**Definición 1.** *Un cuerpo $K$ es un conjunto con dos operaciones, $+$ y $\cdot$ que satisface las siguientes propiedades:*

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* $a+(-a) = 0$
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. $(a+b)c = ac+bc$

Obviamente las operaciones $+$ y $\cdot$ son cerradas en $K$, es decir

$\forall a,b \in K \quad a+b \in K$ y $a \cdot b \in K$

Ejemplos de cuerpos son: $\mathbb{R}$ (nºs reales)
$\mathbb{Q}$ (nºs racionales)

$\mathbb{Z}$ (nºs enteros) No es un cuerpo. La propiedad 8 sólo se cumple para $1$ y $-1$. De hecho $1^{-1} = 1$ y $(-1)^{-1} = -1$

Existen otros cuerpos. Por ejemplo, llamemos

$$\mathbb{Z}_5 = \{0,1,2,3,4\}.$$

(conjunto de los enteros "congruentes módulo 5")

$\mathbb{Z}_5$ está formado únicamente por los restos de dividir entre 5

$\mathbb{Z}_5$ con las operaciones dadas en las tablas:

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| · | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

es un cuerpo.

A través de las tablas, vemos que

$1^{-1} = 1$, pues $1 \cdot 1 = 1$

$2^{-1} = 3$, pues $2 \cdot 3 = 1$ (de hecho $2 \cdot 3 = 6 = 5 + 1 = 0 + 1 = 1$)

$$\begin{array}{r|l} 5 & 5 \\ \hline 0 & 1 \end{array} \qquad \begin{array}{r|l} 6 & 5 \\ \hline 1 & 1 \end{array}$$

$3^{-1} = 2$, pues $3 \cdot 2 = 6 = 5 + 1 = 0 + 1 = 1$

$4^{-1} = 4$

Al operar en $\mathbb{Z}_5$ el valor resultante es el resto de dividir el número entre 5.

Entonces en $\mathbb{Z}_5$ se verifica que

- Cualquier múltiplo de 5 es 0 (que es el resto de dividir dicho número entre 5)
- Cualquier número de la forma $5\mathbb{Z}+1$, en $\mathbb{Z}_5$ es 1 ($5a+1$ $\forall a$, al dividirlo entre 5 da resto 1)

y así sucesivamente.

En $\mathbb{Z}_5$ el opuesto de $a$, es decir $-a$ es aquel valor $b$ de $\mathbb{Z}_5$ tal $a+b$ es un múltiplo de 5 (osea que es 0)

$-2 = 3$ pues $2+3 = 5 = 0$

$-4 = 1$ pues $4+1 = 5 = 0$

Podemos plantearnos determinar inversos y opuestos de nºs mayores que 5 e incluso valores negativos. Por ejemplo

¿ $13^{-1}$ y $-7$? en $\mathbb{Z}_5$

- Antes de calcular el inverso de 13, reducimos el 13 en $\mathbb{Z}_5$ así

$$13 = 3 \quad \text{luego} \quad 13^{-1} = 3^{-1} = 2$$

En efecto $13 \cdot 2 = 26 = 1$.

$$26 \,\underline{|5}$$
$$\ \ 1 \quad 5$$

- Igual que antes $7 = 2$ (en $\mathbb{Z}_5$) luego $-7 = -2 = 3$

En efecto $-7 = 3$ pues $7+3 = 0$ en $\mathbb{Z}_5$.

<u>Ejemplo</u>.- Resolver la ecuación $3x+4=1$ en $\mathbb{Z}_5$

Solución: Se trata de despejar $x$ en el cuerpo $\mathbb{Z}_5$.

$$3x+4=1 \iff 3x = 1-4 \iff 3x = -3 = 2$$
$$\iff x = \underbrace{3^{-1}}_{2} \cdot 2 = 2 \cdot 2 = 4 \,//$$

Otro ejemplo de enteros congruentes que también es un cuerpo es $\mathbb{Z}_7$ (congruentes modulo 7). Los restos de dividir entre 7 son: 0, 1, 2, 3, 4, 5 y 6

es decir $$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

Sabemos ya como determinar las tablas de la suma y del producto.

$\mathbb{Z}_7$

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

<u>Ejemplo</u>.- Resolver la ecuación $3x+4=1$ en $\mathbb{Z}_7$

Solución: Se trata de despejar $x$ en el cuerpo $\mathbb{Z}_7$.

$$3x+4=1 \iff 3x = 1-4 \iff 3x = -3 = 4 \quad (3+4=0)$$

$$\iff x = \underbrace{3^{-1}}_{5 \text{ (ver en tabla)}} \cdot 4 = 2\cdot 4 = 8 = 1 \qquad 8 \,\underline{|7}\ ;\ 1$$

(1)

- ¿$\mathbb{Z}_6$ (enteros congruentes módulo 6) es cuerpo?

No hace falta hacer la tabla de multiplicar de $\mathbb{Z}_6$ para ver que $\mathbb{Z}_6$ no es cuerpo.

Cumple todas las propiedades de cuerpo excepto la propiedad 8.

Comprobemos si el 2 en $\mathbb{Z}_6$ tiene inverso. Tenemos:

| · | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |

→ no hay un 1. Eso significa que <u>no</u> existe $b \in \mathbb{Z}_6$ tal que $2\cdot b = 1$, luego el 2 no tiene inverso

Además del 2, tampoco tiene inverso el 3 ni el 4

Sin embargo en $\mathbb{Z}_6$ : $1^{-1}=1$ y $5^{-1}=5$ (fácil de comprobar)

Otra propiedad curiosa, por ejemplo es que en $\mathbb{Z}_6$

$$2 \neq 0, \quad 3 \neq 0 \quad \text{y sin embargo} \quad 2\cdot 3 = 0$$

Esa propiedad no se da en los cuerpos. De hecho sabemos que en un cuerpo $K$,

$$a\cdot b = 0 \Rightarrow a=0 \text{ ó } b=0 \text{ (o ambos)}$$

Aquellos elementos no nulos $a$ ($a\neq 0$) para los que existe un elemento $b\neq 0$ y tal que $a\cdot b = 0$, se denominan "divisores de cero".

En resumen: en un cuerpo 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 $m$ filas y $n$ columnas.
- El conjunto de todas las matrices de tamaño $m\times n$ sobre $K$ se denotará $\mathbf{M}_{m\times n}(K)$.
- Si $A$ es una matriz de $\mathbf{M}_{m\times n}(K)$, $i\in\{1,2,\cdots,m\}$ y $j\in\{1,2,\cdots,n\}$ 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:
  1. Multiplicación de un elemento $\lambda\in K$ por una matriz $A$. El producto se hará componente a componente, es decir $(\lambda\cdot A)_{ij}=\lambda\cdot A_{ij}$.
  2. Suma de matrices. Para sumar dos matrices tienen que tener exactamente el mismo tamaño y la suma se realiza componente a componente, es decir, $(A+B)_{ij}=A_{ij}+B_{ij}$.
  3. 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 elemento $(i,j)$ de la matriz producto $A\cdot B$ coloquialmente se expresa como

$$(A_{i1}\ A_{i2}\ \cdots\ A_{in})\times\begin{pmatrix}B_{1j}\\ B_{2j}\\ \vdots\\ B_{nj}\end{pmatrix}$$ (producto de la fila $i$ de $A$ por la columna $j$ de $B$)

El conjunto $M_{m\times n}(K)$, con la suma y el producto definidos anteriormente cumple:

1. $(A+B)+C = A+(B+C)$ siempre que las matrices $A$, $B$ y $C$ se puedan sumar.
2. $A+B = B+A$ siempre que las matrices $A$ y $B$ se puedan sumar.
3. Existe $0$ tal que $A+0 = A$. La matriz $0$ es la que tiene todas sus entradas iguales a $0$.
4. Para todo $A$ existe $-A$ tal que $A+(-A) = 0$. Esta matriz $-A$ es igual a $(-1)\cdot A$.
5. $(AB)C = A(BC)$ siempre que las matrices $A$, $B$ y $C$ se puedan multiplicar en este orden.
7. Existe $I$ tal que $AI = A$ para cualquier matriz $A$. Esta matriz $I$ se llama matriz identidad y es una matriz cuadrada que tiene 1 cuando los dos índices son iguales (en la diagonal principal)y 0 en caso contrario.
9. $(A+B)C = AC+BC$ siempre que esta operación tenga sentido.

**Observación:** Sea $A \in M_{m\times n}(K)$.

1) Como $A\cdot I = A$ ¿de que tamaño es la $I$?

2) Como $I\cdot A = A$ ¿de que tamaño es la $I$?

**Ejercicios**

1.- Determina si es posible el tamaño de $X$ para que la expresión

$$\begin{bmatrix} -1 & 2 & -\frac{1}{2} \\ 0 & 0 & 0 \\ -1 & 0 & 2 \end{bmatrix} X = \begin{bmatrix} -2 \\ -2 \end{bmatrix}$$

tenga sentido.

Soluc. Tenemos

$$\underbrace{\underset{3\times 3}{\begin{bmatrix} -1 & 2 & -1/2 \\ 0 & 0 & 0 \\ -1 & 0 & 2 \end{bmatrix}} \underset{3\times -}{X}}_{3\times -} \neq \underset{2\times 1}{\begin{bmatrix} -2 \\ -2 \end{bmatrix}}$$

No existe $X$

2.- Determina si es posible el tamaño de $X$ para que la expresión

$$\begin{bmatrix} 3 & 0 & 0 & 1 \\ 2 & 2 & 4 & 1 \end{bmatrix} X^T + \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$

tenga sentido.

Soluc. Tenemos

$$\begin{bmatrix} 3 & 0 & 0 & 1 \\ 2 & 2 & 4 & 1 \end{bmatrix} \cdot X^T + \underbrace{\begin{bmatrix} 0 \\ 2 \end{bmatrix}}_{2\times 1}$$

El primer sumando debe ser una matriz de tamaño $2\times 1$

Para que se pueda sumar con la matriz $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$.

Tenemos

$$\underbrace{\underset{2\times 4}{\begin{bmatrix} 3 & 0 & 0 & 1 \\ 2 & 2 & 4 & 1 \end{bmatrix}} \cdot \underset{\times -}{X^T}}_{2\times 1}$$

$\Rightarrow X^T$ es de tamaño $4\times 1$

luego $X \in M_{1\times 4}(K)$

Otras propiedades sobre las matrices son:

- El producto no cumple en general que $AB = BA$ y no todas las matrices distintas de 0 tienen inversa.
- La **matriz traspuesta** de una matriz $A$ de tamaño $m \times n$ es una matriz que denotaremos $A^T$, de 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 $(AB)^T = B^T A^T$ 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 $a \equiv b \pmod{n}$, $a \equiv b\ (n)$ 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 $\{0, 1, 2, \cdots, n-1\}$ con las operaciones definidas *salvo múltiplos de $n$*.

**Proposición 2.** *Para cualquier entero positivo $n$ y cualquier $a$ en $\mathbb{Z}$, existe un elemento $r \in \{0, 1, \cdots, n-1\}$ 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.

$\mathbb{Z}_n$ como sabemos son los restos de dividir entre $n$

La suma $+$ y el producto $\cdot$ en $\mathbb{Z}_n$ se determina como:

$\forall a, b \in \mathbb{Z}_n$ $a+b$ en $\mathbb{Z}_n$ es el resto de dividir el "entero" $a+b$ entre $n$.

y $a \cdot b$ en $\mathbb{Z}_n$ es el resto de dividir el "entero" $a \cdot b$ entre $n$

$\mathbb{Z}_n$ con estas operaciones definidas tiene las mismas propiedad que el conjunto de los enteros $\mathbb{Z}$.
Se cumplen todas las propiedades del concepto de cuerpo excepto la propiedad 8, relativa a la existencia de inverso para cualquier elemento $\neq 0$. No siempre se cumple.

## Operaciones elementales

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

1. *Multiplicar la fila $p$ por la constante $\lambda \in K$ distinta de 0. Esta operación la denotaremos $E_{\lambda(p)}$.*
2. *Suma a la fila $p$, la fila $q$ (distinta de $p$) multiplicada por $\lambda$. Esta operación la denotaremos $E_{(p)+\lambda(q)}$.*
3. *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.*
$$E^{-1}_{\lambda(p)} = E_{\lambda^{-1}(p)} \qquad E^{-1}_{(p)+\lambda(q)} = E_{(p)+(-\lambda)(q)} \qquad E^{-1}_{(p,q)} = E_{(p,q)}.$$

En $\mathbb{Z}_5$

$$\begin{bmatrix} 2 & 3 & 1 \\ 4 & 0 & 2 \\ 1 & 3 & 2 \end{bmatrix} \overset{E_{(2)+3(1)}}{\sim} \begin{bmatrix} 2 & 3 & 1 \\ 10 & 9 & 5 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 0 & 4 & 0 \\ 1 & 3 & 2 \end{bmatrix}$$

**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 $E$.*

Sobre $I_n$ (identidad de tamaño $n\times n$)

$E_{\lambda(p)}$ es la matriz elemental
$$\begin{array}{cc} & \text{columna } p \\ \text{fila } p & \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \lambda & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & \cdots & & 1 \end{bmatrix} \end{array}$$

$$E_{(p)+\lambda(q)} \text{ es la matriz elemental } \begin{array}{c|c} & \begin{array}{ccccc} \phantom{1} & p & & q & \phantom{1} \end{array} \\ \begin{array}{c} \\ p \\ q \\ \\ \end{array} & \begin{bmatrix} 1 & \cdots & & & \\ & 1 & \cdots & \lambda & \\ & & \ddots & \vdots & \\ & & & 1 & \cdots \\ & & & & 1 \end{bmatrix} \end{array}$$

$$E_{(p,q)} \text{ es la matriz elemental } \begin{array}{c|c} & \begin{array}{ccccc} \phantom{1} & p & & q & \phantom{1} \end{array} \\ \begin{array}{c} \\ p \\ \\ q \\ \\ \end{array} & \begin{bmatrix} 1 & \cdots & & & \\ & 0 & \cdots & 1 & \\ & \vdots & \ddots & \vdots & \\ & 1 & \cdots & 0 & \cdots \\ & & & & 1 \end{bmatrix} \end{array}$$

**Proposición 5.** *Hacer una operación elemental por filas es equivalente a multiplicar por la izquierda por la matriz elemental por filas asociada a la operación. Dicho de otra forma:*

$$E(A) = EA$$

*donde la $E$ de la izquierda es una operación elemental por filas y la de la derecha es la matriz elemental por filas que denotamos del mismo modo.*

*Demostración.* Utilizando el teorema y que $IA = A$, tenemos que

$$E(A) = E(IA) = E(I)A = EA.$$

Ejemplo: En $\mathbb{Z}_5$

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

fila tercera
de A multiplicada
por 4

$\downarrow$

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

fila3 + (-1) fila2 de A'

A'

## Reduccion por filas

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

I. Para cada una de las filas $i = 1, 2, \cdots, m$, si no son filas nulas, hacer:

1. 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.
3. 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:

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

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.*

**Ejercicio 31.** *Calcula la matriz reducida por filas completa de la siguiente matriz utilizando el orden estricto explicado en clase y calcula la matriz de paso:*

$$\begin{bmatrix} 0 & 4 & 0 & 4 \\ 1 & 2 & 3 & 2 \\ 0 & 2 & 0 & 2 \end{bmatrix} \in \mathbf{M}_{3,4}(\mathbb{Z}_5)$$

Soluc.

$$\left[\begin{array}{cccc|ccc} 0 & 4 & 0 & 4 & 1 & 0 & 0 \\ 1 & 2 & 3 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 & 0 & 1 \end{array}\right] \overset{E_{4^{-1}(1)} = E_{4(1)}}{\sim} \left[\begin{array}{cccc|ccc} 0 & 1 & 0 & 1 & 4 & 0 & 0 \\ 1 & 2 & 3 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 & 0 & 1 \end{array}\right]$$

$$\underset{E_{(3)-2(1)}}{\overset{E_{(2)-2(1)}}{\sim}} \left[\begin{array}{cccc|ccc} 0 & 1 & 0 & 1 & 4 & 0 & 0 \\ 1 & 0 & 3 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{array}\right]$$

$$\overset{E_{(1,2)}}{\sim} \left[\begin{array}{cccc|ccc} 1 & 0 & 3 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{array}\right]$$

La matriz de paso es

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

Lo comprobamos:

$$\underbrace{\begin{bmatrix} 2 & 1 & 0 \\ 4 & 0 & 0 \\ 2 & 0 & 1 \end{bmatrix}}_{P} \cdot \underbrace{\begin{bmatrix} 0 & 4 & 0 & 4 \\ 1 & 2 & 3 & 2 \\ 0 & 2 & 0 & 2 \end{bmatrix}}_{A} = \underbrace{\begin{bmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{R}$$

# 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. □

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.*

1. *Si la columna de los términos independientes es una columna pivote, entonces el sistema no tiene solución. Diremos que el sistema es* **incompatible**.
2. *Si eso no sucede, haremos parámetros las variables correspondientes a las columnas no pivote y despejaremos 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 :*

$$x_1 + x_2 - x_4 = 4$$

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

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

Soluc.

$$(A|B) = \left[\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 4 \\ -1 & -1 & 1 & 3 & 0 \\ 2 & 2 & -1 & 1 & 4 \end{array}\right]$$

Reducimos por filas

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 4 \\ -1 & -1 & 1 & 3 & 0 \\ 2 & 2 & -1 & 1 & 4 \end{array}\right] \underset{E_{(3)-2(1)}}{\overset{E_{(2)+(1)}}{\sim}} \left[\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 4 \\ 0 & 0 & 1 & 2 & 4 \\ 0 & 0 & -1 & 3 & 1 \end{array}\right]$$

$$\overset{E_{(3)+(2)}}{\sim} \left[\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 4 \\ 0 & 0 & 1 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

El sistema reducido es:

$$\left.\begin{array}{r} x_1 + x_2 - x_4 = 4 \\ x_3 + 2x_4 = 4 \end{array}\right\}$$

Sistema compatible indeterminado. Parámetros $x_2 = \alpha$ y $x_4 = \beta$

(variables cuyas columnas no son pivotes)

Solución:

$$\left.\begin{array}{ll} x_1 = 4 - \alpha + \beta & = 4 + 4\alpha + \beta \\ x_2 = \alpha & = \alpha \\ x_3 = 4 - 2\beta & = 4 + 3\beta \\ x_4 = \beta & = \beta \end{array}\right\} \quad \alpha, \beta \in \mathbb{Z}_5$$