Fundación POLAR

Matemática Maravillosa

Matrices y aplicaciones

La presentación de las películas de la trilogía Matrix, toma como imagen códigos que contienen un mensaje sólo conocido por sus autores. El resultado final de dichos códigos es el nombre de la película. The Matrix (1999), The Matrix Reloaded (2002), The Matrix Revolutions (2004).

Fascículo 23

EMPRESAS POLAR
65 años cumpliéndole a Venezuela

Últimas Noticias

Matrices y códigos

Los códigos secretos han acompañado a la humanidad desde épocas remotas. Se emplean diferentes términos, para indicar que un mensaje ha sido escrito de manera que en principio sólo el destinatario lo pueda leer. Entre las palabras utilizadas para ello están: codificación, cifrado, encriptamiento,...

Se define la criptografía (del griego kryptos, "escondido", y graphein, "escribir") como el arte de enmascarar los mensajes con signos convencionales que sólo cobran sentido a la luz de una clave secreta.

Para mayor precisión, señalemos que se llama cifrado (codificación o transformación criptográfica) a una transformación del texto original que lo convierte en el llamado texto cifrado o criptograma. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.

SABÍAS QUE...

Ya en el año 450 a.C. los espartanos de Grecia enviaban mensajes codificados. Para ello enrollaban una banda de cuero o cinturón sobre un cilindro, se escribía el mensaje y al desenrollar la banda de cuero ésta parecía que sólo estaba adornada con marcas inocentes. Sin embargo, si el destinatario del mensaje arrollaba nuevamente la banda alrededor de un cilindro similar al utilizado cuando se escribió dicho mensaje, éste podía ser leído sin dificultad. Este método es un sistema de codificación por transposición.

En el cifrado por sustitución, cada letra o grupo de letras es reemplazada por una letra o grupo de letras. Uno de los más antiguos cifrados es el "Cifrado de César", atribuido a Julio César, quien sustituyó cada letra por la que ocupa tres puestos más allá en el alfabeto. Con ese método, *a* se convierte en *D*, *b* en *E*, *c* en *F*,..., y *z* en *C*.

Una técnica de codificación por sustitución fue utilizada por el insigne escritor estadounidense Edgar Allan Poe (1809-1849) en su célebre narración *El escarabajo de oro*. También este tipo de técnica aparece con frecuencia en diarios y pasatiempos en los cuales se le propone al lector la solución de un criptograma.

En el siglo XIII, Roger Bacon (1214-1294) describió varios métodos de codificación.

De trascendental importancia, durante la II Guerra Mundial, fue el hecho de que los estadounidenses lograran descifrar el código naval japonés JN25 y los ingleses hiciesen lo propio con la máquina alemana *Enigma*.

Actualmente se utilizan sofisticadas técnicas de encriptamiento de mensajes las cuales se basan en las propiedades de los números primos.

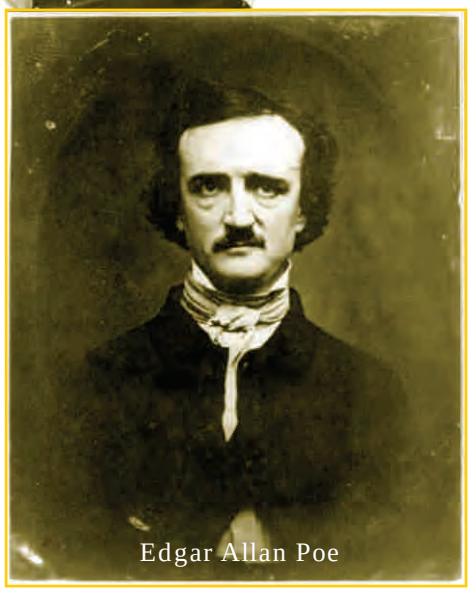
Uno de los sistemas modernos para encriptar mensajes es el criptosistema de clave pública. Uno de éstos es el sistema RSA (en honor de sus creadores los matemáticos Rivest, Shamir y Adler), el cual se basa en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos números primos grandes.

La máquina *Enigma* era un dispositivo para codificar mensajes empleado por los alemanes en la II Guerra Mundial.

El artefacto consistía de las siguientes partes:

- Un teclado con 26 letras
- Un tablero con 26 letras
- 3 ruedas con 26 letras cada una sobre un eje

Luego de la obtención por parte de los aliados de algunas de estas máquinas, el equipo polaco conformado por Jerzy Rozycki, Henryk Zygalski y Marian Rejewski, dedujeron el código. A raíz de esto, los alemanes complicaron el proceso mediante una doble codificación. Este nuevo proceso fue decodificado, en 1941, por el equipo de Bletchley Park encabezado por el matemático Alan Turing (Inglaterra, 1912-1954).


Edgar Allan Poe

En la obra de Poe *El escarabajo de oro* se señala:

Y al llegar aquí, Legrand, habiendo calentado de nuevo el pergamino, lo sometió a mi examen. Los caracteres siguientes aparecían de manera toscamente trazada, en color rojo, entre la calavera y la cabra:

53‡‡+305))6*;4826)4‡.)4‡);806*;48+8¶60))85;1‡ (;:‡*8
+83(88)5*+;46(;88*96*?;8)* ‡ (;485);5*+2:* ‡ (;4956*2(5*—
4)8¶8*;4069285);)6+8)4‡‡;1(‡9;48081;8:8‡1;48+85;4)485
+528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188; ‡?;

—Pero—dije, devolviéndole la tira—sigo estando tan a oscuras como antes. Si todas las joyas de Golconda esperasen de mí la solución de este enigma, estoy en absoluto seguro de que sería incapaz de obtenerlas.

El descifrador partió del supuesto de que el texto original estaba escrito en idioma inglés.

Ahora bien, la letra que se encuentra con mayor frecuencia en ese idioma, así como en el castellano, el alemán y el francés, es la e. Después, la serie en inglés es la siguiente: a o i d h n r s t u y c f g l m w b k p q x z.

Del criptograma se obtiene la siguiente tabla, en la cual aparecen en la primera fila los caracteres presentes en el mensaje codificado y en la segunda la frecuencia de aparición de éstos.

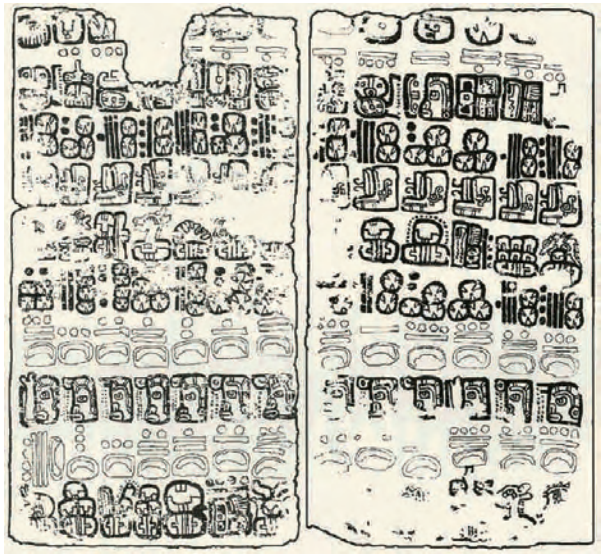
8	;	4	‡	)	*	5	6	(	+	1	0	9	2	:	3	?	¶	_
33	26	19	16	16	13	12	11	10	8	8	6	5	5	4	4	3	2	1

Luego, el 8 muy probablemente debe ser la letra e.

Además, el descifrado que se va logrando usando la tabla anterior conjuntamente con los conocimientos idiomáticos de la lengua inglesa, conduce en una etapa intermedia del proceso a esta otra tabla, en la cual en la fila superior están los caracteres que aparecen en el criptograma, y en la inferior el símbolo que les corresponde en el mensaje original.

5	+	8	3	4	6	*	‡	(	;	?
a	d	e	g	h	i	n	o	r	t	u

Códigos más complejos



Una técnica un poco más sofisticada consiste en el empleo del cifrado en dos pasos. Primero se le aplica al mensaje una sustitución, seguida luego de una transposición.

Para el primer paso consideremos el siguiente cifrado por sustitución:

Tabla Nº 1

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

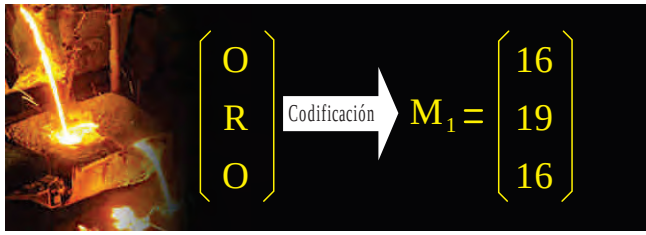
s	t	u	v	w	x	y	z	espacio	.	,
20	21	22	23	24	25	26	27	28	29	30

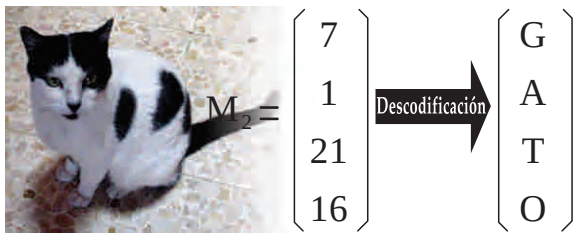
Como vemos en la Tabla Nº 1, a cada letra de nuestro alfabeto así como al espacio entre letras y a los signos de puntuación más usuales se les ha asignado un número. Esto matemáticamente corresponde a una función *f*, la cual además es biyectiva, por lo cual es posible efectuar el proceso inverso: pasar de los números a las letras o signos que ellos representan.

Así, por ejemplo, la palabra ORO quedaría codificada como 16 19 16.

Por su parte, 7 1 21 16 es la codificación de la palabra gato.

De aquí en adelante usaremos la notación matricial para representar las palabras. Lo anterior quedaría representado como se muestra a la derecha.





Pasemos ahora a un segundo paso o nivel de codificación, multiplicando por la izquierda (premultiplicando) la matriz M_i que representa al mensaje que queremos codificar, por una matriz *C* que llamaremos Matriz de Codificación.

C no puede ser cualquier matriz. *C* debe cumplir dos condiciones:

1. El número de columnas de C debe ser igual al número de filas de M_i.
2. Debe ser posible realizar el proceso inverso, la descodificación, para lo cual C debe poseer inversa. A la inversa C^{-1} la llamaremos Matriz de Descodificación.

La función *f* y la matriz *C* son las claves secretas que permiten codificar (y sus inversas descodificar) cualquier mensaje.

Consideremos el mensaje ACA

Usando $C\begin{pmatrix}0&2&3\\1&4&7\\2&3&6\end{pmatrix}$ como matriz de codificación, se tiene $CM_3=\begin{pmatrix}0&2&3\\1&4&7\\2&3&6\end{pmatrix}\begin{pmatrix}1\\3\\1\end{pmatrix}=\begin{pmatrix}9\\20\\17\end{pmatrix}$

Así obtenemos que: $\begin{pmatrix}1\\3\\1\end{pmatrix}$ ⟹ luego de codificado o cifrado por transposición produce: $\begin{pmatrix}9\\20\\17\end{pmatrix}$

En términos alfabéticos, aplicando la Tabla Nº 1, CM_3 es ISP.

Observe que C posee 3 columnas, es igual al número de filas de M_1. Además se tiene que:

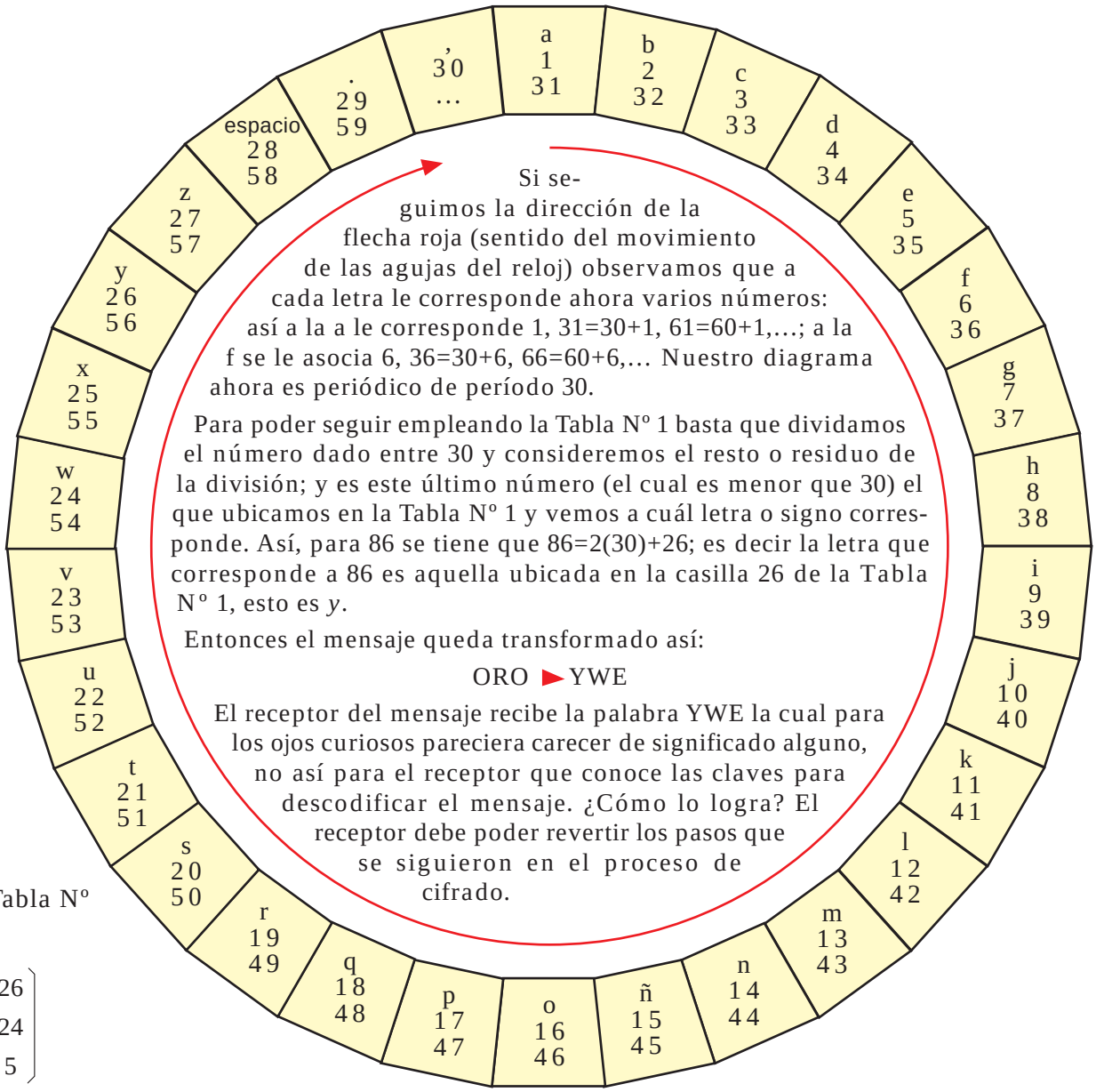
$$\begin{pmatrix}0&2&3\\1&4&7\\2&3&6\end{pmatrix}\begin{pmatrix}3&-3&2\\8&-6&3\\-5&4&-2\end{pmatrix}=\begin{pmatrix}3&-3&2\\8&-6&3\\-5&4&-2\end{pmatrix}\begin{pmatrix}0&2&3\\1&4&7\\2&3&6\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

Luego $C^{-1}=\begin{pmatrix}3&-3&2\\8&-6&3\\-5&4&-2\end{pmatrix}$ es la inversa de C.

Volvamos al mensaje ORO, entonces $CM_1=\begin{pmatrix}0&2&3\\1&4&7\\2&3&6\end{pmatrix}\begin{pmatrix}16\\19\\16\end{pmatrix}=\begin{pmatrix}86\\204\\185\end{pmatrix}$

Si queremos reescribir CM_1 en términos alfabéticos, nos tropezamos con el inconveniente de que todas las entradas de la matriz CM_1 resultaron números mayores que 30 y, en consecuencia, es inaplicable la Tabla Nº 1. ¿A qué letra corresponde, por ejemplo, 86? ¿Qué modificaciones debemos hacerle a nuestro proceso para solventar esta situación?

Si observamos la Tabla Nº 1, y en lugar de mirar una disposición lineal como la allí mostrada la pensamos como un diagrama cerrado, haciendo coincidir los dos extremos, obtenemos una representación como la que se presenta a continuación:



Empleando la Tabla Nº 1 se tiene:

$$\begin{pmatrix} Y \\ W \\ E \end{pmatrix} \Longrightarrow \begin{pmatrix} 26 \\ 24 \\ 5 \end{pmatrix}$$

Como queremos descodificar el mensaje recibido hemos de emplear la matriz C^{-1}:

$$C^{-1}\begin{pmatrix} 26 \\ 24 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 2 \\ 8 & -6 & 3 \\ -5 & 4 & -2 \end{pmatrix}\begin{pmatrix} 26 \\ 24 \\ 5 \end{pmatrix} = \begin{pmatrix} 16 \\ 79 \\ -44 \end{pmatrix} \qquad \begin{pmatrix} 16 \\ 79 \\ -44 \end{pmatrix} \Longrightarrow$$

16	O
79=2(30)+19	R
-44	?

¿A cuál letra corresponde -44?

-44=-2(30)+16, es decir que hemos realizado dos vueltas completas en el sentido opuesto a las agujas del reloj, y de seguidas, hemos avanzado 16 casillas en el sentido de las agujas del reloj; pero 16 corresponde a la letra O. La palabra descodificada entonces es ORO, como era de esperarse.


L'ALGEBRA
PARTE MAGGIORE
DELL'ARIMETICA
DI RAFAEL BOMBELLO
BOLOGNESE.
Libro Secondo.

Matrices y números complejos

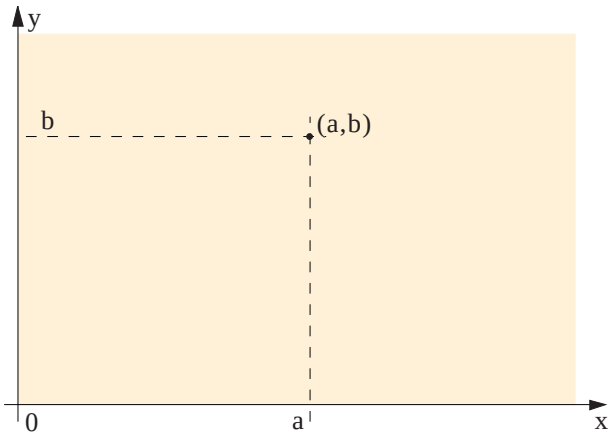
En el conjunto de los puntos P del plano, de coordenadas (x,y), podemos definir las operaciones de adición y multiplicación como se indica a continuación:

(a ,b) + (c ,d) = (a+c , b+d) (a , b) (c , d) = (ac-bd , ad+bc)

Estas operaciones cumplen propiedades similares a las operaciones de adición y multiplicación de los números reales: asociatividad, conmutatividad y existencia de elemento neutro para ambas operaciones; existencia de opuesto aditivo y de inverso multiplicativo (si es distinto de (0,0)); y distributividad de la multiplicación respecto a la adición.

Este conjunto de puntos con estas dos operaciones es lo que se conoce como el cuerpo de los números complejos. El punto (0, 0) es el elemento neutro para la adición, mientras que el punto (1, 0) lo es para la multiplicación.

Los números complejos los hemos representado como pares de números de la forma (a , b). Otra manera de representarlos es utilizando la forma binómica $a+bi$, donde i es la unidad imaginaria, solución de la ecuación x^2-1 (que no tiene solución real) y está dada por i = (0 , 1).



Existen otras maneras de representar los números complejos.

Una de ellas es utilizando las matrices cuadradas de orden 2.

Si identificamos cada número complejo (a,b) con el vector columna $\begin{pmatrix} a \\ b \end{pmatrix}$ y usamos las operaciones con matrices podemos escribir:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Considerando la matriz identidad y la matriz de rotación de 90° en sentido antihorario $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, la expresión anterior la podemos reescribir:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}\right)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

De esta manera, todo número complejo los podemos escribir como el trasformado del vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ por una matriz del tipo $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, y así podemos tomar esta matriz como una representación del número complejo.

INTERESANTE

Con esta identificación la unidad imaginaria se representa por la matriz

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

Si multiplicamos esta matriz por sí misma, resulta:

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

De esta manera la matriz A es solución de la "ecuación matricial" $X^2 = -I$

Matrices y sistemas de ecuaciones lineales

Un comerciante le dice a un empleado que le cambie en el banco 10 000 bolívares en 150 monedas de Bs 100 y Bs 20.

Denotando por *x* el número de monedas de Bs 100 requeridas y por *y* el número de monedas de Bs 20, este simple problema se traduce en resolver las 2 ecuaciones:

$$\begin{cases} 100x + 20y = 10\,000 \\ x + y = 150 \end{cases}$$

En general, tenemos que un sistema de ecuaciones con dos incógnitas se expresa por:

$$\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{cases}$$

Sistema de ecuaciones lineales con 2 incógnitas; x e y son las incógnitas y a_1, a_2, b_1, b_2, c_1 y c_2 son conocidos.

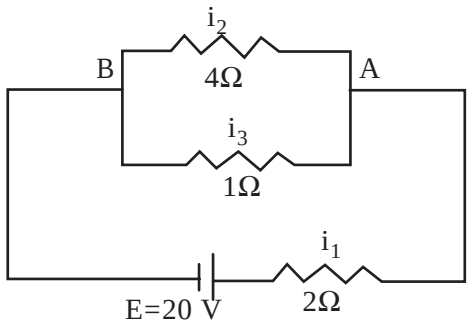
Forma matricial

$$\text{Si } A=\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \quad X=\begin{pmatrix} x \\ y \end{pmatrix} \quad X'=\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$$AX=C$$

Consideremos el circuito eléctrico mostrado en la figura, donde tenemos una fuente de 20V y tres resistencias: de 1 ohmn, 2 ohmnios y de 4 omnios. De acuerdo a las leyes de Kirchoff, se tienen las siguientes relaciones lineales entre las intensidades.



$$\begin{cases} i_1 - i_2 - i_3 = 0 \\ 2i_1 + 4i_2 = 20 \\ 2i_1 + i_3 = 20 \end{cases}$$

Esto da un sistema lineal con 3 incógnitas.

A es una matriz
X matriz de incógnitas
X' matriz conocida

$$\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \end{cases}$$

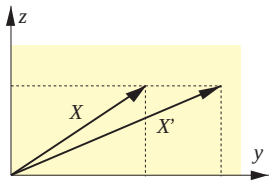
Forma matricial

$$A=\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \end{cases}, \quad X=\begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad X'=\begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix}$$

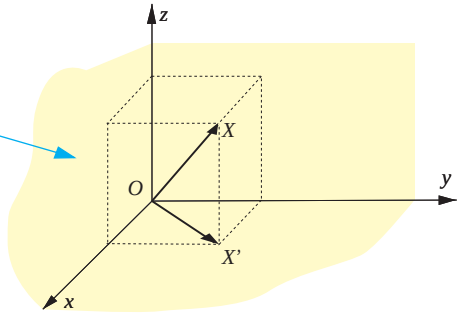
$$AX = X'$$

Al escribir un sistema de ecuaciones de la forma AX=X', podemos pensar a la matriz A como una transformación o función que transforma el vector X en el vector X'.

$$\text{Si } A=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ y } X=\begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ entonces } AX=\begin{pmatrix} 2 \\ 1 \end{pmatrix}$$



$$\text{Si } A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ y } X=\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \text{ entonces } AX=\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$



Estos fascículos están disponibles en línea, visitando la página web:
http://www.fpolar.org.ve/matematica3