_{12} \\ -z_{21} & z_{11} \end{pmatrix}.$$

Así, se ha establecido que G es un grupo. Para demostar que G no es conmutativo basta recordar que la multiplicación de matrices no es conmutativa.

Puede generalizarse el problema anterior al caso de las matrices no singulares de n x n. Simplemente se requiere conocer la regla del producto para los determinantes, a saber **det(X)det(Y) = det(XY).**

¿Qué ocurrirá si las entradas provienen de los reales,alterará en algo si las entradas son números enteros? Sugerimos al lector meditar sobre esta pregunta para verificer el grado de entendimiento que está adquiriendo sobre el concepto de grupo.

PROBLEMA 4

Veamos ahora un conjunto finito formado por las seis matrices que presento a continuación. Si es un grupo, este sería un subgrupo de todas las matrices cuadradas 2 x 2, pero inversibles. Para afirmar lo antes dicho tengo que probar que es cerrado bajo la operación de grupo.

Tenemos las siguientes matrices

$$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

$$B=\begin{pmatrix}-\frac{1}{2} & \frac{1}{2}\sqrt{3}\\ \frac{1}{2}\sqrt{3} & \frac{1}{2}\end{pmatrix}, \qquad C=\begin{pmatrix}-\frac{1}{2} & -\frac{1}{2}\sqrt{3}\\ -\frac{1}{2}\sqrt{3} & \frac{1}{2}\end{pmatrix},$$

$$D=\begin{pmatrix}-\frac{1}{2} & \frac{1}{2}\sqrt{3}\\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2}\end{pmatrix}, \qquad F=\begin{pmatrix}-\frac{1}{2} & -\frac{1}{2}\sqrt{3}\\ \frac{1}{2}\sqrt{3} & -\frac{1}{2}\end{pmatrix}$$

y formamos la tabla de multiplicación de los 36 productos que resultan de multiplicar una matriz con otra de acuerdo con la regla para multiplicar matrices. Vemos que para toda matriz del grupo, el producto es otra matriz que pertenece al grupo, esto indica que la operación es cerrada en el grupo.

Lo podemos observar en la tabla de multiplicar adjunta, para cualquiera dos matrices que pertenecen al grupo el producto de la matriz producto también pertenece al conjunto.

	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	E	D	F	B	C
B	B	F	E	D	C	A
C	C	D	F	E	A	B
D	D	C	A	B	F	E
F	F	B	C	A	E	D

1.La ley asociativa.Por ser un caso particular de matrices sabemos que se cumple la ley asociativa.

2.Existe una matriz E para cada elemento del grupo, hay uno (y sólo uno) que es llamado idéntico o elemento unidad, E el cual tiene la propiedad de que al multiplicarlo con cualquier elemento da exactamente el otro elemento. EA=AE=A.

3.Cada elemento tiene su inverso multiplicativo. Es decir:

$$A^{-1} = A,\ B^{-1} = B,\ C^{-1} = C,\ D^{-1} = F,\ F^{-1} = D \text{ y } E^{-1} = E$$

Esto prueba que el conjunto con la operación binaria de la multiplicación entre matrices es un grupo.

De este grupo podemos formar subgrupos.Por ejemplo, aquel que tiene dos elementos: E y A.

PROBLEMA 5

Entre los muchos grupos de matrices que es posible considerar, aparecen útilmente aquellos en que intervienen matrices diagonales. Para sumar o multiplicar matrices diagonales, basta con sumar o multiplicar los elementos correspondientes alineados en tales diagonales. (*¿por qué ?)*. De aquí resulta que una matriz diagonal tiene una inversa si ningún elemento de la diagonal es nulo, y sólo en este caso. Por lo tanto tenemos que todas las matrices diagonales no singulares forman un subgrupo del grupo de todas las matrices n x n inversibles con elementos en los reales.

PROBLEMA 6

Probar que el conjunto S de las matrices de rotación

$$\begin{pmatrix} \cos\theta & sen\theta \\ -sen\theta & \cos\theta \end{pmatrix} \quad (\theta \in R)$$

bajo la multiplicación matricial común, es un grupo conmutativo.

Solución. i) Debe verificarse que S es cerrado bajo la multiplicación. Esto se concluye basándose en la Trigonometría elemental, ya que

$$\begin{pmatrix} \cos\alpha & sen\alpha \\ -sen\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & sen\beta \\ -sen\beta & \cos\beta \end{pmatrix}=\begin{pmatrix} \cos\alpha\cos\beta - sen\alpha\, sen\beta & \cos\alpha\, sen\beta + sen\alpha\cos\beta \\ -sen\alpha\cos\beta - \cos\alpha\, sen\beta & -sen\alpha\, sen\beta + \cos\alpha\cos\beta \end{pmatrix}$$

$$=\begin{pmatrix} \cos(\alpha+\beta) & sen(\alpha+\beta) \\ -sen(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \quad (\alpha,\beta\in R) \quad (1)$$

lo cual es de la forma requerida. La multiplicación de matrices es asociativa y

ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} \cos 0 & sen0 \\ -sen0 & \cos 0 \end{pmatrix}$ es la identidad de S.

iii) La inversa de una rotación de amplitud θ es la rotación de amplitud -θ, así que la matriz inversa es

$$\begin{pmatrix} \cos\theta & sen\theta \\ -sen\theta & \cos\theta \end{pmatrix}^{-1}=\begin{pmatrix} \cos(-\theta) & sen(-\theta) \\ -sen(-\theta) & \cos(-\theta) \end{pmatrix}=\begin{pmatrix} \cos\theta & -sen\theta \\ sen\theta & \cos\theta \end{pmatrix}$$

de lo cual se infiere que todos los elementos de S tienen inversos en S. La matriz que resulta es precisamente la transpuesta de la original. ¿Será esta circunstancia generalizada para las matrices *n* x *n? Medítelo.*

De aquí que S es un grupo. Intercambiando α y β en la ecuación 1 se ve que S es conmutativo. Y tenemos un caso especial de grupo de matrices conmutativo.

CAPITULO 3 ANILLOS

3.1 INTRODUCCION

En el capítulo anterior hemos visto los conjuntos únicamente con una operación binaria en ellos. Una buena cantidad de estructuras algebraicas conocidas e importantes tienen dos operaciones binarias que generalmente se escriben como + y • . La operación "aditiva" (+) es ejemplo de buen funcionamiento, mientras que la operación "multiplicativa" (•) no tanto, y en general hay leyes distributivas que relacionan las dos operaciones.

En este capítulo introduciremos brevemente anillos que es una de las estructuras algebraicas más importante con dos operaciones.

3.2 DEFINICION Y PROPIEDADES BASICAS

ANILLO

DEFINICION 1

Un anillo $< R, +, \bullet >$ es un conjunto R junto con dos operaciones binarias + y • , que llamamos suma y multiplicación, definidas en R tales que se satisfacen los siguientes axiomas:

i) $< R, + >$ es un grupo abeliano.

ii) La multiplicación es asociativa.

iii) Para todas las $a,b,c \in R$, se cumple la ley distributiva izquierda $a(b+c)=ab+ac$ y la ley distributiva derecha $(a+b)c=ac+bc$.

EJEMPLO 1 Los conjuntos **Z**, **Q** y **R** son cada uno un grupo bajo la suma y cerrado bajo la multiplicación. Para cada uno de estos conjuntos, las operaciones + y • son conmutativas y asociativas. Además estas operaciones satisfacen las leyes distributivas.

Debido a una convención semejante a nuestra notación en teoría de grupos, nos referiremos de manera algo incorrecta, a un anillo R, en lugar de a un anillo $\langle R,+,\bullet\rangle$ siempre que no haya confusión. En particular, de ahora en adelante, **Z** será <Z,+,• > y **Q**, **R** y **C** serán también los anillos obvios. Si es necesario, nos referiremos a <R,+> como el *grupo aditivo del anillo R*.

Nosotros queremos estar en posibilidad de operar en anillos casi exactamente como con los números reales, recordando siempre que hay diferencias - puede suceder que ab≠ba o que no podamos dividir. Es en vista de estas posibilidades es que queremos probar el próximo teorema que confirma que ciertas cosas que nos gustaría que fuesen ciertas en los anillos lo son realmente.

TEOREMA 1 Si R es un anillo con identidad aditiva 0 entonces, para cualquier a,b ∈ R, tenemos

i) 0a=a0=0

ii) a(-b)=(-a)b= -(ab)

iii) (-a)(-b)=ab

Si, además, R tiene un elemento unitario 1, entonces

iv) (-1)a= -a

v) (-1)(-1)= 1

Demostración. Para la condición i), nótese que

$$a0=a(0+0)=a0+a0$$

Entonces, por la ley de cancelación para el grupo aditivo $<R, + >$ tenemos $0=a0$. Así mismo

$$0a=(0+0)a=0a+0a$$

implica que $0a=0$. Esto prueba la condición i).

Para entender la demostración de la condición ii) hay que recordar que, por definición, -(ab) es el elemento que, sumado a ab, da 0. Así, para mostar que a(-b)= -(ab), debe mostrarse precisamente que a(-b)+ab=0. Por la ley distribituva izquierda.

$$a(-b)+ab=a(-b+b)= a0=0$$

pues, por la condición 1, a0=0. Así mismo,

$$(-a)b+ab=(-a+a)b=0b=0$$

Para la condición iii), nótese que, por la condición ii),

$$(-a)(-b)= -(a(-b)).$$

De nuevo por la condición ii),

$$-(a(-b))= -(-(ab)),$$

y -(-(ab)) es el elemento que, sumando a -(ab), da 0. Este es ab por definición de -(ab) y por la unicidad de un inverso en un grupo. Así (-a)(-b)=ab.

Para la condición iv), supongamos que R tiene un elemento unitario 1; entonces

$$a+(-1)a=1a+(-1)a=(1+(-1))a=0a=0$$

de donde (-1)a=a.

En particular, si a= -1 entonces (-1)(-1)= -(-1)=1 lo que deja establecido la parte v).

3.3 EL ANILLO $\langle M_n(R),+,\bullet\rangle$.

Las propiedades de las operaciones de suma y de multiplicación en $M_n(R)$, introducidas y exaustivamente estudiadas en el capítulo 1, permiten afirmar, que $\langle M_n(R),+,\bullet\rangle$ es un anillo con unitario 1=I. Se llama *anillo matricial completo sobre R*, y también *anillo de las matrices cuadradas de orden n (o de dimensiones n x n) sobre R*. Este es uno de los más importantes anillos.

Veamos detalladamente porque es un anillo:

i) $\langle M_n(R),+\rangle$ es un grupo abeliano. (problema 1, capítulo 2).

ii) El teorema 3 del capítulo 1 nos indica que la multiplicación en $M_n(R)$ es asociativa y distributiva. Es decir con esto se probaría que $M_n(R)$ cumple con los axiomas 2 y 3 de la definición de anillo.

Así como para $n > 1$ las matrices, como regla general, no son permutables, entonces, $\langle M_n(R),+,\bullet\rangle$ es un anillo no conmutativo.

El contiene en calidad de subanillos, a los anillos, $\langle M_n(Q),+,\bullet\rangle$ y $\langle M_n(Z),+,\bullet\rangle$ de las matrices cuadradas del mismo orden, sobre Q y sobre Z, respectivamente. En general, $\langle M_n(R),+,\bullet\rangle$ está saturado de subanillos de todo género.

EJEMPLO 2. Restringiremos ahora nuestra atención a matrices $M_3(R)$. Se aconseja al lector traslade estas mismas ideas al caso de $M_2(R)$. Es posible proceder con mayor generalidad, pero prescindiremos de esta generalidad en interés de la sencillez.

Por lo que se ha dicho en el capítulo 1y 2 es claro que $\langle M_n(R),+\rangle$ forman un grupo abeliano, que la ley asociativa se cumple para la multiplicación, como también las leyes distributivas. Esto completa la prueba de que el conjunto de todas las matrices 3 x 3 cuyos elementos son números reales junto con las operaciones "aditiva" y "multiplicativa" forman un anillo.

Podemos también indicar que la matriz

$$I=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

actúa como elemento identidad en la multiplicación. Por lo tanto estas matrices forman un anillo con unitario

Este anillo no es conmutativo, como vemos en este ejemplo:

$$\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\1&0&1\end{pmatrix}=\begin{pmatrix}2&0&1\\0&1&0\\1&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&1&0\\1&0&1\end{pmatrix}\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&1\\0&1&0\\1&0&2\end{pmatrix}$$

En el anillo de las matrices 3 x 3 existe esta situación particular que no se da en el anillo de los reales es decir: $AB=0 \wedge \neg(A=0 \vee B=0)$ por ejemplo,

$$\begin{pmatrix}1&0&0\\0&3&0\\0&0&0\end{pmatrix}\begin{pmatrix}0&0&0\\0&0&0\\3&1&5\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$$

Esto significa que pueden existir dos matrices distintas de cero y sin embargo el producto de ellas puede darnos la matriz cero.

Esto es un limitante que impide que el conjunto de matrices con estas operaciones poseen una estructura algebraica más compleja, como las que veremos en el capítulo siguiente.

Esta propiedad de que existan o no estos elementos en el anillo nos permite definir el siguiente concepto importante.

DIVISORES DEL CERO

DEFINICION 2

Se denomina así los elementos no nulos de un anillo cuyo producto es cero.

Simbólicamente,

$$a \neq 0, \quad b \neq 0, \quad a.b = 0$$

EJEMPLO 1 Ver ejemplo 11 del capítulo 1.

CAPITULO 4 CAMPO

4.1 ALGUNAS CLASES ESPECIALES DE ANILLO.

ANILLO CONMUTATIVO

DEFINICION 1

Si $<R, . >$ es conmutativo, entonces decimos que el anillo $< R, +, . >$ es *conmutativo.*

ANILLO CON UNITARIO

DEFINICION 2

Si tiene una identidad multiplicativa que es distinta de cero, generalmente llamamos a ésta, identidad multiplicativa 1 tal que $1x = x1 = x$ para todas las $x \in R$, decimos que el anillo es un *anillo con unitario* o con identidad.

Un inverso multiplicativo de un elemento a en un anillo R con unitario 1 es un elemento $a^{-1} \in R$ tal que $aa^{-1} = a^{-1}a = 1$

ANILLO CON DIVISION

DEFINICION 3

Si los elementos distintos de cero de un anillo R con unitario forman un grupo bajo la multiplicación se dice que es un *anillo con división.*

Damos finalmente la definición del muy importante objeto matemático conocido como campo.

4.2 DEFINICION DE CAMPO

Un campo es un anillo conmutativo con división.

Resultando ser un campo un anillo con (mayor exigencia estructural), es evidente que toda la teoría de anillos es trasladable, completamente a los campos.

Existen estructuras intermedias en que precisamente un anillo no tiene divisores de cero, daremos por eso la siguiente definición.

4.3 ANILLO DE INTEGRIDAD; DOMINIOS ENTEROS

ANILLO DE INTEGRIDAD

DEFINICION 6

Se califica así a todo anillo que no tiene divisores del cero. Por tanto, en estos anillo, si el producto de dos elementos es cero, es que al menos uno de los factores es nulo. De este modo:

Si $< R, +, . >$ es anillo de integridad,

$$a \wedge b \in R, a.b = 0 \Rightarrow \begin{cases} a = 0 \text{ o} \\ b = 0 \text{ o} \\ a = b = 0 \end{cases}$$

Si, como es normal, el anillo de integridad tiene elemento unitario, recibe el nombre de dominio entero. ¿ y qué es entonces un dominio entero?

DOMINIO ENTERO

DEFINICION 7

Un *dominio entero D* es un anillo conmutativo unitario que no contiene divisores de cero.

TEOREMA 1 Todo campo F es un dominio entero.

Demostración Sea $a, b \in F$, supóngase que $a \neq 0$. Entonces, si $ab=0$ tenemos

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0$$

Pero entonces,

$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b$$

Hemos mostrado que $ab=0$ con $a \neq 0$ implica que $b=0$ en F, de modo que no existen divisores de 0 en F. Es claro que F es un anillo conmutativo con unitario y así queda probado el teorema.

En los anillos (y dominios) de integridad se puede utilizar la *regla de simplificación,* cosa que no es lícita si el anillo tiene divisores del cero.

Sea $< R, +, . >$ un anillo de integridad y sean a, b y c elementos de él no nulos, de modo que

$$a \times c = b \times c \Rightarrow a \,.\, c - b \,.\, c = 0 \Rightarrow c.\,(a-b) = 0$$

Por hipótesis uno de los dos factores, al menos, ha de ser nulo; pero $c \neq 0$, luego

$$a - b = 0 \Rightarrow a = b,$$

resultando que justifica haber simplificado inicialmente la primera expresión.

4.4 MATRICES SOBRE UN CAMPO

Sea F cualquier campo (digamos **Q, R** o **C**), considérese el conjunto $M_n(F)$ de todos los arreglos cuadrados de 2 x 2

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

donde todas las a_{ij} están en F. El primer subíndice i de a_{ij} indica la fila donde está a_{ij} en el arreglo cuadrado y el segundo subíndice j indica la columna. Así, a_{12} es el elemento de F situado en la primera fila y segunda columna del arreglo cuadrado. Dicho arreglo cuadrado es una **matriz de 2 x 2 sobre F.** El conjunto $M_n(F)$ de todas las **matrices de n x n sobre F** se define de manera análoga.

Definimos la suma de matrices en $M_2(F)$ por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

esto es, sumando los elementos de lugares correspondientes. Después de pensarlo un momento, se verá que, debido a que F satisface los axiomas de campo, $\langle M_2(F), + \rangle$ es un grupo abeliano con identidad aditiva Nótese que esto es una generalización de lo que se ha efectuado en el capítulo 1 con los reales, en el caso particular en que el campo es los reales.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

y con

$$-\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}.$$

La multiplicación de matrices en $M_2(F)$ está definida por

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}$$

Esta multiplicación parece dificil, se recuerda mejor por

$$(a_{ij})(b_{ij}) = (c_{ij}), \text{ donde } c_{ij} = \sum_{k=1}^{2} a_{ik} b_{kj}.$$

Con la definición análoga para la multiplicación de matrices, en donde la suma va de i=1 a n y la definición análoga obvia para la suma de matrices, todo lo que se ha hecho es válido para el conjunto $M_n(F)$ de todas las matrices de n x n sobre F.

Nótese que el cero es la identidad aditiva en el campo F, no necesariamente el número cero y por es la operación binaria definida como producto en el campo F, no necesariamente el por entre los reales.

EJEMPLO 2 En $M_2(Q)$

$$\begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$$

y

$$\begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 2 & -5 \end{pmatrix} = \begin{pmatrix} 0 & -5 \\ 11 & -20 \end{pmatrix}$$

Para mostrar que $\langle M_n(F), +, \bullet \rangle$ es un anillo, falta probar las leyes asociativa y distributiva.Lo ilustramos con la ley asociativa para la multiplicación de matrices en $M_n(F)$. Usando las propiedades de campo de F y la definición de multiplicación de matrices en $M_n(F)$, si d_{rs} está en el lugar correspondiente a $(a_{ij})[(b_{ij})(c_{ij})]$, tenemos

$$d_{rs} = \sum_{k=1}^{n} a_{rk} \left(\sum_{j=1}^{n} b_{kj} c_{js} \right) = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_{rk} b_{kj} \right) c_{js} = e_{rs}$$

donde e_{rs} está en el r-ésima fila y s-ésima columna de $\left[\left(a_{ij}\right)\left(b_{ij}\right)\right]\left(c_{ij}\right)$.Las leyes distributivas se prueban de manera análoga. Consideramos demostrado el siguiente teorema.

TEOREMA 1 Si F es un campo, entonces el conjunto $M_n(F)$ de todas las matrices cuadradas de elementos de F forma un anillo bajo la suma y multiplicación de matrices.

Estos anillos de matrices se usan en Algebra Lineal. En este contexto pueden considerarse correspondientes a ciertos tipos de funciones y, desde este punto de vista, se puede mostrar que la multiplicación de matrices es precisamente la composición de funciones. Como la composición de funciones siempre es asociativa, da otra demostración, más elegante, de la ley asociativa.

Nótese que $M_n(F)$ es no conmutativo si $n \geq 2$. El ejemplo 3 lo ilustra para $M_2(F)$.

EJEMPLO 3 Como todo campo F contiene elementos 0 y 1, $M_2(F)$ siempre tiene entre sus elementos a

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

La definición de multiplicación de matrices muestra que

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

mientras que

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Así, $M_2(F)$ es no conmutativo. Como

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

es la identidad aditiva, este ejemplo muestra, además, que existen divisores de cero en $M_2(F)$. Lo mismo es cierto sobre $M_n(F)$, para $n \geq 2$. Dejemos como ejercicio la demostración de que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

es el elemento unitario en $M_2(F)$. En donde 1 es la notación para la identidad de la multiplicación en el campo F y no necesariamente el número 1.

CONCLUSIONES

1. Establecer la importancia del estudio de las matrices y sus operaciones en la enseñanza de las Matemáticas a nivel medio.

2. $\langle M_n(R), + \rangle$ es un grupo abeliano.

3. $\langle M_n(R), \bullet \rangle$ no es un grupo.

4. Las matrices n x n, pero inversibles bajo la operación producto forman un grupo.

5. Todas las matrices diadonales no singulares forman un subgrupo del grupo de todas las matrices n x n.

6. El conjunto de las matrices de rotación bajo la multiplicación matricial común, es un grupo conmutativo.

7. $\langle M_n(R), +, \bullet \rangle$ es un anillo no conmutativo.

8. El conjunto $M_n(F)$ de todas las matrices n x n sobre un campo F forman un anillo bajo la suma y la multiplicación de matrices.

BIBLIOGRAFIA

1. ABELLANAS M., LODARES D. Matemática Discreta, Macrobit Editores, México. (1991).

2. BUDNICK Frank S. Matemáticas aplicadas para Administración, Economía y Ciencias Sociales, Mc Graw-Hill, México. (1990).

3. BUSH G., OBREANU P., Introducción a la Matemática Superior, Editorial F. Trillas, S.A.., México. (1968).

4. ENCICLOPEDIA DE MATEMATICA BASICA, Editorial Alhambra, España. (1979).

5. FRALEIGH John B., Algebra Abstracta, Addison-Wesley Iberoamericana, S.A., Estados unidos. (1987).

6. FRALEIGH John B. y BEAUREGARD Raymond A. Algebra Lineal, Addison-Wesley Iberoamericana, S. A.., Estados Unidos. (1989).

7. GARRETT B., SAUNDERS M., Algebra Moderna, Editorial Teide, España.(1953).

8. GERBER Harvey Algebra Lineal, Grupo Editorial Iberoamérica, México.(1992).

9. GOLOVINA L.I., Algebra Lineal y algunas de sus aplicaciones, Editorial Mir, Rusia. (1986).

10. GROSSMAN Stanley I., Algebra Lineal con aplicaciones, Mc Graw-Hill, México. (1991).

11. HERSTEIN I.N. Algabra Moderna, Editorial F. Trillas, S.A., México. (1970).

12. HERSTEIN I.N. y WINTER David, Algebra Lineal y Teoría de Matrices, Grupo Editorial Iberoamérica, México. (1989)

13. KREYSZIG Erwin, Matemáticas avanzadas para Ingeniería, Editorial Limusa S.A., México. (1991).

14. PITA RUIZ Claudio, Algebra Lineal, Mc Graw-Hill, México (1991).

15. PONTRIAGUIN L.S., Grupos Contínuos, Editorial Mir, Rusia.(1978).

16. ROSS Kenneth A.. y WRIGHT Charles, Matemáticas Discretas, Prentice-Hall Hispanoamericana S.A. México. (1991).

17. STRANG Gilbert, Algebra Lineal y sus aplicaciones, Fondo Educativo Interamericano, Estados Unidos. (1982).

18. WALLACE D.A.R., Grupos, Editorial Limusa, México.(1978).

19. WIGNER Eugene P. Teoría de Grupo, Acadenic Press, Inc., Estados Unidos. (1959).

20. WINTER David, Algebra de Matrices, Macmillan Publishing Company, Estados Unidos. (1992).