Definición 1. Un cuerpo K es un conjunto con dos operaciones, + y \cdot que satisface las siguientes propie-

1.
$$(a + b) + c = a + (b + c)$$

1.
$$(a + b) + c = a + (b + c)$$

2. a + b = b + a

3. Existe 0 tal que
$$a + 0 = a$$

4. Para todo a existe
$$-a$$
 tal que $a + (-a) = 0$
8. Para todo $a \neq 0$ existe a^{-1} tal que $aa^{-1} = 1$

5.
$$(ab)c = a(bc)$$

6.
$$ab = ba$$

7. Existe 1 tal que
$$a1 = a$$

8. Para todo
$$a \neq 0$$
 existe a^{-1} tal que $aa^{-1} = 1$

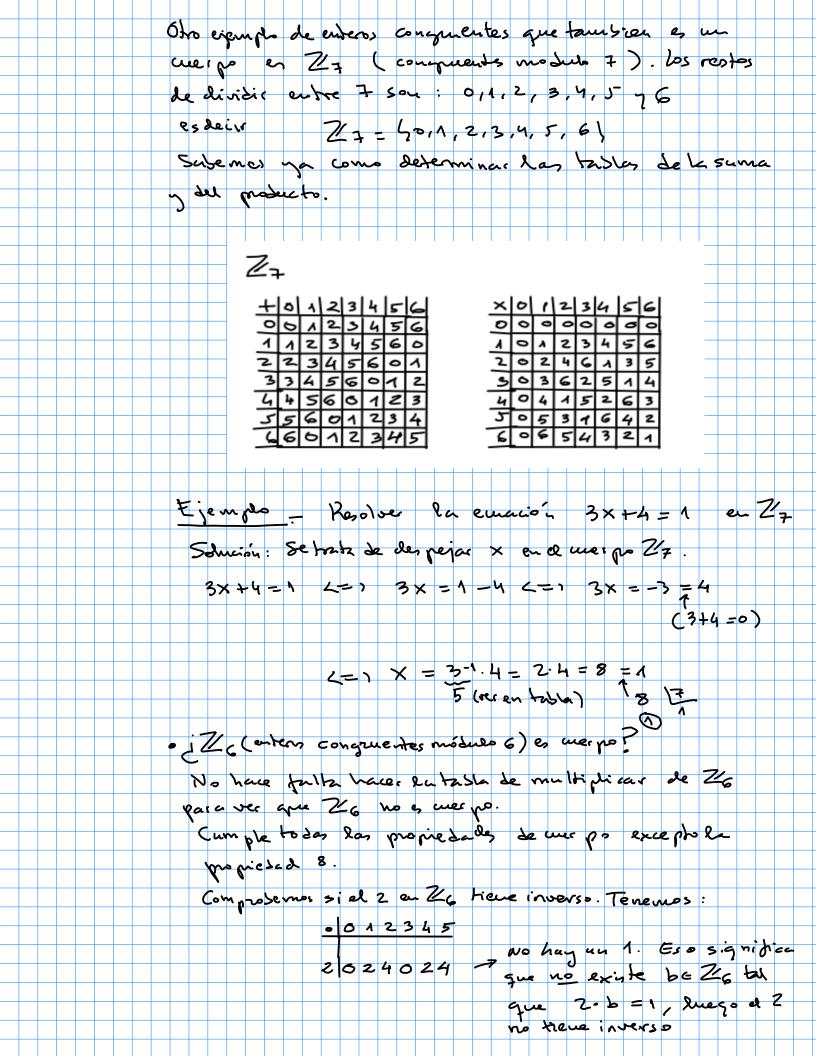
9.
$$(a+b)c = ac + bc$$

e, un overpo.

Através de las tablas, vers que

5) 5

47=4 Al operar en 25 et valor rentante es et reso de dividir el n's mero entre 5. Enhonces en 2/5 se en bice que · Cualquier multiple de 5 es 0 (que es cl resto de dividir dido vi verp entre 5) · Chalquier número de la jorna 52+1 en 25 es 1 (5a+1 4 a , a) dividires entre 5 du resto 1) y asi suceivamente. En Z; et questo de a, enderir -a en aquel valor b de 7/5 tal at besum miltipo de 5 (osea que es 0) -2=3 yus 2+3=5=0 -4=1 que 4+1=5=0 Posemos plantearnos de terminar inversos y spuestos de nºs marpos que 5 e indus. valors negativos. Por ejampo i 125) y -2? en 25 . Any a commar el i noerse de 12, reduinner el 13 en 25 · I gual que antes 7 = 2 (en 2/5) liee go -7 = -2 = 3 In electo -7 = 3 pues 7 + 3 = 0 en 2/5. Ejemplo - Resolver la emación 3x+4=1 en 2/5 Someon: Se bosts de des pejas x en a mes po 2/5. 3x+4=1 4=1 3x=1-4 4=1 3x=-3=2 <= > × = 3-1.2 = 2.2 = 4//



Adomás del 2, tamposo tiene inverso el 3 mi el 4 Sin emburgo en 26: 1-1=1 y 5-1=5 (fácil de comprodar) Otra propiedad acciosa, por ejembs en que en 26 2 \$0, 3 \$0 y in embargo 2.3 = 0 Esa propiedad no se da en los acerpos. De hecho sasemos que an un une coo x a.b = 0 = > a = 0 6 b = 0 (0 ambes) Acreles elements no mules a (a 70) par la que existe un elevento b to o tol que a b = 0, se denomina " divisors de cen'. En resumen: en un cue i po no hay divisores de cero. **MATRICES** • Una matriz de tamaño $m \times n$ sobre un cuerpo K es un conjunto de elementos de K ordenados en mfilas y n columnas. El conjunto de todas las matrices de tamaño m × n sobre K se denotará M_{m×n}(K). Si A es una matriz de M_{m×n}(K), i ∈ {1,2,···,m} y j ∈ {1,2,···,n} denotaremos A_{ij} al elemento de K que hay en la fila i y columna j de la matriz. Dos matrices A y B son iguales si tienen el mismo tamaño y A_{ij} = B_{ij} para todo i y j. Las operaciones que se hacen entre elementos del cuerpo inducen operaciones en el conjunto de las matrices. Son las siguientes: Multiplicación de un elemento λ ∈ K por una matriz A. El producto se hará componente a componente, es decir $(\lambda \cdot A)_{ij} = \lambda \cdot A_{ij}$. Suma de matrices. Para sumar dos matrices tienen que tener exactamente el mismo tamaño y la suma se realiza componente a componente, es decir, $(A + B)_{ij} = A_{ij} + B_{ij}$. Producto de matrices. Dos matrices A y B se pueden multiplicar si y solo si el número de columnas de A es igual al número de filas de B. Si A es de tamaño $m \times n$ y B de tamaño $n \times p$, el producto AB será una matriz de tamaño $m \times p$ definida como $(AB)_{ij} = A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj}$. El elamento (i, j) de la matirir pombuelo A·B coloquialmente

se exmerce como

anterior mente aunçle:

2 como

(Air Air - Air) X

(B)

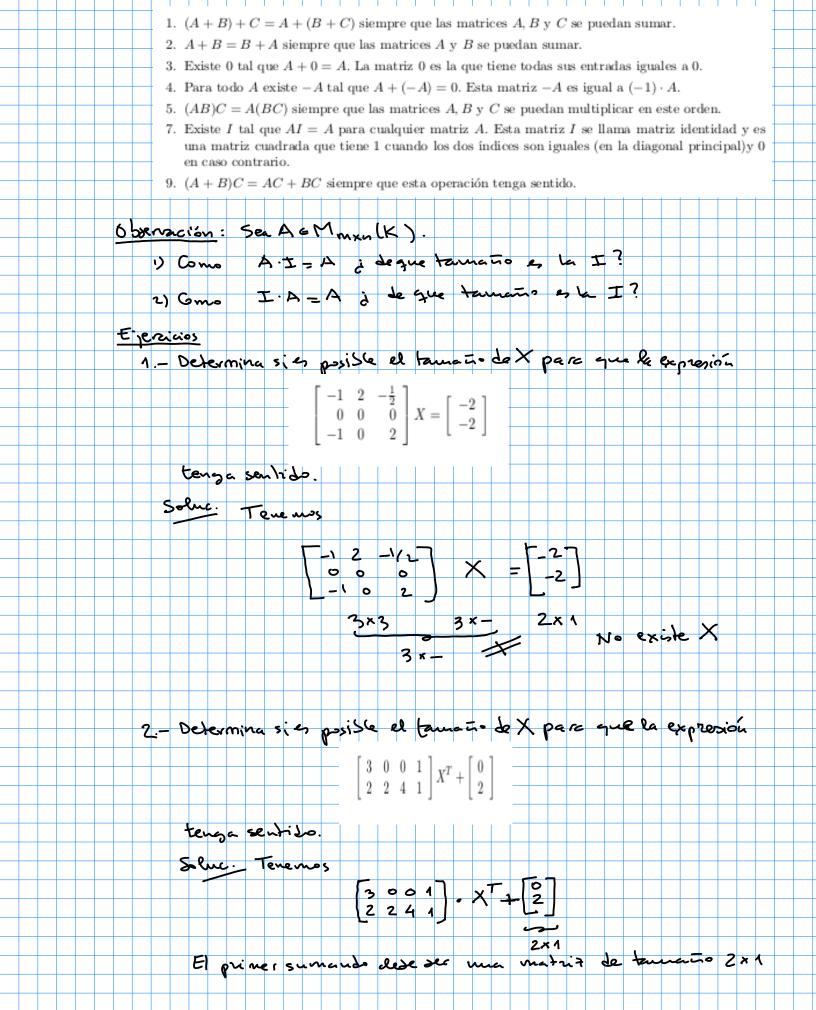
(B)

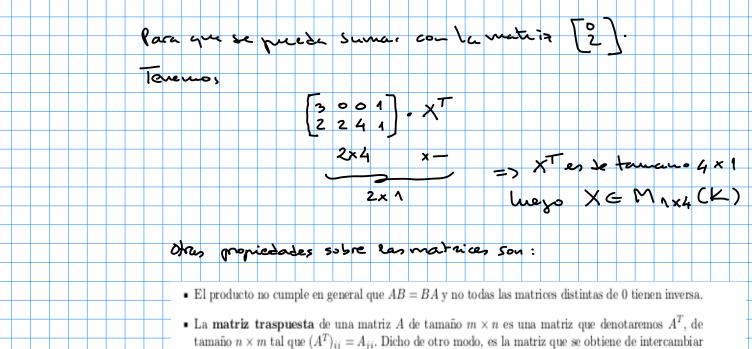
(producto de la file i de A

(Bnj)

(por la columna j de B)

El conjunto Mmxn (K), con la suma y el producto depinidos





- tamaño $n \times m$ tal que $(A^T)_{ij} = A_{ji}$. Dicho de otro modo, es la matriz que se obtiene de intercambiar filas con columnas.
- La matriz traspuesta cumple que (AB)^T = B^TA^T siempre que A y B se puedan multiplicar.

Aritmetica Modular

Definición 1. Sea n entero positivo y sean $a, b \in \mathbb{Z}$. Diremos que a y b son congruentes módulo n (lo escribiremos $a \equiv b \pmod{n}$, $a \equiv b \pmod{n}$ o simplemente a = b cuando estemos sobre un módulo fijo) cuando a-b sea un múltiplo de n, es decir, cuando a-b=nt para algún $t \in \mathbb{Z}$.

Denotaremos \mathbb{Z}_n al conjunto $\{0, 1, 2, \dots, n-1\}$ con las operaciones definidas salvo múltiplos de n.

Proposición 2. Para cualquier entero positivo n y cualquier a en \mathbb{Z} , existe un elemento $r \in \{0, 1, \dots, n-1\}$ tal que $a \equiv r \pmod{n}$. Esto garantiza que el resultado de cualquier operación aritmética en \mathbb{Z}_n se podrá poner de nuevo en \mathbb{Z}_n eligiendo este elemento r que llamaremos reducido módulo n correspondiente a a.

Demostración. Si dividimos a entre n tenemos un cociente q y un resto r enteros. El resto será un número menor que el divisor, es decir, entre 0 y n-1, y se cumplirá la relación fundamental de que dividendo es igual a divisor por cociente más resto. Es decir,

$$a = nq + r$$

por lo tanto a - r = nq que es un múltiplo de n y por lo tanto $a \equiv r \pmod{n}$.

Al hacer operaciones en aritmética modular, no es necesario estar reduciendo constantemente al elemento más reducido posible. No hay ningún problema si se suman o restan múltiplos del módulo en cualquier operación intermedia. Esto permite una mayor agilidad a la hora de operar.

Zn como sasemos son los restes de dividir entre n La suma + y el producto o en Zu se determina como:
Va, be Zn ato en Zu es el resto de disdir e "entero" at b entre n. ab en Z/n en el resto de dividir "entero" a.b entre n

Zn con estos o peracious definidas tiene las mismas

propriedad que el conjunto de los enteros Z.

Se cumplen todas has propriedades del concepto de cuerpo excepto la propriedad 8, relativa a la existencia de inverso para curquier elemento to. No siempro se cumple.

Operaciones elementales

Definición 1. Existen tres tipos de operaciones elementales por filas que se pueden realizar a una matriz $A \in \mathbf{M}_{m \times n}(K)$:

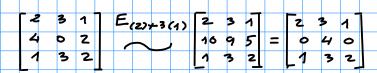
- Multiplicar la fila p por la constante λ ∈ K distinta de 0. Esta operación la denotaremos E_{λ(p)}.
- Suma a la fila p, la fila q (distinta de p) multiplicada por λ. Esta operación la denotaremos E_{(p)+λ(q)}.
- Intercambiar la fila p con la fila q. Esta operación la denotaremos E_(p,q).

Proposición 2. Las operaciones elementales por filas son invertibles.

Demostración.

$$E_{\lambda(p)}^{-1} = E_{\lambda^{-1}(p)} \qquad E_{(p)+\lambda(q)}^{-1} = E_{(p)+(-\lambda)(q)} \qquad E_{(p,q)}^{-1} = E_{(p,q)}.$$

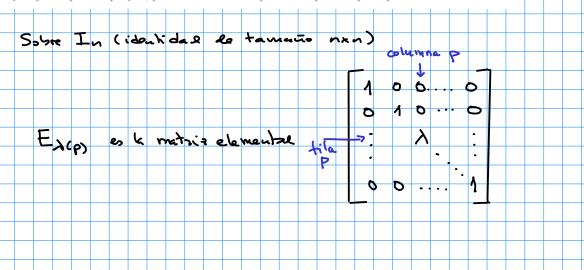
E, 2-

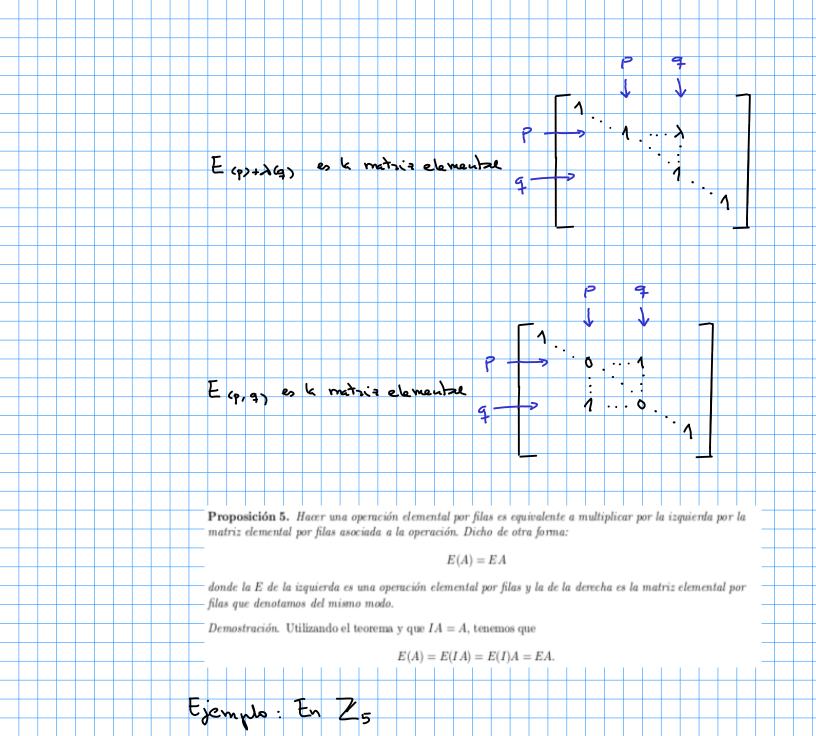


Teorema 3. Dada una operación elemental por filas E y un producto de matrices AB se cumple que

$$E(AB) = E(A)B.$$

Definición 4. Llamaremos matrices elementales por filas a aquellas que resultan de hacer las operaciones elementales por filas sobre la matriz identidad I. Denotaremos de la misma forma a la matriz elemental por filas y a la operación por filas, por lo tanto tendremos que EI = E para cualquier operación elemental E.

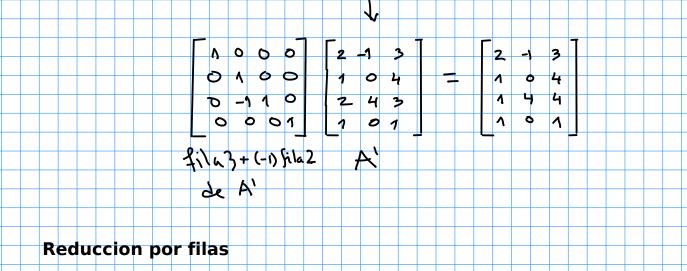




fila tercera

de A mutiplicada

AI



Para calcular la matriz reducida completa de una matriz A realizaremos los siguientes pasos:

- I. Para cada una de las filas $i = 1, 2, \dots, m$, si no son filas nulas, hacer:
 - Buscar el primer elemento no nulo de la fila i. Este elemento se llamará elemento pivote y la columna que lo contiene columna pivote.
 - 2. Si el pivote no es 1, convertirlo en un 1 multiplicando la fila por el inverso del pivote.
 - Eliminar todos los elementos no nulos que haya encima y debajo del pivote realizando operaciones elementales del segundo tipo.
- II. Ordenar las filas con operaciones del tercer tipo, de forma que las filas nulas estén debajo y que cada pivote esté más a la derecha que el pivote de la fila superior.

Cuando realicemos las operaciones en este orden preciso, diremos que será el orden estricto explicado en clase. Este método siempre funciona, pero cuando tengamos más práctica, veremos que dependiendo de los valores concretos que aparezcan en la matriz, se podrá intercambiar el orden de las operaciones. También veremos que a veces no es necesario obtener la reducida completa y únicamente con una matriz parcialmente reducida tenemos información suficiente. De momento calcularemos la reducida completa y en este orden.

Teorema 1 (Teorema Fundamental de la Reducción por Filas). Sea A una matriz, [A|I] la matriz ampliada con la matriz identidad a la derecha. Si realizamos el proceso de reducción por filas a la matriz ampliada [A|I] para obtener [R|P], entonces se cumple que

$$PA = R$$
.

A esta matriz P se le llamará matriz de paso.

Demostración. Supongamos que para pasar de la matriz A a la reducida R hay que hacer las siguientes operaciones elementales:

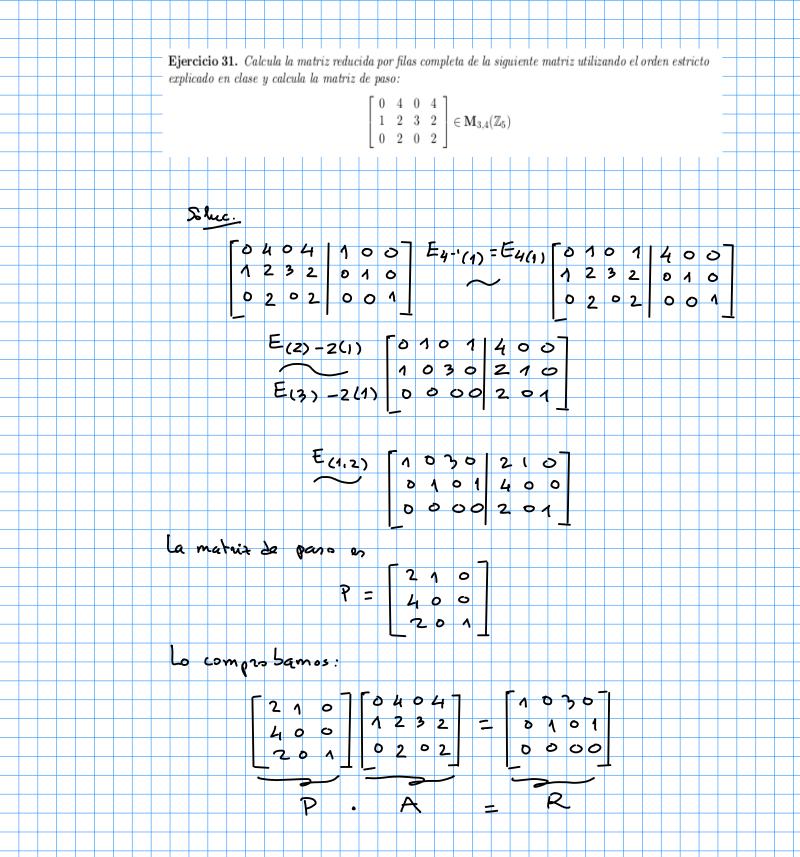
$$E_t E_{t-1} \cdot \cdot \cdot E_3 E_2 E_1 A = R$$

Si realizamos las mismas operaciones sobre la matriz ampliada [A|I] lo que obtenemos es

$$E_t E_{t-1} \cdots E_3 E_2 E_1 [A|I] = [E_t E_{t-1} \cdots E_3 E_2 E_1 A | E_t E_{t-1} \cdots E_3 E_2 E_1 I],$$

Y si llamamos $P = E_t E_{t-1} \cdots E_3 E_2 E_1$, entonces mirando la parte izquierda de la matriz, tenemos el resultado del teorema, que PA = R.

Nota 2. Cuando hagamos operaciones por filas a la matriz ampliada, solo buscaremos pivotes hasta la línea vertical, es decir, si por ejemplo la matriz A tiene una fila nula, pero a la derecha tiene valores no nulos, la consideraremos una fila nula y la pondremos al final sin hacer pivotes más allá de la línea. Si en alguna ocasión nos pasamos y hacemos pivotes en esa parte, el teorema también será cierto (incluso es cierto si no hacemos la reducida completa), pero simplemente habremos hecho operaciones innecesarias.



Sistemas de Ecuaciones y reduccion

Teorema 1. Sea [A|B] la matriz ampliada del un sistema de ecuaciones y E una operación elemental por filas. Entonces el sistema asociado a [EA|EB] tiene exactamente las mismas soluciones que el sistema asociado a [A|B].

Demostración. X es solución de [A|B] si y solo si AX = B, pero AX = B si y solo si EAX = EAB por ser E una operación elemental invertible, y eso es equivalente a que X sea solución de [EA|EB].

Proposición 2. Las soluciones de un sistema de ecuaciones con matriz ampliada [A|B] son las mismas que las del sistema asociado a la matriz reducida por filas de [A|B] (que llamaremos **sistema reducido**).

Demostración. La matriz reducida se obtiene aplicando una sucesión de operaciones elementales por filas $E_k \cdots E_2 E_1[A|B]$. Aplicando en cada paso el teorema anterior, concluimos el resultado de la proposición. \square

Para resolver un sistema de ecuaciones, procederemos del siguiente modo:

Teorema 3. Sea [A|B] la matriz ampliada de un sistema de ecuaciones lineales y R su matriz reducida por filas.

- Si la columna de los términos independientes es una columna pivote, entonces el sistema no tiene solución. Diremos que el sistema es incompatible.
- Si eso no sucede, haremos parámetros las variables correspondientes a las columnas no pivote y depejaremos el resto de las variables respecto a ellas.
 - a) Si todas las columnas de la parte de los coeficientes son pivotes, entonces la solución es única.
 Diremos que el sistema es compatible determinado.
 - b) Si no, las soluciones dependerán de los parámetros que puden tomar cualquier valor en el cuerpo K. Diremos que el sistema es compatible indeterminado.

Ejercicio 30. Estudia y resuelve si es posible el siguiente sistema de ecuaciones sobre el cuerpo de 5 elementos :

$$x_1 + x_2 - x_4 = 4$$
$$-x_1 - x_2 + x_3 + 3x_4 = 0$$
$$2x_1 + 2x_2 - x_3 + x_4 = 4$$

