



MasterCrack

[www.wuolah.com/student/MasterCrack](http://www.wuolah.com/student/MasterCrack)

4205

## **Algebra Lineal y Estr. Matemáticas.pdf**

*Apuntes Temario Completo*



**1º Álgebra Lineal y Estructuras Matemáticas**



**Grado en Ingeniería Informática**



**Escuela Técnica Superior de Ingenierías Informática y de  
Telecomunicación  
UGR - Universidad de Granada**

# Álgebra Lineal y Estructuras Matemáticas

Jose Carlos Rosales González

-Facultad de Ciencias, sección matemáticas, Departamento de álgebra, despacho 137

Tutorías:

Lunes, martes y jueves → 9:00 a 11:00

Apuntes en: [www.ugr.es/~pedro/aleu](http://www.ugr.es/~pedro/aleu)

1. Conjuntos, relaciones y aplicaciones
2. Aritmética entera y modular
3. El anillo de los polinomios con coeficiente en un cuerpo
4. Matrices con coeficiente en un cuerpo
5. Espacios vectoriales y aplicaciones lineales
6. Sistemas de ecuaciones lineales
7. Diagonalización de matrices
8. Combinatoria.

La evaluación de las prácticas es de 0 a 2

Sacando un 3º en TEORÍA y teniendo en ~~contado~~ prácticas la máxima nota (2) el alumno está aprobado

LUN  
20  
MAY

Noticias para  
el mundo  
universitario.

nº 37. Semana del 20 al 26

## La Selectividad ha llegado, ¡Sube tus apuntes!

**Wuolah, la plataforma que ha salvado la vida de millones de universitarios también está en selectividad.**

Si tienes apuntes de selectividad esta es tu oportunidad. Cada año muchos estudiantes se enfrentan a las duras Pruebas de Acceso a la Universidad. Hubo un día que tú fuiste uno de ellos, ¿recuerdas? Saca tus apuntes de ese viejo cajón y súbelos a Wuolah. Los futuros universitarios te lo agradecerán. Recuerda que por cada descargas obtendrás tu recompensa, como siempre.

Wuolah, la startup española que ha creado una plataforma dirigida a los estudiantes, ha decidido dar un importante paso llevando la plataforma a los alumnos que quieren acceder a los estudios universitarios: ya se encuentra activa la selectividad de las 17 comunidades autónomas de toda España. Incluyendo, además, las dos ciudades autónomas Ceuta y Melilla.

Wuolah cuenta en España con más de 1,5 millones de usuarios, más de 2 millones de documentos subidos y compartidos por toda la comunidad y más de 15 millones de descargas, siendo la primera web posicionada en el buscador Google por la palabra 'apuntes'.

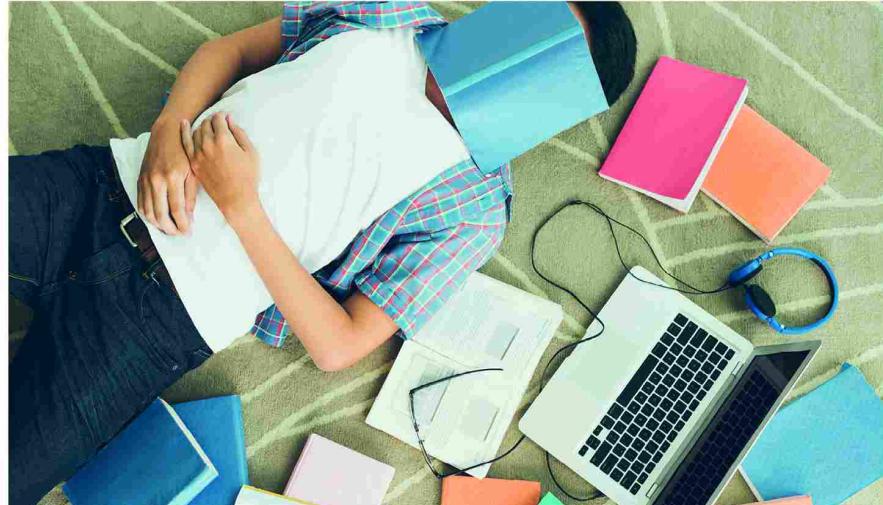
### ¿Quieres saber cómo funciona?

Wuolah está dirigido a 2 tipos de estudiantes. En primer lugar, aquellos estudiantes que asisten a clase y toman notas y elaboran unos buenos apuntes. Para estos Wuolah ofrece la posibilidad de que ganen dinero con sus apuntes o trabajos.

¿Cómo? Para ello, los usuarios deberán registrarse en la web, donde podrán subir sus apuntes organizados por comunidad autónoma, especialidad de Bachillerato (arte, ciencias, ciencias sociales, etc.) y asignaturas comunes.

### Wuolah Giveaway

**Set de tenis.** Mata el gusanillo del Roland Garros con este set de Tenis que incluye dos raquetas y tres pelotas.



Una vez subidos los documentos el usuario podrá ganar dinero en función de las descargas que realicen otros usuarios.

Además, la calidad de estos documentos es avalada por los propios usuarios mediante un sistema de votaciones. Con lo que se va a recompensar el esfuerzo.

En segundo lugar, aquellos estudiantes que dedican menos tiempo a elaborar sus apuntes o toman pocas notas, y piden los apuntes en el último momento también tiene un lugar en Wuolah. Estos son los que tienen la oportunidad de descargar los apuntes de sus compañeros totalmente gratis, únicamente registrándose en la web.

### ¿Qué puede aportar Wuolah a estudiantes de selectividad?

Conseguir unos buenos apuntes no es nada fácil. Con la ayuda de Wuolah los estudiantes podrán complementar sus apuntes de clases con otros colgados en la web. Así podrán unificar todo el contenido y tener un buen material para estudiar de cara a selectividad. Por otra parte, podrás ayudar a muchos otros estudiantes y

compañeros que te necesitan. Si subes tu apuntes a Wuolah aquellos que como tú quieren acceder a la universidad te lo agradecerán. Además, cada vez que alguien descarga tus apuntes puedes obtener una remuneración y, como hemos visto, la descarga es totalmente gratuita.

**Pero esto no es todo, Wuolah aún tiene más que ofrecer.**

Los usuarios contarán con un espacio reservado en el que podrán preguntar y resolver dudas, anunciar la subida de apuntes, etc. Todo esto entre los propios compañeros. Es una forma de fomentar la interacción entre estudiantes.

Por otro lado, Wuolah cuenta con un sorteo semanal o Giveaway, donde se sortean dos productos por semana. Desde videojuegos, patinetes eléctricos, hoverboards, e-reader, funkis e incluso portátiles. Para conseguir estos premios, los estudiantes sólo tienen que subir sus documentos y obtendrán tickets que podrán canjear para participar en los sorteos activos de cada semana. Además, Wuolah ofrece 1 ticket semanal a todos los usuarios.

### Wuolah Giveaway

**Extensor Wi-Fi TP-LINK.** Día Mundial de Internet, no te quedes sin Wi-Fi en tu propia casa, ¡Participa ya!

# Tema 1: Conjuntos, relaciones y aplicaciones.

Un conjunto es una colección de objetos a los que llamaremos elementos del conjunto.

- Cuando  $x$  sea un elemento de un conjunto  $A$ , escribiremos  $x \in A$  y diremos que  $x$  pertenece a  $A$ .
  - Diremos que un conjunto  $A$  es un subconjunto de un conjunto  $B$  y lo denotaremos  $A \subseteq B$  si todo elemento de  $A$  pertenece al conjunto  $B$ .
  - Diremos que dos conjuntos  $A$  y  $B$  son iguales y lo denotaremos  $A = B$  si  $A \subseteq B$  y  $B \subseteq A$ .
  - Admitiremos la existencia de un conjunto que no tiene elementos, a dicho conjunto lo llamaremos "conjunto vacío" y lo denotaremos  $\emptyset$ .
- △ - El vacío es subconjunto de cualquier conjunto.

Ejemplo:

$$A = \{1, 2, 3, 4, 5\} \quad B = \{2, 4, 6\} \quad C = \{1, 3, 5\}$$

$1 \in A$	$B \not\subseteq A$	$\emptyset \not\subseteq A$	$\{\} \neq \{1\}$
$6 \notin A$	$\{1\} \neq \emptyset$	$\emptyset \subseteq A$	
$\emptyset \subseteq A$	$\emptyset \subseteq \emptyset$		

Series de ejercicios

## Operaciones con conjuntos.

Sean  $A$  y  $B$  dos conjuntos.

- 1) La intersección de  $A$  y  $B$  es  $A \cap B = \{x \mid x \in A, x \in B\}$
- 2) La unión de  $A$  y  $B$  es  $A \cup B = \{x \mid x \in A \text{ o } x \in B\}$
- 3) La diferencia de  $A$  y  $B$  es  $A \setminus B = \{x \in A \mid x \notin B\}$
- 4) El conjunto parte del conjunto  $A$  (o conjunto potencia de  $A$ ) es  $P(A) = \{X \mid X \subseteq A\}$
- 5) El producto cartesiano de  $A$  y  $B$  es  $A \times B = \{(a, b) \mid a \in A \text{ y } b \in B\}$   
A los elementos del producto cartesiano se les llama pares de coordenadas
- 6) Si  $A_1, A_2, \dots, A_n$  son conjuntos, entonces el producto cartesiano de todos ellos es  $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$   
A estos elementos se le llama n-tuplas
- 7) Al conjunto  $A \times A \times \dots \times A \rightarrow A^n$

El cardinal de un conjunto es el nº de elementos de dicho conjunto. Denotaremos  $\#A$  al cardinal del conjunto  $A$ .

Proposición:

- 1) El cardinal de parte de  $A$  es  $\#P(A) = 2^{\#A}$
- 2) El cardinal del producto cartesiano es  $\#(A_1 \times A_2 \times A_3 \times \dots \times A_n) = \#A_1 \times \#A_2 \dots \#A_n$

Ejemplo:

$$A = \{1, 2, 3\} \quad B = \{2, 3, 5, 7\}$$

$$A \cup B = \{1, 2, 3, 5, 7\} \quad A \cap B = \{2, 3\} \quad A \setminus B = \{1\} \quad B \setminus A = \{5, 7\}$$

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\} \quad \#P(A) = 2^{\#A} = 8$$

$$\#(A \times B) = \#A \cdot \#B = 12 \quad \#P(\emptyset) = 2^0 = 1 \quad P(\emptyset) \neq \emptyset \quad P(\emptyset) = \{\emptyset\}$$

$$\#P(\emptyset) = \{\emptyset\} \quad \#P(\{\emptyset\}) = 2^1 = 2$$

$$A \times B = \{(1, 2), (1, 3), (1, 5), (1, 7), (2, 1), (2, 3), (2, 5), (2, 7), (3, 1), (3, 2), (3, 5), (3, 7)\}$$

## Relaciones de equivalencia

Sea  $A$  un conjunto. Una relación binaria en  $A$  es un subconjunto  $R$  de  $A \times A$ . Si  $(x, y)$  pertenece a  $R$ ,  $(x, y) \in R$ , escribiremos  $xRy$  y diremos que  $x$  está relacionado con  $y$ .

• Ejemplo:

$$A = \{1, 2, 3, 4, 5\} \quad R = \{(1,1), (2,3), (4,5), (3,2), (5,3)\}$$

$$2R3 \quad 3R4 \quad 4R5 \quad 5R4$$

Una relación binaria  $R$  sobre un conjunto  $A$  será una relación de equivalencia si verifica las siguientes propiedades:

- 1) Reflexiva  $aRa \forall a \in A$
- 2) Simétrica  $aRb \Rightarrow bRa$
- 3) Transitiva si  $aRb$  y  $bRc \Rightarrow aRc$

Si  $R$  es una relación de equivalencia sobre un conjunto  $A$  y  $a \in A$  entonces la "clase" del elemento  $a$  es el conjunto  $[a] = \{x \in A \text{ tq } xRa\}$

Proposición:

- 1)  $aRb$  si y sólo si  $[a] = [b]$  (la clase de  $a$  = la clase de  $b$ )
- 2)  $aRb$  si y sólo si  $[a] \cap [b] \neq \emptyset$

Llamarémos conjuntos cocientes de  $A$  por la relación de equivalencia  $R$  al conjunto:  $\frac{A}{R} = \{[a] \text{ tq } a \in A\}$

Ejemplo:

Sabiendo que  $R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (3,4), (4,3)\}$  y es una relación de eq. Sobre el conjunto  $A = \{1, 2, 3, 4, 5\}$ . Calcular el cardinal del conjunto cociente de  $A$  ( $\frac{A}{R}$ )

$$\frac{A}{R} = \{[a] \text{ tq } a \in A\} = \{[1], [2], [3], [4], [5]\} = * \{ \{1, 2\}, \{3, 4\}, \{5\} \}$$

$$* [1] = \{1, 2\} = [2]$$

$$[3] = \{3, 4\} = [4]$$

$$[5] = \{5\}$$

$$\boxed{\# \frac{A}{R} = 3}$$



## Ejemplos:

① En el conjunto  $A = \{1, -1, 2, 3, -3, 5\}$  definimos la siguiente relación binaria:  $xRy$  si  $x^2 = y^2$

a) Demostrar que  $R$  es una relación de equivalencia

b) Calcular  $\# \frac{A}{R}$

a) Reflexiva: si  $x \in A$  entonces  $x^2 = x^2$  por tanto  $xRx$

Simétrica: si  $xRy$  entonces  $x^2 = y^2$  por tanto  $y^2 = x^2$   
 $\Rightarrow yRx$

Transitiva: si  $xRy$  y  $yRz \Rightarrow x^2 = y^2$  y  $y^2 = z^2 \Rightarrow x^2 = z^2$   
 $\Rightarrow xRz$ .

b)  $\frac{A}{R} = \{[a] \text{ tq } a \in A\} = \{[1], [-1], [2], [3], [-3], [5]\} =$   
 $= \{\{1, -1\}, \{2\}, \{3, -3\}, \{5\}\}$

\*  $[1] = \{1, -1\} = [-1]$

$[2] = \{2\}$

$[3] = \{3, -3\}$

$[5] = \{5\}$

$$\boxed{\# \frac{A}{R} = 4}$$

② Sea  $X = \{1, 2, 3, 4, 5, 6\}$ , en  $X \times X$  definimos la siguiente relación binaria  $(a, b)R(c, d)$  si  $a+b = c+d$

a) Demostrar que  $R$  es una relación de equivalencia

b)  $\# \frac{X \times X}{R}$

a) Reflexiva:  $a+b = a+b \Rightarrow (a, b)R(a, b)$

Simétrica: si  $(a, b)R(c, d) \Rightarrow a+b = c+d \Rightarrow c+d = a+b \Rightarrow (c, d)R(a, b)$

Transitiva: si  $(a, b)R(c, d)$  y  $(c, d)R(e, f) \Rightarrow a+b = c+d$  y  
 $c+d = e+f \Rightarrow a+b = e+f \Rightarrow (a, b)R(e, f)$

b)  $[(3, 4)] = \{(1, 6), (5, 1), (2, 5), (5, 2), (3, 4), (4, 3)\}$

$$\# \frac{X \times X}{R} = 11$$

En una clase están todas las parejas que suman 2, en otra están las que suman 3, ... en otra están las que suman 12.

③ En el conjunto  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$  definimos la siguiente relación binaria  $xRy$  si  $x-y$  es múltiplo de 3

- Reverstir que  $R$  es una relación binaria de equivalencia
- Calcular  $[2]$
- Calcular  $\# \frac{\mathbb{Z}}{R}$

a) Reflexiva:  $a-a=0$  es múltiplo de 3  $\Rightarrow aRa$

Simétrica: si  $aRb \Rightarrow a-b$  es múltiplo de 3  $\Rightarrow b-a$  es mult. 3  
 $\Rightarrow bRa$

Transitiva: Si  $aRb$  y  $bRc \Rightarrow a-b$  es mult. 3 y  $b-c$  es mult. 3  
 $\Rightarrow a-b+b-c$  es mult. 3  $\Rightarrow a-c$  es mult. 3  
 $\Rightarrow aRc$

b)  $[2] = \{x \in \mathbb{Z} \mid q \mid x-2\} = \{x \in \mathbb{Z} \mid q \mid x-2 \text{ es mult. 3}\} = \{2, 5, 8, 11, 14, -1, -4, -7, -10, \dots\} = \{2+3k \mid k \in \mathbb{Z}\}$

c)  $[1] = \{1, 4, 7, 10, 13, \dots\} = \{1+3k \mid k \in \mathbb{Z}\}$

$[0] = \{0, 3, 6, 9, 12, \dots\} = \{3k \mid k \in \mathbb{Z}\}$

$$\# \frac{\mathbb{Z}}{R} = 3$$

Si al dividir un n° da resto  $i$ , es la clase a la que pertenece dicho n°.

Una partición de un conjunto  $X$  es una familia de sus conjuntos de  $X = \{A_i \mid i \in I\}$  verificando la siguiente condición:

- $A_i \neq \emptyset \forall i \in I$
- $A_i \cap A_j = \emptyset$  si  $i \neq j$
- $\bigcup_{i \in I} A_i = X$  (la unión de todo).

Ejemplo:

$\{\{1, 3\}, \{2, 4\}, \{5\}\}$  es una partición del conjunto  $\{(1, 2, 3, 4, 5)\}$

## Proposición:

Si  $R$  es una relación de equivalencia sobre el conjunto  $A$  entonces el conjunto cociente  $\frac{A}{R}$  es una partición de  $A$ .

## Relaciones de orden.

Una relación binaria ( $\leq$ ) sobre un conjunto  $A$  diremos que es una relación de orden si verifica las siguientes propiedades:

- 1) Reflexiva:  $a \leq a \quad \forall a \in A$
- 2) Antisimétrica: si  $a \leq b$  y  $b \leq a$  entonces  $a = b$
- 3) Transitiva: si  $a \leq b$  y  $b \leq c \Rightarrow a \leq c$

## Ejemplos:

- Orden usual de los no naturales ( $\mathbb{N} \subseteq \mathbb{U}$ )

no enteros ( $\mathbb{Z} \subseteq \mathbb{U}$ )

no racionales ( $\mathbb{Q} \subseteq \mathbb{U}$ )

no reales ( $\mathbb{R} \subseteq \mathbb{U}$ )

### Ejemplo:

①  $N = \{0, 1, 2, \dots\}$  definimos la siguiente relación binaria:

$a \leq_m b$  si  $b$  es múltiplo de  $a$ .  $a \leq_m b \rightarrow$  múltiplo

$$2 \leq_m 6 \quad 2 \not\leq_m 3$$

a) Demostrar que es una relación de orden.

- Reflexiva:  $a$  es múltiplo de  $a \Rightarrow a \leq_m a$

- Antisimétrica:  $a \leq_m b$  y  $b \leq_m a \Rightarrow b$  es múlt. de  $a$  y  $a$  es múlt. de  $b$ .  
 $\Rightarrow \exists s, t \in \mathbb{N}$  tq  $b = a \cdot s$  y  $a = b \cdot t \Rightarrow b = b \cdot t \cdot s \Rightarrow t \cdot s = 1 \Rightarrow$

- Transitiva:  
 $\Rightarrow t = s = 1 \Rightarrow b = a$

si  $a \leq_m b$  y  $b \leq_m c \Rightarrow b$  es múltiplo de  $a$  y  $c$  es múltiplo de  $b \Rightarrow$

$\Rightarrow \exists x, y \in \mathbb{N}$  tq  $b = ax$  y  $c = by \Rightarrow c = axy \Rightarrow$

$c$  es múlt. de  $a \Rightarrow a \leq_m c$

② Sea  $X$  un conjunto, en  $P(X)$  definimos la siguiente relación binaria:

$A \leq_i B$  si  $A \subseteq B$  - Demuestra que es una relación de orden.

- Reflexiva:  $A \subseteq A \Rightarrow A \leq_i A$

- Antisimétrica: si  $A \leq_i B$  y  $B \leq_i A \Rightarrow A \subseteq B$  y  $B \subseteq A \Rightarrow A = B$

- Transitiva: si  $A \leq_i B$  y  $B \leq_i C \Rightarrow A \subseteq B$  y  $B \subseteq C \Rightarrow A \subseteq C \Rightarrow A \leq_i C$

## PRACTICAS.

Tutorías → M-Z → 16:00 - 19:00

Facultad de ciencias Despacho 33 (Becarios)

Maria Calvo Sotelo  
mariacc@ugr.es

### Relaciones de equivalencia:

Ej:  $X = \mathbb{Z}$   $x R y \Leftrightarrow x-y$  es múltiplo de 3  
 $\frac{X}{R} \rightarrow$  conjunto cociente.

$$[x] = \{y \in X, x R y\} \quad \frac{X}{R} = \{[x], x \in X\}$$

$$[0] = \{y \in \mathbb{Z}, y - 0 \text{ mlt. } 3\}$$

$$[1] = \{y \in \mathbb{Z}, y - 1 = 3k\}$$

$$[2] = \{y \in \mathbb{Z}, y - 2 = 3k\}$$

$$\frac{\mathbb{Z}}{R} = \{[0], [1], [2]\} = \mathbb{Z}_3$$

Ej:  $X = \mathbb{R}$   $x R y \Leftrightarrow x - y \in \mathbb{Z}$

1) Probar que R es una relación de equivalencia.

- Reflexiva:  $\forall x \in \mathbb{R}, x R x \Leftrightarrow x - x = 0 \in \mathbb{Z}$

- Simétrica:  $\forall x R y \Leftrightarrow x - y \in \mathbb{Z} \Rightarrow y - x = -z \in \mathbb{Z}$

- Transitiva:  $x R y, y R z \Leftrightarrow x R z \Leftrightarrow$

2) ¿Qué es el conjunto cociente?  
 $x - y \in \mathbb{Z}, y - z \in \mathbb{Z} \Rightarrow x - y + y - z = x - z \in \mathbb{Z}$

$$[0] = \{0, 1, 2, \dots\} = \mathbb{Z} = \{0 + k, k \in \mathbb{Z}\}$$

$$[\frac{1}{2}] = \{\frac{1}{2} + 0, \frac{1}{2} + 2, \frac{1}{2} + 3, \frac{1}{2} + 4, \dots\} = \{\frac{1}{2} + k, k \in \mathbb{Z}\}$$

$$[\frac{1}{3}] = \{\frac{1}{3} + 0, \frac{1}{3} + 2, \frac{1}{3} - 2, \dots\} = \{\frac{1}{3} + k, k \in \mathbb{Z}\}$$

$$\frac{X}{R} = \boxed{[0, 1]}$$

$$x \in R$$

$$\pi R 0^{\circ} 14159265$$

$$23 R 0$$

$$\frac{7}{5} R \frac{2}{5}$$

Una relación de orden ( $\leq$ ) sobre un conjunto  $A$ , diremos que es un orden total si dados dos elementos cualesquier  $a, b \in A$  se verifica que  $a \leq b$  ó  $b \leq a$ . Ej:  $(\mathbb{N}, \leq_u)$   $(\mathbb{Z}, \leq_u)$   $(\mathbb{Q}, \leq_u)$   $(\mathbb{R}, \leq_u)$

El orden "si es múltiplo" e "inclusión" NO son totales.

Elementos notables de un conjunto ordenado.

Sea  $(A, \leq)$  un conjunto ordenado y sea  $B$  un subconjunto de  $A$  ( $B \subseteq A$ )

- 1) Un elemento  $b \in B$  diremos que es un elemento maximal de  $B$  si verifica lo siguiente: si  $x \in B$  y  $b \leq x$  entonces  $x = b$ . (No hay nadie más grande)
- 2) Un elemento  $b \in B$  diremos que es el máximo de  $B$  si  $x \leq b, \forall x \in B$
- 3) Un elemento  $b \in B$  diremos que es un elemento minimal de  $B$  si verifica lo siguiente: si  $x \in B$  y  $x \leq b \Rightarrow x = b$
- 4) Un elemento  $b \in B$  diremos que es el mínimo de  $B$  si  $b \leq x, \forall x \in B$
- 5) Un elemento  $a \in A$  es una cota superior de  $B$  si  $x \leq a, \forall x \in B$
- 6) El supremo de  $B$  es el mínimo del conjunto formado por todas las cotas superiores de  $B$  (el supremo es la menor de las cotas superiores)
- 7) Un elemento  $a \in A$  diremos que es una cota inferior de  $B$  si  $a \leq x, \forall x \in B$
- 8) El ínfimo de  $B$  es el máximo del conjunto formado por todas las cotas inferiores de  $B$

Ejemplo:

$$(\mathbb{N}, \leq_u); B = \{1, 2, 3, 4, 5\}$$

- maximales ( $B$ ) = {3, 4, 5}

- máximo ( $B$ ) = 5

- minimales ( $B$ ) = {1}

- mínimo ( $B$ ) = 1

- cotas superiores de  $B$  = {0, 60, 120, 180, ...} = {60k}

- supremo ( $B$ ) = 60

- cotas inferiores de  $B$  = {1}

- ínfimo ( $B$ ) = 1

## Orden producto cartesiano

Sean  $(A_1, \leq_1), (A_2, \leq_2), \dots, (A_n, \leq_n)$  conjuntos ordenados. En el conjunto  $A_1 \times A_2 \times \dots \times A_n$  podemos definir la siguiente relación de orden:

$(a_1, a_2, \dots, a_n) \leq_p (b_1, b_2, \dots, b_n)$  si  $a_1 \leq_1 b_1, a_2 \leq_2 b_2, \dots, a_n \leq_n b_n$

A dicha orden la llamaremos orden producto cartesiano. ( $\leq_p$ )

Ejemplo:

Consideremos  $(\mathbb{Z}, \leq_u)$  y  $(\mathbb{N}, \leq_m)$  como conjuntos ordenados y también  $(\mathbb{Z} \times \mathbb{N}, \leq_p)$ .  $(a_1, b_1) \leq_p (a_2, b_2) \Leftrightarrow a_1 \leq_u a_2 \text{ y } b_1 \leq_m b_2 \Leftrightarrow a_1 \leq_u a_2 \text{ y } b_2 \text{ es mult de } b_1$ .

Calcular los elementos notables del conjunto  $B = \{(2, 3), (3, 6), (-1, 1), (4, 7)\}$

$$(-6, 2) \leq_p (1, 4) \quad (-6, 2) \not\leq_p (1, 11)$$

- máximales ( $B$ ) =  $\{(3, 6), (4, 7)\}$  - cotas sup. de  $B$ :  $(a, b) \in B \Leftrightarrow 4 \leq a \text{ y } b \text{ es mult de } 4$

- máximo ( $B$ ) =  $\emptyset$  - sup. ( $B$ ) =  $(4, 7)$

- mínimales ( $B$ ) =  $\{(-1, 1)\}$  - cotas inf. de  $B$ :  $(a, b) \in B \Leftrightarrow a \leq_u -1 \text{ y } b = 1$

- mínimo ( $B$ ) =  $(-1, 1)$  - inf. ( $B$ ) =

Cuando hablamos del orden producto cartesiano en  ~~$\mathbb{N}^n$~~   $\mathbb{N}^n$  nos referiremos al siguiente orden:  $(a_1, a_2, \dots, a_n) \leq_p (b_1, b_2, \dots, b_n)$  si  $a_1 \leq_u b_1, a_2 \leq_u b_2, \dots, a_n \leq_u b_n$

Este orden NO es total, ya que por ejemplo  $(2, 3) \not\leq_p (1, 4)$  y  $(2, 4) \not\leq_p (2, 3)$

Sin embargo existen órdenes en  $\mathbb{N}^n$  que sí son totales como

por ejemplo el orden lexicográfico que se define de la siguiente forma:

~~una n-tupla~~  $(a_1, a_2, \dots, a_n) \leq_{lex} (b_1, b_2, \dots, b_n)$  si  $\begin{cases} a_i <_u b_i \\ \exists i \in \mathbb{N}, 1 \leq i \leq n \text{ tal que} \\ a_1 = b_1, \dots, a_{i-1} = b_{i-1} \\ a_{i+1} <_u b_{i+1} \end{cases}$

~~una n-tupla~~  $(a_1, a_2, \dots, a_n) \leq_{lex} (b_1, b_2, \dots, b_n)$  si  $\begin{cases} a_i <_u b_i \\ \exists i \in \mathbb{N}, 1 \leq i \leq n \text{ tal que} \\ a_1 = b_1, \dots, a_{i-1} = b_{i-1} \\ a_{i+1} <_u b_{i+1} \end{cases}$

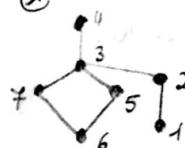
Ejemplo:

Ordena de menor a mayor con el orden lexicográfico los elementos del siguiente conjunto:  $\{(1,1,1), (0,1,1), (0,0,2), (1,0,1), (2,3,1)\}$

$$(0,0,2) \leq_{lex} (0,1,1) \leq_{lex} (1,0,1) \leq_{lex} (1,1,1) \leq_{lex} (2,3,1)$$

Representación gráfica de órdenes

Ejemplo: ①



$$6 \leq 3 \quad 2 \not\leq 7 \quad 6 \not\leq 1$$

$$1 \leq 4 \quad 1 \not\leq 7$$

Calcular los elementos notables de  $B = \{3, 5, 7\}$

$$\text{maximales } (B) = \{3\}$$

$$\text{cotas superiores de } B = \{3, 4\}$$

$$\text{máximo } (B) = \{3\}$$

$$\text{sup } (B) = 3$$

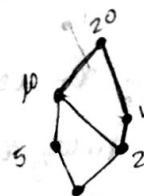
$$\text{minimales } (B) = \{5, 7\}$$

$$\text{cotas inferiores de } B = \{6\}$$

$$\text{mínimo } (B)$$

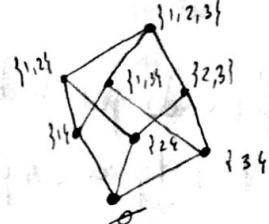
$$\text{lubf } (B) = 6$$

② Representar gráficamente el siguiente orden:  $(\{1, 2, 4, 5, 10, 20\}, \leq_m)$



③ Representar gráficamente  $(P(\{1, 2, 3\}), \leq_i)$

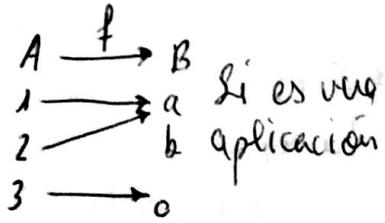
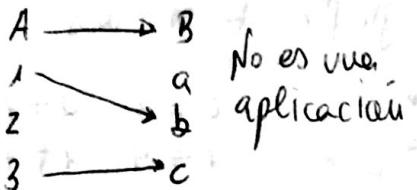
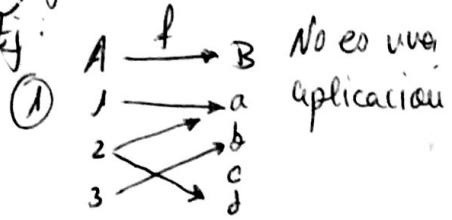
$$P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$



## Aplicaciones entre conjuntos.

Sean  $A$  y  $B$  dos conjuntos. Una aplicación  $f$  de  $A$  en  $B$ , que denotaremos como  $f: A \rightarrow B$ , es una correspondencia que a cada elemento del conjunto  $A$  le asocia un único elemento del conjunto  $B$ .

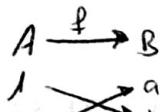
Ej:



② Es la correspondencia  $f: \mathbb{Q} \rightarrow \mathbb{R}$   $f(x) = \frac{x+1}{x-1}$  una aplicación?

- No, porque el  $1$  no tiene asociado ningún  $\mathbb{R}$  real ( $\mathbb{R}$ )

Sea  $f: A \rightarrow B$ , si  $a \in A$  entonces al elemento que le asocia  $f$  en  $B$  lo denotaremos como  $f(a)$  y diremos la imagen de  $a$ .

  
 $f(2) = b$   $\text{Im}(f) = \{a, b\}$

Llamaremos imagen de  $f$  al conjunto formado por todos los imágenes de

$$\text{Im}(f) = \{f(a) \mid a \in A\}$$

Si  $f: A \rightarrow B$  es una aplicación, entonces a los conjuntos  $A$  y  $B$  se les llamará el dominio y el codominio de  $f$  respectivamente. Notese que la imagen de  $f$  es siempre un subconjunto de  $B$ .

Ejemplo:

Dada la aplicación  $f: \mathbb{N} \rightarrow \mathbb{Q}$   $f(n) = 2n+1$ , calcular  $\text{Im}(f)$ .

$$\text{Im}(f) = \{ f(n) \mid n \in \mathbb{N} \} = \{ 2n+1 \mid n \in \mathbb{N} \} = \{ 1, 3, 5, 7, \dots \}$$

Son todos los impares positivos.

- Tipos especiales de aplicaciones:

Una aplicación  $f: A \rightarrow B$  diremos que es:

1) Inyectiva si  $f(x) = f(y)$  implica que  $x = y$

2) Sobreyectiva si  $\text{Im}(f) = B$  (esto es lo mismo que decir que  $B \subseteq \text{Im}(f)$ )

3) Biyectiva si es inyectiva y sobreyectiva

Ejemplo:

① Demuestra que la aplicación  $f: \mathbb{Q} \rightarrow \mathbb{R}$ ,  $f(x) = \frac{2x+1}{3}$  es inyectiva y no es sobreyectiva

$$f(x) = f(y) \Rightarrow \frac{2x+1}{3} = \frac{2y+1}{3} \Rightarrow 2x+1 = 2y+1 \Rightarrow 2x = 2y \Rightarrow x = y$$

$\pi \notin \text{Im}(f)$  ya que  $\pi$  es irracional y todos los elementos que hay en  $\text{Im}(f)$  son racionales.

② Demuestra que la aplicación  $f: \mathbb{Z} \rightarrow \mathbb{N}$ ,  $f(x) = |x|$  NO es inyectiva y sí es sobreyectiva

La aplicación no es inyectiva ya que  $f(1) = f(-1)$

Para demostrar que  $f$  es sobreyectiva debemos probar que el codominio  $\mathbb{N}$  está en la imagen ( $\text{Im}(f)$ )  $\mathbb{N} \subseteq \text{Im}(f)$

$$n \in \mathbb{N} \rightarrow n \in \mathbb{Z} \text{ y } f(n) = |n| = n \Rightarrow n \in \text{Im}(f)$$

$$\text{Im}(f) = \{ f(n) \mid n \in \mathbb{Z} \}$$

③ Demuestra que la aplicación  $f: \mathbb{Q} \rightarrow \mathbb{Q}$ ,  $f(x) = \frac{2x+1}{3}$  es biyectiva.  $\text{Im } f = \{f(x) \mid x \in \mathbb{Q}\}$

$$\text{Inyectiva: } f(x) = f(y) \Rightarrow \frac{2x+1}{3} = \frac{2y+1}{3} \Rightarrow 2x+1 = 2y+1 \Rightarrow 2x = 2y \Rightarrow x = y$$

Para demostrar que es sobreductiva debemos probar que el codominio pertenece a la imagen. ( $\mathbb{Q} \subseteq \text{Im } f$ )

$$q \in \mathbb{Q} \Rightarrow \frac{3q-1}{2} \in \mathbb{Q} \Rightarrow q = f\left(\frac{3q-1}{2}\right) \Rightarrow q \in \text{Im } f.$$

$$\left[ f(\text{?}) = q = \frac{2\text{?}+1}{3} \Rightarrow \text{?} = \frac{3q-1}{2} \right]$$

④ Demostrar que la aplicación  $f: \mathbb{Z} \rightarrow \mathbb{N}$ ,  $f(x) = x^2$  no es ni inyectiva ni sobreductiva.

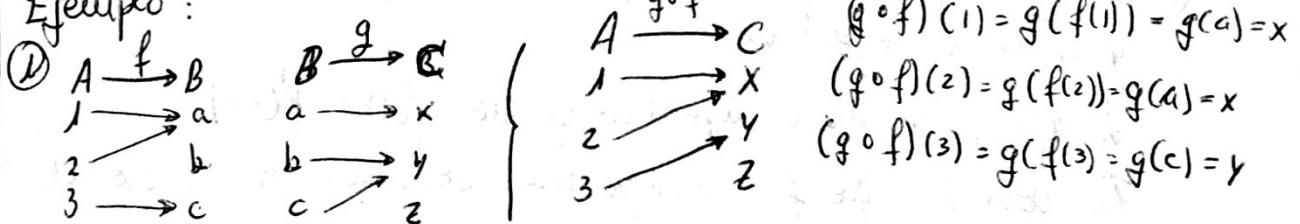
No es inyectiva ya que  $f(1) = f(-1)$

La aplicación no es sobreductiva ya que  $3 \in \text{Im } f$

- Composición de aplicaciones.

Sea  $f: A \rightarrow B$  y  $g: B \rightarrow C$  dos aplicaciones. Llamaremos aplicación composición de  $f$  y  $g$  a la aplicación  $g \circ f: A \rightarrow C$  definida por  $(g \circ f)(a) = g(f(a))$ .

Ejemplo:



② Sea  $f: \mathbb{N} \rightarrow \mathbb{Z}$ ,  $f(n) = n^2$  y  $g: \mathbb{Z} \rightarrow \mathbb{Q}$ ,  $g(x) = x+1$ .

Calcular la composición de  $f$  y  $g$

$$g \circ f: \mathbb{N} \rightarrow \mathbb{Q}$$

$$(g \circ f)(n) = g(f(n)) = g(n^2) = n^2 + 1$$

- NOTA:
- 1) La composición de aplicaciones es asociativa, esto quiere decir que si tenemos 3 aplicaciones  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  y  $h: C \rightarrow D$  entonces  $h \circ (g \circ f) = (h \circ g) \circ f$
  - 2) La composición de aplicaciones NO es commutativa, esto quiere decir que aunque en el caso en que  $g \circ f$  y  $f \circ g$  tengan sentido, en general  $g \circ f \neq f \circ g$ .

$$f: \mathbb{N} \rightarrow \mathbb{N} \quad y \quad g: \mathbb{N} \rightarrow \mathbb{N}$$

$$f(n) = n^2 \quad g(x) = x + 1$$

$$g \circ f : \mathbb{N} \rightarrow \mathbb{N}$$

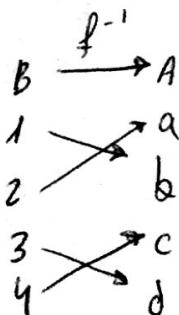
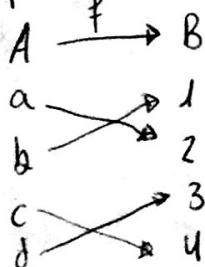
$$\begin{array}{c} g \\ \circ \\ f \end{array}$$

Sea  $A$  un conjunto, llamaremos aplicación identidad en  $A$  a la siguiente aplicación  $1_A: A \rightarrow A$ ,  $1_A(a) = a$ .

Proposición:

Si  $f: A \rightarrow B$  es una aplicación biyectiva, entonces existe una única aplicación  $g: B \rightarrow A$  verificando que  $g \circ f: 1_A$  y  $f \circ g = 1_B$ . A dicha aplicación  $g$  la llamaremos "la inversa de  $f$ ", y la denotaremos  $f^{-1}$ .

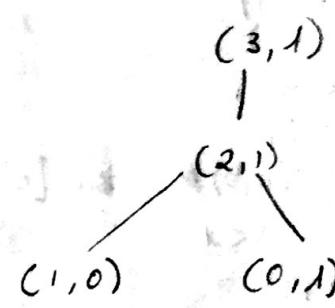
Ejemplo:



PRACTICAS → 6/10/15

- Dado el conjunto ordenado  $(\mathbb{N}^2, \leq_p)$  calcula los elementos notables de  $\{(1,0), (0,1), (2,1), (3,1)\}$ .

- máximos (B) :  $(3,1)$
- mínimos (B) :  $(1,0), (0,1)$
- máximo :  $(3,1)$
- mínimo :  $\emptyset$
- cota superior  $(a,b) \in \mathbb{N}^2 / a \geq 3, b \geq 1$
- cota inferior  $(0,0)$
- supremo  $(3,1)$
- ínfimo.  $(0,0)$



CÁLCULOS:

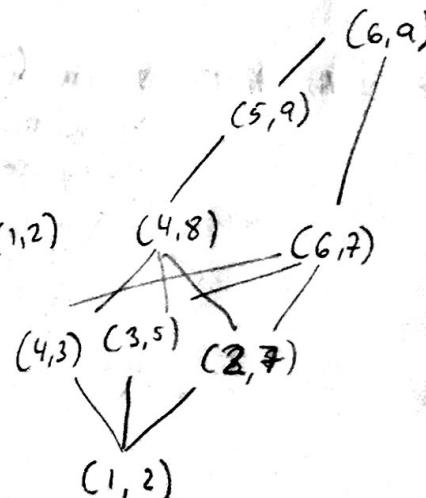
$(1,0)$  y  $(0,1)$  NO están relacionados porque  $1 \not\leq 0 \neq 0 \leq 1$   
 $(1,0)$  y  $(2,1)$  SÍ están relacionados porque  $1 \leq 2$  y  $0 \leq 1$   
El supremo siempre será el máximo.

- Sea  $A = \{(1,2), (4,3), (3,5), (2,7), (4,8), (6,9), (6,3), (5,9)\} \subseteq \mathbb{N}^2$

Calcular los elementos notables con el orden  $\leq_p$

$\leq_p$  lexicográfico.

- máximos: ~~(1,2)~~,  $(6,9)$ , ~~(6,3)~~
- mínimos  $(1,2)$
- máximo  $(6,9)$
- mínimo  $(1,2)$
- c. superior  $(a,b) / a \leq 6, b \leq 9$
- c. inferior  $(0,0), (0,1), (1,0), (1,1), (1,2)$
- supremo  $(6,9)$
- ínfimo  $(1,2)$



El ínfimo es el más grande  
de las cotas inferiores

## lexicográfico

$$(1,2) - (2,7) - (3,5) - (1,3) - (4,8) - (5,9) - (6,7) - (6,9)$$

- maximales  $(6,9)$
- minimales  $(1,2)$
- máximo  $(6,9)$
- mínimo  $(1,2)$
- c. superiores  $(a,b)$  \*  $a \geq 6$  [o'  $a=6$ ,  $b \geq 9$ ]
- c. inferiores  $a < 1$
- supremo  $(6,9)$
- infimo  $(1,2)$

El orden total  $\rightarrow$  maximales = máximo = supremo  
 minimales = mínimo = infimo

- Decir si las siguientes funciones son inyectivas, sobre y estrictas o biyectivas.

a)  $f: \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(n) = n^2$       si inyectiva,  $f(x) = f(y) \rightarrow x^2 = y^2$   
 No sobre yectiva  $\Rightarrow \sqrt{3} \notin \mathbb{N}$   
 NO biyectiva

b)  $f: \mathbb{Q} \rightarrow \mathbb{R}$ ,  $f(x) = 2x$       si inyectiva,  $f(x) = f(y) \Rightarrow 2x = 2y \rightarrow x = y$   
 NO sobre yectiva,  $2\pi \notin \mathbb{Q} \rightarrow x = y$   
 NO biyectiva.  $\nexists x \in \mathbb{Q}$  tq  $2x = \pi$  ( $2x \in \mathbb{R}$ )  
 $\pi \notin \mathbb{Q}$ )

c)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(n) = n+1$       si inyectiva  $f(n) = f(m) \Rightarrow n+1 = m+1 \Rightarrow n = m$   
 si sobre yectiva  $n \in \mathbb{Z} \Rightarrow f(n-1) = n - (+1) = n$   
 si biyectiva.

Ej:

d)  $f: \mathbb{Q} \rightarrow \mathbb{Q}$        $f(x) = \frac{3x+2}{4}$

e)  $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ ,  $f(x) = +\sqrt{x}$

## Tema 2

## "Aritmética entera y modular."

Denotaremos por  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$  al conjunto de los  $\mathbb{N}^0$  enteros.

- Propiedades de la suma:

- 1) Comunitativa:  $a+b = b+a \quad \forall a, b \in \mathbb{Z}$
- 2) Asociativa:  $a+(b+c) = (a+b)+c \quad \forall a, b, c \in \mathbb{Z}$
- 3) Elemento neutro:  $a+0 = a \quad \forall a \in \mathbb{Z}$  (cero es el elem. neutro de la suma)
- 4) Elemento inverso:  $\forall a \in \mathbb{Z} \exists b \in \mathbb{Z} \text{ tq } a+b=0$  (en cuyo caso  $b = -a$ )
- 5) Cancelativa:  $a+b=a+c \Rightarrow b=c$

- Propiedades del producto:

- 1) Comunitativa:  $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$
- 2) Asociativa:  $a(b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{Z}$
- 3) Elemento neutro:  $a \cdot 1 = a \quad \forall a \in \mathbb{Z}$  (1 es el elem. neutro del producto)
- 4) Cancelativa por elemento distinto de cero:  $a \cdot c = b \cdot c \text{ y } c \neq 0 \Rightarrow a = b$
- 5) Distributiva:  $a(b+c) = ab+ac \quad \forall a, b, c \in \mathbb{Z}$

- Propiedad de la división:

- Si  $a, b \in \mathbb{Z}$  y  $b \neq 0 \Rightarrow \exists$  uos únicos  $q, r \in \mathbb{Z}$  tq  $a = qb + r$  y  $0 \leq r < |b|$

A  $q$  y  $r$  los llamaremos el cociente y el resto de dividir  $a : b$  y los denotaremos  $\text{adiv } b$  y  $\text{mod } b$  respectivamente.

Ej: Calcular  $127 \text{ div } 9$  y  $127 \text{ mod } 9$

$$\begin{array}{r} 127 \\ 37 \quad \boxed{14} \\ \quad \quad 1 \end{array}$$

$$\boxed{\begin{array}{l} 127 \text{ div } 9 = 14 \\ 127 \text{ mod } 9 = 1 \end{array}}$$

Ejemplo:

- ① Calcular  $-127 \text{ div } 9$  y  $-127 \text{ mod } 9$

$$\begin{array}{r} 127 \\ 37 \quad 14 \\ \hline 1 \end{array} \Rightarrow 127 = 14 \cdot 9 + 1$$
$$-127 = (-14) \cdot 9 - 1 =$$
$$= (-14) \cdot 9 - 9 + 9 - 1 =$$
$$= (-15) \cdot 9 + 8$$

$$\boxed{\begin{aligned} -127 \text{ div } 9 &= -15 \\ -127 \text{ mod } 9 &= 8 \end{aligned}}$$

- ② Calcular  $-135 \text{ mod } 7$

$$\begin{array}{r} 135 \\ 65 \quad 19 \\ \hline 1 \end{array} \quad 135 = 19 \cdot 7 + 2$$
$$-135 = (-19) \cdot 7 - 2$$
$$-2 + 7 = 5$$

$$\boxed{-135 \text{ mod } 7 = 5}$$

- ③ Calcular  $-63 \text{ mod } 10$

$$\begin{array}{r} 63 \\ 03 \quad 6 \\ \hline \end{array} \quad \boxed{-63 \text{ mod } 10 = 7}$$
$$-3 + 10 = 7$$

Sean  $a, b \in \mathbb{Z}$ , diremos que  $a$  divide a  $b$  ( $a$  divide a  $b$  es un múltiplo de  $a$ ) y lo denotaremos  $a|b$  si  $\exists c \in \mathbb{Z}$  tq  $b = c \cdot a$

Ej:  $2|6$   $2|7$

Un número entero distinto de 1 y -1 diremos que es primo si los únicos  $n^o$  enteros que lo dividen son 1, -1, él y -él.

$n^o$  primos: 2, -2, 3, -3, 5, -5, 7, -7, 11, -11, ...

Dos  $n^o$  enteros diremos que son primos relativos si los únicos enteros que dividen a dichos números son el 1 y el -1.

Ej: 6, 10 No      8, 25 Sí

## Teorema de Bezout.

Sea  $a, b \in \mathbb{Z} \Rightarrow a$  y  $b$  son primos relativos si y solamente si  $\exists u, v \in \mathbb{Z}$  tq  $au + bv = 1$

Ejemplo:  $8 y 25 \Rightarrow 8u + 25v = 1 \quad \begin{cases} u = -3 \\ v = 1 \end{cases}$   
 $196 y 121 \Rightarrow 196u + 121v = 1$  (difícil).

## Teorema fundamental de la Aritmética.

Todo nro entero  $\geq 2$  se puede poner de forma única (salvo reordenaciones) como producto de nros primos positivos

Ejercicio: Calcular la descomposición en primos de 360

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \end{array} \Rightarrow 360 = 2^3 \cdot 3^2 \cdot 5^1$$

Corolario. (consecuencia del Th fundamental)

Si  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  es la descomposición en primos de un entero positivo  $n$ , entonces  $(\alpha_1+1) \cdot (\alpha_2+1) \cdots (\alpha_r+1)$  es el nro de divisores positivos que tiene el nro  $n$ .

Ejemplo: ¿Cuántos divisores tiene el nro 360?

$$360 = 2^3 \cdot 3^2 \cdot 5^1$$
$$(3+1) \cdot (2+1) \cdot (1+1) = 4 \cdot 3 \cdot 2 = 24 \text{ divisores positivos.}$$

Por tanto el nro 360 tiene 48 divisores ( $24^+$  y  $24^-$ )

Sean  $a, b \in \mathbb{Z}$  tales que  $a \neq 0$  ó  $b \neq 0$ , un entero  $d$ . diremos que es un máximo común divisor de  $a$  y  $b$  si verifica:

1)  $d | a$  y  $d | b$

2) si  $c | a$  y  $c | b$  entonces  $c | d$

NOTA: Si  $d$  es un máximo común divisor de  $a$  y  $b$  entonces  $-d$  es también un máximo común divisor de  $a$  y  $b$ . Denotaremos  $\text{m.c.d}\{a, b\}$  al máximo común divisor de  $a$  y  $b$  positivo.

Ej:  $2, -2$  son los m.c.d de  $6$  y  $10$ .  $\Rightarrow \text{m.c.d}\{6, 10\} = 2$

Sean  $a, b \in \mathbb{Z}$ , un entero  $m$  diremos que es un mínimo común múltiplo de  $a$  y  $b$  si verifica lo siguiente:

1)  $a | m$  y  $b | m$

2) si  $a | c$  y  $b | c \Rightarrow m | c$

NOTA: Si  $m$  es un mínimo común múltiplo de  $a$  y  $b$ , entonces  $-m$  es también un mínimo común múltiplo de  $a$  y  $b$ . Denotaremos  $\text{m.c.m}\{a, b\}$  al mínimo común múltiplo positivo.

Ej:  $6, 10 \rightarrow \text{m.c.m.}$

$30, -30$  son los m.c.m. de  $6$  y  $10 \Rightarrow \text{m.c.m}\{6, 10\} = 30$

### \* 1er Método para calcular el "m.c.d" y el "m.c.m"

Sean  $a, b$  enteros positivos  $\geq 2$  y  $a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r}$  y  $b =$

$B = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdots P_r^{\beta_r}$  su descomposición en factores primos.

Entonces:

$$1) \text{m.c.d}\{a, b\} = P_1^{\min\{\alpha_1, \beta_1\}} \cdot P_2^{\min\{\alpha_2, \beta_2\}} \cdots P_r^{\min\{\alpha_r, \beta_r\}}$$

$$2) \text{m.c.m}\{a, b\} = P_1^{\max\{\alpha_1, \beta_1\}} \cdot P_2^{\max\{\alpha_2, \beta_2\}} \cdots$$

NOTA:

- 1) m.c.d {a, 1} = 1
- 2) m.c.d {-7, 9}  $\Rightarrow$  m.c.d {a, b} = m.c.d {|a|, |b|}
- 3) m.c.m {a, 1} = a
- 4) m.c.m {a, 0} = ~~0~~ 0
- 5) m.c.d {a, 0} = a
- 6) m.c.d {0, 0} =  $\emptyset$

Ejemplo: Calcular el m.c.d {360, 210}; m.c.m {360, 210}

$$360 = 2^3 \cdot 3^2 \cdot 5^1$$

$$360 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^0$$

$$\begin{array}{r} \cancel{360}^2 \\ \cancel{210}^2 \\ \hline \cancel{60}^2 \\ \cancel{30}^2 \\ \cancel{15}^3 \\ \cancel{5}^1 \\ \hline 1 \end{array}$$

$$210 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1$$

$$\text{m.c.d } \{360, 210\} = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 30$$

$$\text{m.c.m } \{360, 210\} = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 2.520$$

Proposición:

$$\text{Si } a, b \in \mathbb{Z}^+ \Rightarrow \text{m.c.d } \{a, b\} \cdot \text{m.c.m } \{a, b\} = a \cdot b$$

$$\Rightarrow \text{sabiendo por ej: m.c.d } \{a, b\} \rightarrow \text{m.c.m } \{a, b\} = \frac{a \cdot b}{\text{m.c.d}}$$

2º Método: Algoritmo de Euclides

Entrada: a, b enteros positivos

Salida: m.c.d {a, b}

$$(a_0, a_1) = (a, b)$$

$$\text{Mientras } a_i \neq 0 \rightarrow (a_0, a_1) = (a_1, a_0 \text{ mod } a_1)$$

Devuelve  $a_0$

Ej: Utilizando el Alg. de Euclides, calcular m.c.d {360, 210}

$$(a_0, a_1) = (360, 210) = (210, 150) = (150, 60) = (60, 30)$$

$$= (30, 0) \quad \text{m.c.d } \{360, 210\} = 30$$

Ejemplo: Calcular utilizando el Algoritmo de Euclides  
u.c.d {237, 99}

$$\begin{aligned} (a_0, a_1) &= \cancel{(237, 99)} = (99, 39) = (39, 21) = (21, 18) \\ &= (18, 3) = (3, 0) \quad \text{u.c.d } \{237, 99\} = 3 \end{aligned}$$

~~Resumen:~~

- Ecuaciones diofánticas lineales:

Una ecuación diofántica lineal es una expresión de la forma

$$a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_nx_n = b, \quad \text{donde } a_1, a_2, \dots, a_n \in \mathbb{Z}$$

y  $x_1, x_2, \dots, x_n$  son incógnitas  $\in \mathbb{Z}^n$

Una solución de dicha ecuación es una  $n$ -tuple  $(c_1, c_2, c_3, \dots, c_n)$  tq ~~a~~  $a_1c_1 + a_2c_2 + \dots + a_nc_n = b$ .

- Teorema de Bezout Generalizado:

Sean  $a_1, a_2, \dots, a_n$  y  $b \in \mathbb{Z}$  y  $d = \text{u.c.d } \{a_1, a_2, \dots, a_n\}$   
entonces la ecuación diofántica  $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$   
tiene solución si y solo si  $d | b$ , además en  
dicho caso la ecuación tiene las mismas soluciones que  
la ecuación  $\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + \dots + \frac{a_n}{d}x_n = \frac{b}{d}$

Ejemplo:

- ① La ecuación diofántica  $6x - 8y + 10z = 7$  no tiene solución  
ya que  $\text{u.c.d } \{6, -8, 10\} = 2$  y  $2 \nmid 7$
- ② La ec. diofántica  $6x - 8y + 10z = 14$  tiene solución  
ya que  $\text{u.c.d } \{6, -8, 10\} = 2$  y  $2 | 14$ , además  
tiene las mismas soluciones que la ecuación  $3x - 4y + 5z = 7$

## Resolución de ecuaciones diofánticas con dos incógnitas:

Sean  $a, b, c \in \mathbb{Z}$  tq  $\text{m.c.d}\{a, b\} = 1$ . Si  $(x_0, y_0)$  es una solución de la ecuación  $ax + by = c$  entonces el conjunto formado por todas las soluciones de la ecuación es  $\{(x_0 + bk, y_0 - ak) \mid k \in \mathbb{Z}\}$

Ej: Resolver la ecuación  $6x - 8y = 4$

$$\text{m.c.d}\{6, -8\} = 2 \quad | : 2 \Rightarrow 3x - 4y = 2 \quad (\text{tiene las mismas sols})$$

$$3x - 4y = 2 \rightarrow \text{m.c.d}\{3, -4\} = 1$$

$$\begin{cases} x=2 \\ y=1 \end{cases} \text{ es una solución} \Rightarrow \boxed{\{(2 + -4k, 1 - 3k) \mid k \in \mathbb{Z}\}}$$

## Algoritmo extendido de Euclides

Entrada:  $a$  y  $b$  enteros  $\geq 2$

Salida:  $s, t, d \in \mathbb{Z}$  tq  $d = \text{m.c.d}\{a, b\}$  y  $as + bt = d$

$$(a_0, a_1) = (a, b)$$

$$(s_0, s_1) = (1, 0)$$

$$(t_0, t_1) = (0, 1)$$

Mientras  $a_i \neq 0$

$$q = a_0 \text{ div } a_1$$

$$(a_0, a_1) = (a_1, a_0 - q \cdot a_1)$$

$$(s_0, s_1) = (s_1, s_0 - s_1 \cdot q)$$

$$(t_0, t_1) = (t_1, t_0 - t_1 \cdot q)$$

Devuelve  $d = a_0$ ,  $s = s_0$ ,  $t = t_0$

Ejemplo:

Aplicar el Algoritmo extendido de Euclides a los n°  $a = 120$  y  $b = 93$

$$(a_0, a_1) = (120, 93) = (93, 27) = (27, 12) = (12, 3) = (3, 0)$$

$$(s_0, s_1) = (1, 0) = (0, 1) = (1, -3) = (-3, 7) = (7, -)$$

$$(t_0, t_1) = (0, 1) = (1, -1) = (-1, 4) = (4, -9) = (-9, -)$$

$$[q=1] \rightarrow$$

$$[q=3] \rightarrow$$

$$[q=2] \rightarrow$$

$$[q=4]$$

$$\text{m.c.d}\{120, 93\} = 3 \quad // \quad 120 \cdot 7 + 93(-9) = 3$$

Ejemplo: Calcular todas las soluciones de la ec. diofántica:

$$120x - 93y = 6$$

$$1) \text{ m.c.d } \{120, 93\} = 3$$

2) Pues 3|6, la ec. tiene solución, además tiene las mismas soluciones que la ecuación:  $40x - 31y = 2$

$$3) \text{ m.c.d } \{40, 31\} = 1$$

4) Aplicamos el alg. Euclides a 40 y 31:

$$(a_0, a_1) = (40, 31) \stackrel{q=1}{=} (31, 9) \stackrel{q=3}{=} (9, 4) \stackrel{q=2}{=} (4, 1) \stackrel{q=4}{=} (1, 0)$$

$$(s_0, s_1) = (1, 0) = (0, 1) = (1, -3) = (-3, 7) = (7, -1)$$

$$(t_0, t_1) = (0, 1) = (1, -1) = (-1, 4) = (4, -9) = (-9, -1)$$

$$40 \cdot 1 + 31(-9) = 1 \quad x_0 = 14 \quad \text{es una solución.}$$

$$(2x) \rightarrow 40 \cdot 14 + 31(-18) = 2 \quad y_0 = 18$$

$$(-) \rightarrow 40 \cdot 14 - 31(18) = 2$$

El conjunto de todas las soluciones de la ecuación es:

Solución:  $\{(14 - 31k, 18 - 40k) \mid k \in \mathbb{Z}\}$

a) Cuántas soluciones tiene la solución anterior  
verificando que  $x, y \in [-100, 200]$

$$-100 \leq 14 - 31k \leq 200$$

$$-100 \leq 18 - 40k \leq 200$$

↓

$$-200 \leq -14 + 31k \leq 100$$

$$-200 \leq -18 + 40k \leq 100$$

Cambiamos de signo y por lo tanto

las igualdades.

$$-186 \leq 31k \leq 114$$

$$-182 \leq 40k \leq 118$$

$$-6 \leq k \leq 3 \frac{6}{7}$$

$$-4,55 \leq k \leq 2,95$$

$$\rightarrow -4 \leq k \leq 2$$

$$K \in \{-4, -3, -2, -1, 0, 1, 2\}$$

NOTA:  $2 - (-4) + 1 = 7$

FORMA DE CALCULAR

CUANTAS SOL.

[7 soluciones]

PREGUNTA  
TÍRICA DE  
EXAMEN

## • Ecuaciones en congruencia de grado 1.

Sean  $a, b, m \in \mathbb{Z}$ , escribiremos  $a \equiv b \pmod{m}$  y se lee "a congruente b modulo m" si  $m \mid a - b$  (si  $a - b$  es múltiplo de  $m$ ).

Ej:  $8 \equiv 2 \pmod{3}$   
 $8 \not\equiv 4 \pmod{3}$

Una ecuación en congruencia de grado 1 es una expresión de la forma  $ax \equiv b \pmod{m}$  donde  $a, b$  y  $m \in \mathbb{Z}^*$  y  $x$  es una incógnita. Una solución de la ecuación es un  $c \in \mathbb{Z}$  tq  $a \cdot c \equiv b \pmod{m}$ .

Ejemplo: Resolver la ecuación:

•  $3x \equiv 2 \pmod{5}$

$x = 4, \quad 9, -1, 14 \Rightarrow \{4 + 5k \text{ tq } k \in \mathbb{Z}\}$

•  $2x \equiv 1 \pmod{4}$

$\nexists x \Rightarrow$  No tiene solución.

\* Teorema:

- 1) La ecuación  $ax \equiv b \pmod{m}$  tiene solución si y solo cuando si el m.c.d  $\{a, m\} \mid b$
- 2) Si  $d = \text{m.c.d} \{a, m\}$  y  $d \mid b \Rightarrow$  las ecuaciones  $ax \equiv b \pmod{m}$  y  $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$  tienen las mismas soluciones.
- 3) Si  $\text{m.c.d} \{a, m\} = 1$  y  $u$  es una solución de  $ax \equiv b \pmod{m}$  entonces el conjunto de todas sus soluciones es  $\{u + km \text{ tq } k \in \mathbb{Z}\}$
- 4) La ecuación  $ax + c \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $ax \equiv b - c \pmod{m}$
- 5) La ecuación  $ax \equiv b \pmod{m}$  tiene las mismas soluciones que la ecuación  $(a \pmod{m})x \equiv b \pmod{m}$
- 6) Si  $au + mv = 1$  con  $u, v \in \mathbb{Z} \Rightarrow bu \pmod{m}$  es una solución de la ecuación  $ax \equiv b \pmod{m}$

PRACTICAS 13/10/15

$$\boxed{\text{Nota: } \sqrt{x^2} = |x|}$$

$$\begin{aligned} N &= \{1, 2, \dots\} \\ Z &= \{-1, 0, 1, \dots\} \\ Q &= \{ \dots \} \\ R &= \{ \dots \} \end{aligned}$$

Relación ejercicios.

12. Calcula  $g \circ f$  y  $f \circ g$  cuando sea posible

$$1. \quad f: \mathbb{N} \rightarrow \mathbb{N} \\ n \mapsto n+1$$

$$g: \mathbb{N} \rightarrow \mathbb{N} \\ n \mapsto n^2$$

$$2. \quad f: \mathbb{Q} \rightarrow \mathbb{Q} \\ x \mapsto \frac{3x+2}{4}$$

$$g: \mathbb{Q} \rightarrow \mathbb{Q} \\ x \mapsto x^2$$

$$3. \quad f: \mathbb{R}^+ \cup \{0\} \rightarrow \mathbb{R} \\ x \mapsto +\sqrt{x}$$

$$g: \mathbb{R} \rightarrow \mathbb{R}^+ \cup \{0\} \\ x \mapsto x^2$$

$$1. \quad (g \circ f)(a) = g(f(a))$$

$$f(a) = a+1 \quad , \quad g(f(a)) = g(a+1) = \underline{g(a+1)^2}$$

$$(g \circ f)(n) = g(n+1) = (n+1)^2 \neq n^2 + 2n + 1$$

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1$$

$$2) \quad f(g \circ f)(x) = g\left(\frac{3x+2}{4}\right) = \left(\frac{3x+2}{4}\right)^2$$

$$(f \circ g)(x) = f(x^2) = \frac{3x^2+2}{4}$$

$$3) \quad (g \circ f)(x) = g(+\sqrt{x}) = (+\sqrt{x})^2 = x$$

$$(f \circ g)(x) = f(x^2) = +\sqrt{x^2} = |x|$$

15. Sea  $X = \mathbb{R} \setminus \{-1, 1\}$ , y  $f_1, f_2, f_3, f_4, f_5, f_6: X \rightarrow X$  las aplicaciones

$$f_1(x) = x, \quad f_2(x) = 1-x, \quad f_3(x) = \frac{1}{1-x}, \quad f_4(x) = \frac{1}{x},$$

$$f_5(x) = \frac{x}{x-1}, \quad f_6(x) = \frac{x-1}{x}$$

1. Comprueba que la composición de cualesquiera de estas aplic. sea es una de las seis

$$f_1 \circ f_2, f_3, \dots; f_2 \circ f_3; f_3 \circ f_6; f_2 \circ f_2; f_4 \circ f_4; f_5 \circ f_5; f_1 \circ f_1$$

$$f_1 \circ f_2 = f_2(f_1(x)) = 1-x \quad (f_2) \quad f_1 \circ f_4 = \frac{1}{x} \quad f_1 \circ f_6 = \frac{x-1}{x}$$

$$f_1 \circ f_3 = \frac{1}{1-x} \quad f_1 \circ f_5 = \frac{x}{x-1}$$

$$f_2 \circ f_3 = 1 - \frac{1}{x-1} = \frac{x-2}{x-1} \quad f_3 \circ f_6 = \frac{1}{1 - \frac{x-1}{x}} = x$$

$$f_2 \circ f_2 = 1 - (1-x) = 1 - 1 + x = x \quad (f_2)$$

$$f_4 \circ f_4 = \frac{1}{\frac{1}{x}} = x \quad (f_4)$$

$$f_5 \circ f_5 = \frac{\frac{x}{x-1}}{\frac{x}{x-1}-1} = x$$

$$f_1 \circ f_1 = x \quad (f_1)$$

2. Comprueba que cada una de estas aplic. es biyectiva.

Para  $f_2: x \rightarrow x$  y  $g: x \rightarrow x$   $f \circ g(x) = x$  y  $g \circ f(x) = x$

Todas las aplicaciones son biyectivas porque tienen inversa.  $\exists g \text{ tq } f \circ g = x; g \circ f = x$

$$f_1 \rightarrow f_1 \quad f_4 \rightarrow f_4$$

$$f_2 \rightarrow f_2 \quad f_5 \rightarrow f_5$$

$$f_3 \rightarrow f_6 \quad f_6 \rightarrow f_3$$

25. En  $D(90)$  definimos la relación  $xRy$  si  $\text{m.c.d}\{x, 18\} = \text{m.c.d}\{y, 18\}$

$$D(90) = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$$

1. Comprob. que  $R$  es una rel. de equivalencia.

2. Calcula  $[1], [3], [5], [20]$

3. Determinar conj. cociente.

~~→  $\frac{\text{Expresión}}{xRy}$~~

$$2) [1] = \{1, 5\}$$

$$\text{m.c.d } \{1, 18\} = 1 = \text{m.c.d } \{5, 18\}$$

$$[3] = \{3, 15\}$$

$$\text{m.c.d } \{3, 18\} = 3 = \text{m.c.d } \{15, 18\}$$

$$[5] = [1]$$

~~expresión~~

$$[6] = \{6, 30\}$$

$$3) \frac{D(90)}{R} = D(18)$$

Ejemplo:

- ① Resolver la ecuación  $20x \equiv 10 \pmod{50}$

m.c.d {20, 50} = 10, como  $10 | 10$ , la congruencia tiene soluciones, además tiene las mismas soluciones que la ecuación  $2x \equiv 1 \pmod{5}$

Como m.c.d {2, 5} = 1, entonces sabemos por el Teorema anterior, que si conozco una solución, las conozco todas. Como  $x = 3$  es una solución de la ecuación, entonces el conjunto de todas sus soluciones es  $\{3 + 5k \mid k \in \mathbb{Z}\}$

- ② Resolver la ecuación  $292x \equiv 4 \pmod{392}$

$$\text{m.c.d } \{292, 392\} = 2$$

Como 2 | 4, la ecuación tiene solución, además tiene las mismas soluciones que la ecuación  $121x \equiv 2 \pmod{196} \rightarrow \text{m.c.d } \{121, 196\} = 1$

Caso Si  $a \cdot u + m \cdot v = 1 \Rightarrow b \cdot u \pmod{m}$  es solución  $ax \equiv b \pmod{m}$

$$121u + 196v = 1$$

Aplicamos el algoritmo extendido de Euclides a 196 y 121:

$$\begin{aligned} (a_0, a_1) &= (196, 121) \stackrel{q=1}{=} (121, 75) \stackrel{q=1}{=} (75, 46) \stackrel{q=1}{=} (46, 29) \stackrel{q=1}{=} (29, 17) \stackrel{q=1}{=} (17, 12) \stackrel{q=1}{=} (12, 5) \\ (s_0, s_1) &= (1, 0) = (0, 1) = (1, -1) = (-1, 2) = (2, -3) = (-3, 5) = (5, -8) = \\ (t_0, t_1) &= (0, 1) = (1, -1) = (-1, 2) = (2, -3) = (-3, 5) = (5, -8) = (-8, 13) = \\ &\quad \vdots \\ &= (5, 2) = (2, 1) = (1, 0) \\ &= (-8, 21) = (21, -50) = (-50, -) \quad \left\{ \begin{array}{l} 196 \cdot (-50) + 121 \cdot (81) = 1 \\ 196 \cdot (-50) + 121 \cdot (81) = 1 \end{array} \right. \\ &= (13, -34) = (-34, 81) = (81, -) \end{aligned}$$

Por tanto, aplicando el Teorema anterior, sabemos que  $b \cdot u \pmod{m}$  es una solución  $\Rightarrow 2 \cdot 81 \pmod{196} = 162 \pmod{196} = 162$  es una solución de la ecuación, por tanto el conjunto de todas sus soluciones es  $\{162 + 196k \mid k \in \mathbb{Z}\}$

## • Sistemas de ecuaciones en congruencia

Resolver el sistema:

$$\begin{cases} 4x \equiv 6 \pmod{10} \rightarrow \text{tiene solución} \rightarrow 2x \equiv 3 \pmod{5} \\ 3x \equiv 1 \pmod{4} \rightarrow \text{tiene solución} \rightarrow 3x \equiv 1 \pmod{4} \end{cases} \quad x = 4 + 5k$$

$$2x \equiv 3 \pmod{5} \rightarrow x = 4 + 5k$$

$$3x \equiv 1 \pmod{4} \rightarrow 3(4+5k) \equiv 1 \pmod{4}$$

$$12 + 15k \equiv 1 \pmod{4}$$

$$15k \equiv -11 \pmod{4}$$

$$15k \equiv 3 \pmod{4} \rightarrow 3k \equiv 1 \pmod{4} \rightarrow k = 3 + 4\bar{k}$$

$$x = 4 + 5k = 4 + 5(3 + 4\bar{k}) = 19 + 20\bar{k}$$

$$\{ 19 + 20\bar{k} \text{ tq } \bar{k} \in \mathbb{Z} \}$$

Resolver el sistema:

$$2x \equiv 2 \pmod{4} \rightarrow \text{tiene solución} \rightarrow x \equiv 1 \pmod{2}$$

$$6x \equiv 3 \pmod{9} \rightarrow \text{tiene solución} \rightarrow 2x \equiv 1 \pmod{3}$$

$$2x \equiv 3 \pmod{5} \rightarrow \text{tiene solución} \rightarrow 2x \equiv 3 \pmod{5}$$

$$x \equiv 1 \pmod{2}$$

$$2x \equiv 1 \pmod{3}$$

$$2x \equiv 3 \pmod{5}$$

$$x = 1 + 2k$$

$$2(1 + 2k) \equiv 1 \pmod{3} \Rightarrow 4k \equiv -1 \pmod{3}$$

$$k \equiv 2 \pmod{3} \rightarrow k = 2 + 3\bar{k}$$

$$x = 1 + 2(2 + 3\bar{k}) = 5 + 6\bar{k}$$

$$2(5 + 6\bar{k}) \equiv 3 \pmod{5}$$

$$10 + 12\bar{k} \equiv 3 \pmod{5}$$

$$12\bar{k} \equiv -7 \pmod{5}$$

$$2\bar{k} \equiv 3 \pmod{5} \rightarrow \bar{k} = 4 + 5\bar{k}$$

$$x = 5 + 6\bar{k} = 5 + 6(4 + 5\bar{k}) = 29 + 30\bar{k}$$

$$\{ 29 + 30\bar{k} \text{ tq } \bar{k} \in \mathbb{Z} \}$$

Resolver el sistema:

$$\begin{cases} 2x \equiv 2 \pmod{4} \\ 3x \equiv 6 \pmod{12} \end{cases} \left\{ \begin{array}{l} \rightarrow \text{tiene solución} \rightarrow x \equiv 1 \pmod{2} \\ \rightarrow \text{tiene solución} \rightarrow x \equiv 2 \pmod{4} \end{array} \right\}$$

$$x \equiv 1 \pmod{2} \Rightarrow x = 1 + 2k$$

$$x \equiv 2 \pmod{4} \rightarrow 1 + 2k \equiv 2 \pmod{4}$$

$$2k \equiv 1 \pmod{4} \rightarrow \text{no tiene solución.}$$

Como no tiene solución, el sistema no tiene solución.

- ¿Cuántos nº naturales hay menores de 1000, que acaben en 7 y que al dividirlo por 55 dejen resto 12?  $\rightarrow x = 7 + 55k + 12$

$$x \equiv 7 \pmod{10} \rightarrow x = 7 + 10k$$

$$x \equiv 12 \pmod{55} \rightarrow 7 + 10k \equiv 12 \pmod{55} \quad \text{mcd}\{10, 55\} = 5$$

$$10k \equiv 5 \pmod{55} \quad \text{resta 5}$$

$$2k \equiv 1 \pmod{11} \rightarrow k = 6 + 11\bar{k}$$

$$x = 7 + 10k = 7 + 10(6 + 11\bar{k}) = 67 + 110\bar{k}$$

$$\left\{ 67 + 110\bar{k} \text{ tq } \bar{k} \in \mathbb{Z}_4 \right.$$

$$\cancel{0 \leq 67 + 110\bar{k} < 1000}$$

$$-67 \leq 110\bar{k} < 933$$

$$\frac{-67}{110} \leq \bar{k} < \frac{933}{110}$$

$$-0'61 \leq \bar{k} < 8'48 \rightarrow$$

$$\boxed{0 \leq \bar{k} \leq 8}$$

Solución  
↓  
Son 9 nº naturales  
(del 0 al 8)

¿Cuántos nº enteros del intervalo  $[1000, 2000]$  son pares, al dividirlo entre 7 dan de resto 1 y al multiplicarlos por tres y dividirlos entre 5 dan de resto 2?

$$\begin{array}{l} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{7} \\ 3x \equiv 2 \pmod{5} \end{array} \left. \begin{array}{l} \rightarrow \text{tiene solución} \\ \rightarrow \text{tiene solución} \\ \rightarrow \text{tiene solución} \end{array} \right\} x = 0 + 2k$$

$$2k \equiv 1 \pmod{7} \rightarrow k = 4 + 7\bar{k}$$

$$x = 2k = 2(4 + 7\bar{k}) = 8 + 14\bar{k}$$

$$3(8 + 14\bar{k}) \equiv 2 \pmod{5}$$

$$24 + 42\bar{k} \equiv 2 \pmod{5}$$

$$42\bar{k} \equiv -22 \pmod{5} \rightarrow \cancel{42} \in \mathbb{N} \cancel{\bar{k}}$$

$$2\bar{k} \equiv 3 \pmod{5} \rightarrow \bar{k} = 4 + 5\bar{k}$$

$$x = 8 + 14\bar{k} = 8 + 14(4 + 5\bar{k}) = 64 + 70\bar{k}$$

$$1000 \leq 64 + 70\bar{k} \leq 2000$$

$$936 \leq 70\bar{k} \leq 1936$$

$$\frac{936}{70} \leq \bar{k} \leq \frac{1936}{70}$$

$$13.4 \leq \bar{k} \leq 27.1 \rightarrow 14 \leq \bar{k} \leq 27$$

$$\bar{k} \in \{14, 15, \dots, 27\}$$

Solución: hay 14 nº enteros

Un cocinero de un barco pirata relató cómo había conseguido las 18 monedas de oro que llevaba. 15 piratas atracaron un barco, consiguieron un cofre de monedas, las repartieron en partes iguales y les dieron las 5 que sobraban.

$$x = 15 \text{ q} + 5 \\ x - 5 = 12 \text{ q}$$

Tras una tormenta, murieron dos piratas, por lo que juntaron todas las monedas (excepto las del cocinero)

y las volvieron a repartir. A los 4 que les dieron las 5 que sobraban. Por último, tras una epidemia, murieron 5 piratas y los supervivientes repitieron de nuevo la repartición.

Sabiendo que en el cofre no caben más de 2.500. ¿Cuántas monedas contenía el cofre?

$$\begin{array}{l} x \equiv 5 \pmod{15} \\ x - 5 \equiv 10 \pmod{13} \\ x - 15 \equiv 3 \pmod{8} \end{array} \quad \left\{ \begin{array}{l} x \equiv 5 \pmod{15} \\ x \equiv 2 \pmod{13} \\ x \equiv 2 \pmod{8} \end{array} \right\} \quad \left\{ \begin{array}{l} x = 5 + 15K \\ 5 + 15K \equiv 2 \pmod{13} \\ 5 + 15K \equiv 2 \pmod{8} \end{array} \right. \Rightarrow \begin{array}{l} 15K \equiv -3 \pmod{13} \\ 2K \equiv 10 \pmod{13} \\ K = 5 + 13\bar{K} \end{array}$$

$$x = 5 + 15K = 5 + 15(5 + 13\bar{K}) = 80 + 195\bar{K}$$

$$80 + 195\bar{K} \equiv 2 \pmod{8}$$

$$195\bar{K} \equiv -78 \pmod{8} \\ 3\bar{K} \equiv 2 \pmod{8} \rightarrow \bar{K} = 6 + 8\bar{K}$$

$$x = 80 + 195\bar{K} = 80 + 195(6 + 8\bar{K}) = 80 + 1170 + 1560\bar{K}$$

$$x = 1250 + 1560\bar{K}$$

Solución: 1250 monedas

00272504

• Resolución de ecuaciones diofánticas utilizando congruencia.

① Resolver la ecuación diofántica  $6x + 10y = 14$

$$\text{m.c.d } \{6, 10\} = 2$$

Como  $2 \mid 14$ , la ecuación tiene solución, además tiene las mismas soluciones que la ecuación

$$3x + 5y = 7$$

$$3x \equiv 7 \pmod{5}$$

$$3x \equiv 2 \pmod{5} \rightarrow \boxed{x = 4 + 5k}$$

$$5y = 7 - 3x = 7 - 3(4 + 5k) = -5 - 15k$$

$$\boxed{y = -1 - 3k}$$

② Resolver la ecuación diofántica  $3x - 5y = -2$

$$3x \equiv -2 \pmod{5} \Rightarrow 3x \equiv 3 \pmod{5}$$

$$\boxed{x = 1 + 5k}$$

$$5y = 3x + 2 \rightarrow 5y = 3(1 + 5k) + 2$$

$$5y = 5 + 15k \rightarrow \boxed{y = 1 + 3k}$$

③ Resolver  $9x - 15y + 11z = 3$

$$\text{m.c.d } \{9, 15, 11\} = 1$$

$$9x - 15y = 3u$$

$$\text{m.c.d } \{9, 15\} = 3$$

$$\Rightarrow 3u + 11z = 3$$

$$3u \equiv 3 \pmod{11}$$

$$11z = 3 - 3u$$

$$\boxed{u = 1 + 11k}$$

$$11z = 3 - 3(1 + 11k) = 33k \Rightarrow \boxed{z = -3k}$$

$$9x - 15y = 3u \rightarrow 3x - 5y = u \Rightarrow 3x - 5y = 1 + 11k$$

$$3x \equiv 1 + 11k \pmod{5}$$

si  $a \cdot u + b \cdot v = 1 \Rightarrow b \cdot u \pmod{m}$  es solución de  $ax \equiv b \pmod{m}$

solución.

$$3u + 5v = 1 \rightarrow 2(1 + 11k) \text{ es una solución.}$$

$$3(2) + 5(-1) = 1 \rightarrow$$

$$x = 2(1 + 11k) + 5k \rightarrow \boxed{x = 2 + 22k + 5k}$$

$$-5y = 1 + 11k - 3x \rightarrow -5y = 1 + 11k - 3(2 + 22k + 5k)$$

$$-5y = -5 - 55k - 15k$$

$$\boxed{y = 1 + 11k + 3k}$$

\* El anillo de los enteros, módulo un entero positivo.

Dado un entero positivo  $m$ , denotaremos por  $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$  en  $\mathbb{Z}_m$  definimos una operación suma y una operación producto de la siguiente forma:

$$a \oplus b = (a+b) \text{ mod } m$$

$$a \odot b = (ab) \text{ mod } m$$

Ejemplo: Calcular en  $\mathbb{Z}_6$   $4 \oplus 3$  y  $4 \odot 3$ .

$$\boxed{4 \oplus 3 = (4+3) \text{ mod } 6 = 7 \text{ mod } 6 = 1}$$

$$\boxed{4 \odot 3 = (4 \cdot 3) \text{ mod } 6 = 12 \text{ mod } 6 = 0}$$

• Propiedades de la suma de  $\mathbb{Z}_m$ :

$$1) \text{Comunitativa: } a \oplus b = b \oplus a$$

$$2) \text{Asociativa: } a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$3) \text{Elemento neutro: } a \oplus 0 = a$$

$$4) \text{Elemento inverso: } a \oplus (m-a) = a \quad (-a \text{ inverso de } a)$$

$$5) \text{Cancelativa: } a \oplus c = b \oplus c \Rightarrow a = b$$

• Propiedades del producto de  $\mathbb{Z}_m$ :

$$1) \text{Comunitativa: } a \odot b = b \odot a$$

$$2) \text{Asociativa: } a \odot (b \odot c) = (a \odot b) \odot c$$

$$3) \text{Elemento neutro: } a \odot 1 = a$$

$$4) \text{Distributiva: } a \odot (b + c) = a \odot b + a \odot c$$

**NOTA:** 1) El cero nunca tiene inverso para el producto en  $\mathbb{Z}_m$ . De los elementos distintos de cero, de  $\mathbb{Z}_m$  hay algunos que tienen inverso para el producto y otros que no tienen.

Ej: En  $\mathbb{Z}_4$  los elementos que tienen inverso por el producto, son el 1 y el 3

2) En  $\mathbb{Z}_m$  NO se verifica ni tan siquiera la propiedad cancelativa por elemento distinto de cero, ya que por ejemplo en  $\mathbb{Z}_6 : 30 \cdot 2 = 30 \cdot 4$

A los elementos de  $\mathbb{Z}_m$  que tienen inverso para el producto, se les llaman unidades. Si  $a$  es una unidad denotaremos por  $a^{-1}$  al inverso para el producto de  $a$ .

Ej: Calcular las unidades de  $\mathbb{Z}_5$

$$U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$$

$$1^{-1} = 1 \quad 3^{-1} = 2 \\ 2^{-1} = 3 \quad 4^{-1} = 4$$

Teorema:

Un elemento  $a \in \mathbb{Z}_m$  tiene inverso para el producto si y solo si el m.c.d  $\{a, m\} = 1$ . Además, si  $a \cdot u + m \cdot v = 1$  con  $u, v \in \mathbb{Z}$  entonces  $a^{-1} = u \text{ mod } m$ .

Ej: Calcular las unidades de  $\mathbb{Z}_{12}$ :

~~$$U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$$~~

Calcular el inverso para el producto de 35 en  $\mathbb{Z}_{97}$ :

$$\text{m.c.d } \{35, 97\} = 1$$

$$a \cdot u + m \cdot v = 1$$

$$35 \cdot u + 97 \cdot v = 1 \quad \begin{cases} u = \\ v = \end{cases}$$

Aplicamos Alg. Ext. Eucl.

$$(a_0, a_1) = (97, 35) \xrightarrow{q=2} (35, 27) \xrightarrow{q=1} (27, 8) \xrightarrow{q=3} (8, 3) \xrightarrow{q=2} (3, 2) \xrightarrow{q=1} (2, 1) \xrightarrow{q=1} (1, 0)$$

$$(s_0, s_1) = (1, 0) = (0, 1) = (1, -1) = (-1, 1) = (4, -9) = (-9, 13) = (13, -)$$

$$(t_0, t_1) = (0, 1) = (1, -2) = (-2, 3) = (3, -11) = (-11, 25) = (25, 36) = (-36, -)$$

$$97 \cdot 13 + 35 \cdot (-36) = 1$$

$$\begin{matrix} u = -36 \\ v = 13 \end{matrix} \Rightarrow 35^{-1} = (-36) \text{ mod } 97$$

$$\boxed{35^{-1} = 61}$$

# PRACTICAS 20/10/15

- Calcular, si es posible,  $1392^{-1}$  en  $\mathbb{Z}_{7585}$

Encontrar  $x \in \mathbb{Z}_{7585}$  tq  ~~$1392x \equiv 1 \pmod{7585}$~~

$$1392x \equiv 1 \pmod{7585} \rightarrow 7585x + 1392y = 1$$

Aplicamos Algoritmo de Euclides gen.

$$(a_0, a_1) = (7585, 1392) \stackrel{q=5}{=} (1392, 625) =$$

$$(s_0, s_1) = (1, 0) = (0, 1) =$$

$$(t_0, t_1) = (0, 1) = (1, -5) =$$

$$\begin{aligned} * q=2 & \\ = (625, 142) & \stackrel{q=4}{=} (142, 57) \dots = (1, 0) \end{aligned}$$

$$= (1, -2) = (-2, 9) \dots = (49, -)$$

$$= (-5, 11) = (11, -49) \dots = (-267, -)$$

$$1392x - 7585y = 1 \rightarrow 7585a + 1392b = 1$$

$$\begin{aligned} a &= 49 \\ b &= -267 \end{aligned}$$

$$\begin{aligned} a &= -y \\ b &= x \end{aligned}$$

$$\text{Soluciones: } a = 49 + 1392k$$

$$b = -267 - 7585k$$

$$7585 \cdot 49 + 1392(-267) = 1$$

$$1392 \cdot \frac{-267}{49} \equiv 1 \pmod{7585}$$

-267 no está en  $\mathbb{Z}_{7585}$

$$-267 + 7585 = 7318 \in \mathbb{Z}_{7585}$$

$$1392 \cdot \frac{7318}{49} \equiv 1 \pmod{7585}$$

El inverso es para  $k = -1 \rightarrow 7318$



• Resuelve las congruencias:

$$\rightarrow 3x \equiv 2 \pmod{5}$$

$$\rightarrow 7x \equiv 4 \pmod{10}$$

$$1) \rightarrow 3x \equiv 2 \pmod{5}$$

$$3u - 5v = 2 \quad \begin{cases} u=4 \\ v=1 \end{cases} \rightarrow \boxed{x=4}$$

$$\boxed{\{ 4 + 5k \mid k \in \mathbb{Z} \}}$$

$$2) \rightarrow 7x \equiv 4 \pmod{10}$$

$$7u - 10v = 4 \quad \begin{cases} u=2 \\ v=1 \end{cases} \rightarrow \boxed{x=2}$$

$$\boxed{\{ 2 + 10k \mid k \in \mathbb{Z} \}}$$

• Resuelve el sistema.

$$x \equiv 1 \pmod{2} \quad \rightarrow x = 3 \quad \{ 3 + 2k \mid k \in \mathbb{Z} \}$$

$$6x \equiv 3 \pmod{9} \quad \rightarrow 6(3+2k) \equiv 3 \pmod{9}$$

$$3x \equiv 3 \pmod{5} \quad \rightarrow 18 + 12k \equiv 3 \pmod{9}$$

$$12k \equiv -15 \pmod{9}$$

$$12k \equiv 3 \pmod{9}$$

$$k=1 \rightarrow \{ 1 + 9\bar{k} \mid \bar{k} \in \mathbb{Z} \}$$

$$3(1+9\bar{k}) \equiv 3 \pmod{5}$$

$$3 + 27\bar{k} \equiv 3 \pmod{5}$$

$$27\bar{k} \equiv 0 \pmod{5} \rightarrow \{ 5\bar{k} \mid \bar{k} \in \mathbb{Z} \}$$

$$x = 3 + 2(1 + 9(\bar{s}))$$

$$\boxed{x = 5 + 90\bar{k} \mid \bar{k} \in \mathbb{Z}}$$

$$3 + 2(1 + 45\bar{k})$$

$$\rightarrow \boxed{3 + 2 + 90\bar{k} \mid \bar{k} \in \mathbb{Z}}$$

## Ejercicio:

① Resuelve en  $\mathbb{Z}_9$  la ecuación  $x+7 = 5x+2$

$$\begin{aligned} x+7 &= 5x+2 \\ 4x &= 5 \rightarrow \text{Como m.c.d } \{4, 9\} = 1, \text{ entonces} \\ &\exists 4^{-1} \\ \Rightarrow 4^{-1} \cdot 4x &= 4^{-1} \cdot 5 \Rightarrow x = 4^{-1} \cdot 5 \Rightarrow x = 7 \cdot 5 \Rightarrow x = 8 \end{aligned}$$

② Resuelve en  $\mathbb{Z}_7$  la ecuación  $3x+6 = x+2$

$$\begin{aligned} 3x+6 &= x+2 \\ 2x &= -4 \rightarrow 2x = 3 \rightarrow \text{m.c.d } \{2, 7\} = 1 \Rightarrow \\ &\exists 2^{-1} \Rightarrow 2^{-1} \cdot 2x = 2^{-1} \cdot 3 \Rightarrow x = 4 \cdot 3 \Rightarrow x = 5 \end{aligned}$$

③ Resuelve en  $\mathbb{Z}_9$  la ecuación  $6x = 0$

m.c.d  $\{6, 9\} = 3 \neq 1$  entonces no existe  $6^{-1}$

$$6x \equiv 0 \pmod{9}$$

$$2x \equiv 0 \pmod{3}$$

$$x = 0 + 3K \rightarrow \text{Solución: } \{0, 3, 6\}$$

④ Resuelve en  $\mathbb{Z}_{20}$  la ecuación  $x+5 = 7x+1 \Rightarrow 6x = 4$

Como m.c.d  $\{6, 20\} = 2 \neq 1$  no existe  $6^{-1} \Rightarrow$

$$\text{se resuelve} \rightarrow 6x \equiv 4 \pmod{20}$$

$$3x \equiv 2 \pmod{10}$$

$$x = 4 + 10K \rightarrow \text{Solución: } \{4, 14\}$$

⑤ Resolver en  $\mathbb{Z}_{25}$  la ecuación  $8x+3 = 3x+2 \Rightarrow 5x = -1 \Rightarrow 5x = 24$

m.c.d  $\{5, 25\} = 5 \neq 1 \rightarrow \text{No existe } 5^{-1} \Rightarrow$

$5x \equiv 24 \pmod{25}$  Esta congruencia no tiene solución

y por tanto, la ecuación que nos dieron en  $\mathbb{Z}_{25}$

No tiene solución. (Ningún  $n \in \mathbb{Z}_{25}$  verifica esa igualdad).

## PROPOSICIÓN:

Sean  $a_1, a_2, \dots, a_k, m \in \mathbb{Z}$  y  $m \neq 0$ .

$$1) (a_1 + a_2 + \dots + a_k) \bmod m = (a_1 \bmod m + a_2 \bmod m + \dots + a_k \bmod m) \bmod m$$

$$2) (a_1 \cdot a_2 \cdot \dots \cdot a_k) \bmod m = (a_1 \bmod m \cdot a_2 \bmod m \cdot \dots \cdot a_k \bmod m) \bmod m$$

Ejemplos:

① Calcular el resto de dividir  $4225^{1000}$  entre 7.

$$(4225^{1000} \bmod 7)$$

$$= (4225 \cdots 4225) \bmod 7 =$$

$$= (4225 \bmod 7 \cdot 4225 \bmod 7 \cdots)^{(1000)} \bmod 7 =$$

$$\text{Calculamos } 4225 \bmod 7 = 4$$

$$\Rightarrow (4 \cdots 4) \bmod 7 = 4^{1000} \bmod 7$$

$$4^1 \bmod 7 = 4$$

$$4^2 \bmod 7 = 2$$

$$4^3 \bmod 7 = \underline{\underline{1}}$$

$$\Rightarrow 4^{1000} \bmod 7 = 4^{3 \cdot 333+1} \bmod 7 = (4^{3 \cdot 333} \cdot 4^1) \bmod 7 =$$

$$= (4^3 \cdots 4^3 \cdot 4^1) \bmod 7 =$$

$$= \underbrace{(4^3 \bmod 7 \cdots 4^3 \bmod 7 \cdot 4^1 \bmod 7)}_{\downarrow} \bmod 7 =$$

$$= 4 \bmod 7 = \boxed{4}$$

③ Calcular el resto de dividir  $162^{197}$  entre 5

Nos piden  $162^{197} \bmod 5$

$$\Rightarrow (162 \cdots 162)^{(197)} \bmod 5 =$$

$$= (162 \bmod 5 \cdots 162 \bmod 5)^{(197)} \bmod 5 =$$

$$\text{Calcularemos } 162 \bmod 5 = 2$$

$$\Rightarrow (2 \cdots 2)^{(197)} \bmod 5 = 2^{197} \bmod 5$$

$$2^1 \bmod 5 = 2$$

$$2^2 \bmod 5 = 2$$

$$2^3 \bmod 5 = 3$$

$$2^4 \bmod 5 = 1$$

$$\Rightarrow 2^{197} \bmod 5 = 2^{4 \cdot 49 + 1} \bmod 5 =$$

$$= (2^4 \cdots 2^4 \cdot 2^1)^{(49)} \bmod 5 =$$

$$= (\underbrace{2^4 \bmod 5}_{1} \cdots \underbrace{2^4 \bmod 5 \cdot 2^1 \bmod 5}_{2}) \bmod 5 =$$

$$= 2 \bmod 5 = \boxed{2}$$

③ Demuestra que  $m \in \mathbb{Z} \Rightarrow m^2 \equiv 0 \pmod{8}$

$$m^2 \equiv 0 \pmod{8}$$

$$m^2 \equiv 1 \pmod{8}$$

$$m^2 \equiv 4 \pmod{8}$$

Además, prueba que  
 $8^{125} + 4^{12} + 3$  No tiene  
raíz cuadrada exacta.

Dividimos  $m$  entre 8, entonces  $m = q \cdot 8 + r$

con  $r \in \{0, 1, \dots, 7\}$ . Entonces  $m^2 = (q \cdot 8 + r)^2 = q^2 \cdot 8^2 + 2 \cdot q \cdot 8 \cdot r + r^2$

$$m^2 \pmod{8} = (q^2 \cdot 8^2 + 2 \cdot q \cdot 8 \cdot r + r^2) \pmod{8} =$$

$$= (\underbrace{q^2 \cdot 8^2 \pmod{8}}_0 + \underbrace{2 \cdot q \cdot 8 \cdot r \pmod{8}}_0 + \underbrace{r^2 \pmod{8}}_r) \pmod{8} =$$

$\rightarrow$  Al ser mult de 8, el resto es 0

$$= (r^2 \pmod{8}) \pmod{8} = r^2 \pmod{8}$$

El ejercicio, lo que nos viene a decir es que el resto de dividir  $m^2$  entre 8 vale 0 o 1 o 4

$$0^2 \pmod{8} = 0$$

$$1^2 \pmod{8} = 1$$

$$2^2 \pmod{8} = 4$$

$$3^2 \pmod{8} = 1$$

$$4^2 \pmod{8} = 0$$

$$5^2 \pmod{8} = 1$$

$$6^2 \pmod{8} = 4$$

$$7^2 \pmod{8} = 1$$

Así demostramos que

$$m^2 \equiv 0 \pmod{8}$$

$$m^2 \equiv 1 \pmod{8}$$

$$m^2 \equiv 4 \pmod{8}$$

$$(8^{125} + 4^{12} + 3) \pmod{8} = (\underbrace{8^{125} \pmod{8}}_0 + \underbrace{4^{12} \pmod{8}}_0 + \underbrace{3 \pmod{8}}_3) \pmod{8} =$$

$$= 3 \pmod{8} = 3 \quad \text{No tiene raíz cuadrada exacta.}$$

## \* Sistema de enumeración

Sea  $B$  un entero  $\geq 2$ , entonces todo  $n^o$  natural  $\neq 0$  se puede poner de forma única como  $n = a_k B^k + a_{k-1} B^{k-1} + \dots + a_1 B + a_0$  con  $a_i \in \{0, 1, \dots, B-1\}$   $\forall i \in \{0, 1, \dots, k\}$  y  $a_k \neq 0$ .

A la  $k+1$ -tuple  $(a_k, a_{k-1}, \dots, a_1, a_0)$  la llamaremos expresión en base  $B$  del  $n^o$  natural  $n$ .

Por definición (0) es la expresión en base  $B$  del  $n^o$  natural cero.

Ejemplo:

1) Calcular la expresión en base 3 del  $n^o$  25.

$$25 = 2 \cdot 3^2 + 2 \cdot 3^1 + 1 \rightarrow (2, 2, 1)$$

2) Calcular la expresión en base 2 del  $n^o$  39

$$39 = 1 \cdot 2^5 + 3 \cdot 2^4 + 1 \rightarrow (1, 3, 1)$$

$$= 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \rightarrow (1, 0, 0, 1, 1, 1)$$

3) Calcular la expresión en base 7 del  $n^o$  12523

$$\begin{array}{r} 12523 \\ \hline 55 & 38 & 255 & 17 \\ 62 & 39 & 45 & 36 \\ \boxed{0} & \boxed{4} & \boxed{3} & \boxed{1} \boxed{5} \end{array} \rightarrow (5, 1, 3, 4, 0)$$

4) Calcular la expresión en base 5 del  $n^o$  3227

$$\begin{array}{r} 3227 \\ \hline 22 & 645 & 129 & 25 & 5 \\ 27 & 45 & 29 & 25 & 5 \\ \boxed{2} & \boxed{10} & \boxed{14} & \boxed{10} & \boxed{15} \\ & \boxed{0} & \boxed{1} & \boxed{15} & \boxed{15} \\ & & \boxed{0} & \boxed{1} & \boxed{1} \end{array} \rightarrow \begin{array}{l} \cancel{(0, 4, 0, 2)} \\ (1, 0, 0, 4, 0, 2) \end{array}$$

5) Si la expresión de un nº en base 3 es  $(1,2,0,1,1)_3$   
 Calcular la expresión de dicho número en base 8.

El nº es  ~~$3^3 + 2 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0$~~   
 $1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 1 = 81 + 54 + 3 + 1$   
 $(1,2,0,1,1)_3 = 139$

$$(139)_8 \Rightarrow \begin{array}{r} 139 \\ \underline{-59} \\ 80 \\ \underline{-17} \\ 13 \\ \underline{-12} \\ 1 \end{array} \Rightarrow (2,1,3)$$

Ejercicio: Calcular  $(2,3,4)_5 + (4,3,3,3)_5$  y  
 $(2,3,4)_5 \cdot (4,3,3,3)_5$

1)  $(2,3,4)_5 = 2 \cdot 5^2 + 3 \cdot 5^1 + 4 =$

2)  ~~$(2,3,4)_5$~~   $(4,3,3,3)_5 = 4 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5^1 + 3 =$

$$\begin{array}{r} 4333 \\ + 234 \\ \hline 10122 \end{array} \Rightarrow (2,3,4)_5 + (4,3,3,3)_5 = (10,1,2,2)_5$$

$$\begin{array}{r} 4333 \\ \times 234 \\ \hline 13021 \\ 24104 \\ + 14221 \\ \hline 1302132 \end{array} \Rightarrow (2,3,4)_5 \cdot (4,3,3,3)_5 = (2,3,0,2,1,3,2)_5$$

$$(5,0,0,0,0,1) \quad \text{Base 8}$$

Ejercicio: Calcular  $(4,5,6)_7 \cdot (4,5)_7 = (3,1,5,4,2)_7$

\*Método para pasar de base B a base una potencia de B

Si la expresión en base 2 de un n° es (1,0,1,1,0,1,1,0,1,1,  
1,0,1,0,0,0,~~1~~)<sup>(1,1)</sup>

⇒ Calcular la expresión en base 8 de dicho número

$$(1,0,1,0,1,1,0,1,1,0,1,1,1,0,1,0,0,0,0,1,1) \quad 8=23$$

Solución :  $(2, 5, 5, 5, 6, 4, 3)$

② La expresión en base 3 de un nº es

$$(1, \underline{2, 0}, 1, \underline{2, 1}, 2, 0, 1, 2, 2, 1, 0+1) \rightarrow \text{Calcular en base } q \\ (1, 6, 4, 8, 5, 7, 1) \qquad q = 3^2 *$$

③ Si la expresión en base 8 de un n° es 635  
Calcular la expresión de dicho n° en base 2

$$\begin{array}{c} \cancel{6} \cancel{3} \cancel{5} \cancel{1} \\ \cancel{0} \cancel{1} \cancel{5} \cancel{3} \cancel{1} \cancel{7} \cancel{1} \\ \cancel{6} \cancel{3} \cancel{1} \cancel{1} \cancel{1} \cancel{5} \cancel{3} \cancel{1} \\ \cancel{1} \cancel{7} \cancel{1} \cancel{4} \end{array} \rightarrow \begin{array}{ccc} 6 & 3 & 5 \\ 110 & 011 & 101 \end{array}$$

④ Si la expresión en base 10 de un n° es 15861  
 Calcular la exp. de dicho n° en base 100  $\Rightarrow 10^2$

(1,58,61)

⑥ Si la expresión de un nº en base 100 es  $(25, 1, 37, 2, 24)$   
Calcular la expresión de dicho nº en base 10.

$$(2501370224)_{10}$$

Ejercicios:

1) Encuentrar la base (si existe) entre  $(4, 1)_B \cdot (1, 4)_B = (1, 2, 2, 4)_B$

$$(4, 1)_B \cdot (1, 4)_B = (1, 2, 2, 4)_B$$

$$(4B+1) \cdot (B+4) = B^3 + 2B^2 + 2B + 4$$

$$4B^2 + 17B + 4 = B^3 + 2B^2 + 2B + 4$$

$$B^3 - 2B^2 - 15B = 0$$

$$B(B^2 - 2B - 15) = 0 \xrightarrow{B=0} B=B^2 - 2B - 15 \Rightarrow \boxed{B=5} \quad \boxed{B=-3}$$

La solución es siempre positiva  $> 0$

2) Demostrar que un número escrito en base 10 es  
múltiplo de 3 si y sólo si la suma de  
sus cifras es múltiplo de 3.

$$(a_n, a_{n-1}, \dots, a_1, a_0)_{10} \text{ es múltiplo de } 3 \iff (a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0) \mod 3 = 0$$
$$\iff (a_n \cdot 10^n \mod 3 + a_{n-1} \cdot 10^{n-1} \mod 3, \dots, + a_1 \cdot 10 \mod 3 + a_0 \mod 3) \mod 3 = 0$$

Valemos a ver qué vale  $a_i \cdot 10^i \mod 3 = (a_i \mod 3 \cdot \underbrace{10 \mod 3}_{\mod 3} \cdots \underbrace{10 \mod 3}_{\mod 3})$

$$= (a_i \mod 3) \mod 3 = a_i \mod 3$$

Por lo tanto  $(a_n \mod 3 + a_{n-1} \mod 3 + \dots + a_1 \mod 3 + a_0 \mod 3) \mod 3 = 0$

$$\iff (a_n + a_{n-1} + \dots + a_1 + a_0) \mod 3 = 0 \iff$$

$\boxed{a_n + a_{n-1} + \dots + a_1 + a_0 \text{ es mult. de 3}}$

Para demostrar que es múltiplo de 9, es exactamente igual, cambiando 3 por 9.

3) ¿Cuando un número, escrito en base  $a$ , es múltiplo de 4?

$$(a_n, a_{n-1}, \dots, a_1, a_0)_q \text{ es mult. de 4} \Leftrightarrow (a_n q^n + a_{n-1} q^{n-1} + \dots + a_1 q + a_0) \bmod 4 = 0$$

$$\Leftrightarrow (a_n q^n \bmod 4 + a_{n-1} q^{n-1} \bmod 4 + \dots + a_1 q \bmod 4 + a_0 \bmod 4) \bmod 4 = 0 \Leftrightarrow$$

$$(a_n \bmod 4 + a_{n-1} \bmod 4 + \dots + a_1 \bmod 4 + a_0 \bmod 4) \bmod 4 = 0 \Leftrightarrow$$

$$(a_n + a_{n-1} + \dots + a_1 + a_0) \bmod 4 = 0 \Leftrightarrow a_n + a_{n-1} + \dots + a_1 + a_0 \text{ es mult de 4}$$

\* 4) Cuántos números hay en el intervalo  $[1000, 2000]$  que al expresarlos en base 8, terminan en 12 y que al expresarlos en base 9, terminan en 15.

$$\textcircled{1} (\dots 12)_8 ; \textcircled{2} (\dots 15)_9$$

$$\textcircled{1} x = a_n 8^n + a_{n-1} 8^{n-1} + \dots + a_2 8^2 + 1 \cdot 8 + 2$$

$$\frac{x \bmod 8^2 = 10}{}$$

$$\hookrightarrow x \equiv 10 \pmod{64}$$

$$\textcircled{2} x = a_n 9^n + a_{n-1} 9^{n-1} + \dots + a_2 9^2 + 1 \cdot 9 + 5$$

$$\frac{x \bmod 9^2 = 14}{}$$

$$\hookrightarrow x \equiv 14 \pmod{81}$$

$$x \equiv 10 \pmod{64} \quad \rightarrow x = 10 + 64k$$

$$x \equiv 14 \pmod{81} \quad \rightarrow 10 + 64k \equiv 14 \pmod{81}$$

$$64k \equiv 4 \pmod{81}$$

Aplicamos Algor. Ext. Euclides:

$$(a_0, a_1) = (81, 64) = (64, 17) = (17, 13) = (13, 4) = (4, 1) = (1, 0)$$

$$(S_0, S_1) = (1, 0) = (0, 1) = (1, -3) = (-3, 4) = (4, -15) = (-15, -)$$

$$(t_0, t_1) = (0, 1) = (1, -1) = (-1, 4) = (4, -5) = (-5, 19) = (19, -)$$

$$81(-15) + 64(19) = 1$$

Sabemos por el teorema Largo (pto 6)<sup>qe</sup> si  $a|u + bn.v = 1$  entonces  $bv \bmod u$  es una solución de  $ax \equiv b \pmod{u}$

Por tanto  $K = 4 \cdot 19 \bmod 81 \rightarrow K = 76 \bmod 81 \Rightarrow K = 76$  es 1 sol.

y por consiguiente, el conjunto de todas sus soluciones es

$$\{76 + 81\bar{K} \mid \bar{K} \in \mathbb{Z}\}$$

Continuamos el sistema:  $x = 10 + 64(76 + 81\bar{K})$

$$x = 4874 + 5184\bar{K}$$

Por lo tanto, como necesitamos un valor entre  $[1000, 2000]$ ,

NO EXISTE

5) Calcular todos los  $\text{n}^{\circ}$  naturales que al expresarlos en base 2, terminan en  $(\dots 101)_2$  y al expresarlos en base 3, terminan en  $(\dots 21)_3$

$$x = a_0 \cdot 2^n + a_1 \cdot 2^{n-1} + a_2 \cdot 2^2 +$$

$$2 \cdot 3^1 + 1 \cdot$$

$$6 + 1 = 7$$

$$1) x \equiv 5 \pmod{8} \rightarrow 1 \cdot 2^2 + 0 \cdot 2^1 + 1 = 5 \quad ||| \quad 2^3 = 8$$

$$2) x \equiv 7 \pmod{9} \rightarrow 2 \cdot 3^1 + 1 = 7 \quad ||| \quad 3^2 = 9$$

6) Resolver la ecuación diofántica:

$$28x - 42y + 49z = 35$$

7) ¿Cuántos divisores tiene el  $\text{n}^{\circ} 10!$ ?

$$\begin{aligned} 10! &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1 \end{aligned}$$

$$\Rightarrow (8+1)(4+1)(2+1)(1+1) = 270 +$$

$10!$  tiene 540 divisores (270+ y 270)

Fecha entrega actividades 13 de Nov: (viernes)

Se puede entregar a Jesús García Miranda.

En pareja, también se defiende.

- Encuentra los sistemas de numeración para los que se verifica:

$$1 \rightarrow 3 \times 4 = 22$$

$$2 \rightarrow 41 \times 14 = 1224$$

$$1) \quad 3_B \cdot 4_B = 22_B$$

$$3_B \cdot 4_B = 2B + 2$$

$$12B = 2B + 2 \rightarrow 2B = 10$$

$$10B = 12 \rightarrow B = 5$$

$$\boxed{B = 5}$$

$$2) \quad 41_B \cdot 14_B = 1224_B$$

$$(4B+1)(B+4) = B^3 + 2B^2 + 2B + 4$$

$$4B^2 + 17B + 4 = B^3 + 2B^2 + 2B + 4$$

$$B^3 - 2B^2 - 15B = 0$$

$$B(B^2 - 2B - 15) = 0 \quad \begin{cases} B=0 \\ B=B^2 - 2B - 15 = 0 \end{cases} \quad \boxed{B=5}$$

Se toma siempre las soluciones  $\geq 0$  y naturales. !!

Demuestra que un número escrito en base 10 es par si y solo si, su última cifra es par

$$(a_n, a_{n-1}, \dots, a_1, a_0)_{10} \text{ es par} \iff (a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0) \bmod 2 = 0$$

$$\iff (\cancel{a_n \cdot 10^n} \bmod 2 + \cancel{a_{n-1} \cdot 10^{n-1}} \bmod 2 + \dots + \cancel{a_1 \cdot 10} \bmod 2 + a_0 \bmod 2) \bmod 2 = 0 \iff$$

$$(a_n \bmod 2 + a_{n-1} \bmod 2 + \dots + a_1 \bmod 2 + a_0 \bmod 2) \bmod 2 = 0 \iff$$

$$(a_n + a_{n-1} + \dots + a_1 + a_0) \bmod 2 = 0 \iff a_n + a_{n-1} + \dots + a_1 + a_0 \text{ es par}$$

No

- Debe verse que un número en base 10 es múltiplo de 4 si y solo si, su última cifra es más de dos veces la penúltima es mult. 4

$\times \text{ es mult. 4}$

$$\Leftrightarrow a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0 \equiv 0 \pmod{4} \Leftrightarrow a_n(10^n \pmod{4}) + \dots + a_1(10 \pmod{4}) + a_0 \pmod{4} \equiv 0 \pmod{4}$$

$$\Leftrightarrow 2a_1 + a_0 \equiv \pmod{4} \Leftrightarrow 2a_1 + a_0 \underset{\substack{\text{es mult. 4} \\ \text{es mult. 4}}}{\underset{2}{\equiv}} 0 \pmod{4}$$

$$10^n \equiv 0 \pmod{4} \rightarrow n \geq 2$$

- Si  $a_n, a_{n-1}, \dots, a_1, a_0$  es la expresión decimal de un  $n^o x$ , entonces  $x$  es un múltiplo de 7, si, y solo si, el número  $y = a_n a_{n-1} \dots a_2 a_1 - 2a_0$  es múltiplo de 7.

Pista: Comprueba que  $x \equiv 3y \pmod{7}$

$$y \equiv 0 \pmod{7}$$

$$\text{Si } x \equiv 0 \pmod{7} \Leftrightarrow 3y \equiv 0 \pmod{7} \Leftrightarrow \text{m.c.d}(3, 7) \Rightarrow \cancel{y \equiv 0 \pmod{7}}$$

$$10^n a_n + \dots + 10 a_1 + a_0 \equiv 3(a_n 10^{n-1} + \dots + 10 a_2 + a_1 - 2a_0) \pmod{7}$$

$$3^na_n + \dots + 3a_1 + a_0 \equiv 3 \cdot 3^{n-1} \cdot a_n + \dots + 3 \cdot 3a_2 + 3 \cdot a_1 - 6a_0 \pmod{7}$$

$$a_0 \equiv -6a_0 \pmod{7} \Leftrightarrow 7a_0 \equiv 0 \pmod{7}$$

~~2~~

$$a_n + a_{n-1} + \dots + a_1 + a_0 \equiv 0 \pmod{7}$$

El resultado es más sencillo y se aplica.

Resumiendo, se ha visto que el resto en la división entera de  $x$  entre 7 es igual a:

$$= 36a_0 + 1 \cdot a_1 + 10 \cdot a_2 + \dots + 10^{n-1} \cdot a_n \Leftrightarrow 3a_0 + a_1 + 3a_2 + \dots + 3a_{n-1} + a_n \pmod{7}$$

$$= 3(a_0 + a_2 + \dots + a_{n-2} + a_{n-1}) + a_1 + a_3 + \dots + a_{n-1} + a_n \pmod{7}$$

$$\Rightarrow 0 \cdot 36a_0 + 1 \cdot a_1 + 3a_2 + \dots + 3a_{n-1} + a_n \pmod{7}$$

$$= a_1 + a_3 + \dots + a_{n-1} + a_n \pmod{7}$$

### Tema 3 → El anillo de los polinomios con coeficiente en un cuerpo.

Un anillo es una terna  $(R, +, \cdot)$  donde  $R$  es un conjunto y " $+$ " y " $\cdot$ " son dos operaciones verificando las siguientes propiedades:

- 1) La operación " $+$ " es asociativa, conmutativa, tiene elemento neutro (que denotaremos "0") y todo elemento tiene inverso (Al inverso para la suma de  $a$ , lo denotaremos  $-a$ ).
- 2) La operación " $\cdot$ " es asociativa, tiene elemento neutro (que denotaremos "1") y se verifica la propiedad distributiva.

Si además la operación " $\cdot$ " es conmutativa, diremos que el anillo es conmutativo.

Un cuerpo es un anillo conmutativo en el que todo elemento distinto de "0" tiene inverso para el producto. (Al inverso para el producto de  $a$ , lo denotaremos  $a^{-1}$ )

Nota:

- 1)  $(\mathbb{Z}, +, \cdot)$  es un anillo conmutativo y no es un cuerpo.
- 2)  $(R, +, \cdot)$  es un anillo conmutativo y también un cuerpo  
También es ejemplo  $(\mathbb{Q}, +, \cdot)$
- 3)  $(\mathbb{Z}_6, +, \cdot)$  es un anillo conmutativo y no un cuerpo.
- 4)  $(\mathbb{Z}_5, +, \cdot)$  es un anillo conmutativo y también un cuerpo.

PROPOSICIÓN:  
 $(\mathbb{Z}_n, +, \cdot)$  siempre es un anillo conmutativo, además, es cuerpo, si, y solamente si " $n$ " es primo.

Sea  $K$  un cuerpo. El conjunto de los polinomios con coeficiente en el cuerpo  $K$  y con la indeterminada  $x$  es  $K[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N} \text{ y } a_0, a_1, \dots, a_n \in K\}$

\*Proposición:

$K[x]$  es un anillo conmutativo (y NO un cuerpo) con las operaciones suma y producto de polinomios.

Ejercicio:

Sean  $a(x) = 3x^2 + 4x + 2$ ,  $b(x) = 3x + 2 \in \mathbb{Z}_5[x]$

Calcular  $a(x) + b(x)$  y  $a(x) \cdot b(x)$

$$1) a(x) + b(x) = 3x^2 + 2x + 4$$

$$2) a(x) \cdot b(x) \Rightarrow 4x^3 + 3x^2 + 4x + 4$$

$$\begin{array}{r} 3x^2 + 4x + 2 \\ 3x + 2 \\ \hline 4x^3 + 2x^2 + x \\ x^2 + 3x + 4 \\ \hline 4x^3 + 3x^2 + 4x + 4 \end{array} \rightarrow a(x) \cdot b(x)$$

Si  $a(x) = a_0 + a_1x + \dots + a_nx^n$  con  $a_n \neq 0$  entonces diremos que  $n$  es el grado del polinomio  $a(x)$  y lo denotaremos  $\text{gr}(a(x))$ .

Por definición diremos que el grado del polinomio "0" es  $-\infty$ .

Proposición:

$$\text{gr}(a(x) \cdot b(x)) = \text{gr}(a(x)) + \text{gr}(b(x)).$$

- Un elemento  $a$  de un anillo  $R$  es una unidad si tiene inverso para el producto.
- Un elemento  $a$  de un anillo  $R$  diremos que es un divisor de cero si  $a \neq 0$  y  $\exists b \neq 0$  tq  $a \cdot b = 0$

Ejercicio:

Calcular las unidades y los divisores de  $\mathbb{Z}_6$

$$U(\mathbb{Z}_6) = \{1, 5\}$$

$$DG(\mathbb{Z}_6) = \{2, 3, 4\}$$

NOTA:

~~$U(\mathbb{Z}_m), DG(\mathbb{Z}_m), \{0\}$  es una partición de  $\mathbb{Z}_m$~~

En  $\mathbb{Z}_m$ , los divisores de cero son los elementos que no son ni cero ni unidad.

Ej: Calcular  $U(\mathbb{Z})$  y  $DG(\mathbb{Z})$

$$U(\mathbb{Z}) = \{1, -1\}$$

$$DG(\mathbb{Z}) = \emptyset$$

Proposición:

Si  $K$  es un cuerpo, entonces  $U(K) = K - \{0\}$

$$\text{y } DG(K) = \emptyset$$

Proposición:

El conjunto de las unidades de  $K[x]$  es  $\rightarrow U(K[x]) =$

$$\{a[x] \in K[x] \text{ tq gr}(a[x]) = 0\} = K - \{0\}$$

$$DG(K[x]) = \emptyset$$

Un polinomio  $a(x) \in K[x]$  diremos que es irreducible si verifica lo siguiente:

- 1)  $\text{gr}(a(x)) \geq 1$
- 2) Si  $a(x) = b(x) \cdot c(x)$  entonces  $\text{gr}(b(x)) = 0$  ó  $\text{gr}(c(x)) = 0$

Ejercicio:

¿Es irreducible  $x^2+x \in \mathbb{Z}_3[x]$ ?

No es irreducible, ya que  $x^2+x = x(x+1)$

¿Es irreducible  $x^3+x+1 \in \mathbb{Z}_2[x]$ ?

Vamos a ver que sí es irreducible. Si no fuese irreducible, sería producto de un polinomio de grado 1 y otro de grado 2.

El conjunto de todos los polinomios de grado 1 de  $\mathbb{Z}_2[x]$  es  $\{x+1, x\}$  y el conjunto de todos los polinomios de grado 2 de  $\mathbb{Z}_2[x]$  es  $\{x^2, x^2+1, x^2+x+1, x^2+x\}$

$$(x+1)x^2$$

$$(x+1)(x^2+1)$$

$$(x+1)(x^2+x+1)$$

⋮

Ninguno de esos polinomio nos da el nuestro, por lo tanto es irreducible.

## PROPOSICIÓN:

- 1) todo polinomio  $K[x]$  de grado 1, es irreducible
- 2) Si un polinomio de  $K[x]$  irreducible lo multiplicamos por un elemento del cuerpo  $\neq 0$  entonces obtenemos otro polinomio irreducible.

Un polinomio diremos que es monómico si el coeficiente del término de mayor grado (llamado coeficiente líder) vale 1.

## • Teorema:

Un polinomio  $a(x) \in K[x]$  de grado  $\geq 1$  se puede poner de forma única (salvo reordenaciones) como  $a(x) = u P_1(x)^{\alpha_1} \cdot P_2(x)^{\alpha_2} \cdots P_r(x)^{\alpha_r}$  donde  $u \in K - \{0\}$ ,  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$ , y  $P_1(x), \dots, P_r(x)$  son polinomios monómicos e irreducibles.

A esta expresión la llamaremos "la descomposición en irreducibles del polinomio  $a(x)$ ".

### Ejercicio:

→ Calcular la descomposición en irreducibles del polinomio  $a(x) = (4x+3)(3x+2) \in \mathbb{Z}_7[x]$

Esto es una descomposición en irreducibles del polinomio  $a(x)$ , pero dicha descomposición no es la descomposición en irreducibles de  $a(x)$  porque no son monómicos los polinomios

$$a(x) = 4 \cdot 2 (4x+3) \nmid 5 (3x+2) \Rightarrow [a(x) = 5(x+6)(x+3)]$$

Sea  $a(x), b(x) \in K[x]$ , diremos que  $a(x)$  divide a  $b(x)$  y lo denotaremos  $a(x) | b(x)$  si  $\exists c(x) \in K[x]$  tq  $b(x) = a(x) \cdot c(x)$

Sea  $a(x), b(x) \in K[x]$  tq  $a(x) \neq 0$  ó  $b(x) \neq 0$

Un polinomio  $d(x) \in K[x]$  diremos que es un máximo común divisor de  $a(x)$  y  $b(x)$  si verifica lo siguiente:

$$1) d(x) | a(x) \text{ y } d(x) | b(x)$$

$$2) \text{ si } c(x) | a(x) \text{ y } c(x) | b(x) \Rightarrow c(x) | d(x)$$

NOTA: Si  $d(x)$  es un m.c.d. { $a(x), b(x)$ } entonces también lo es  $ud(x)$   $\forall u \in K - \{0\}$

Cuando escribamos  $\text{u.c.d}\{a(x), b(x)\}$  nos referiremos al máximo común divisor de  $a(x)$  y  $b(x)$  que es moníaco.

Así por ejemplo: si  $a(x)$  y  $b(x) \in \mathbb{Z}_5[x]$  y  $3x^2 + * + 1$  es un máximo común divisor de ambos, entonces también lo son:  $x^2 + 2x + 2$ ,  $4x^2 + 3x + 3$ ,  $2x^2 + 4x + 4$  y  $\text{u.c.d}\{a(x), b(x)\} = x^2 + 2x + 2$ .

Sea  $a(x), b(x) \in K$ . Un polinomio  $u(x) \in K[x]$  diremos que es un mínimo común múltiplo de  $a(x)$  y  $b(x)$  si verifica lo siguiente:

- 1)  $a(x) | u(x)$  y  $b(x) | u(x)$
- 2) Si  $a(x) | c(x)$  y  $b(x) | c(x)$  entonces  $u(x) | c(x)$

NOTA: Similar a la anterior

#### • Teorema:

Si  $a(x) = u \cdot P_1^{\alpha_1}(x) \cdots P_r^{\alpha_r}(x)$  y  $b(x) = v \cdot P_1^{\beta_1}(x) \cdots P_r^{\beta_r}(x)$  con  $u, v \in K[x] - \{0\}$ ,  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$  y  $P_i(x), \dots, P_r(x)$  polinomios moníacos e irreducibles, entonces:

$$1) \text{u.c.d}\{a(x), b(x)\} = P_1(x)^{\min\{\alpha_1, \beta_1\}} \cdots P_r(x)^{\min\{\alpha_r, \beta_r\}}$$

$$2) \text{u.c.m}\{a(x), b(x)\} = P_1(x)^{\max\{\alpha_1, \beta_1\}} \cdots P_r(x)^{\max\{\alpha_r, \beta_r\}}$$

#### Ejercicio:

Dados los polinomios  $a(x) = (x+1)(2x+3)$  y  $b(x) = (x+2)(4x+1)$

de  $\mathbb{Z}_5[x]$ , calcular el  $\text{u.c.d}\{a(x), b(x)\}$  y

$\text{u.c.m}\{a(x), b(x)\}$

Solución al ejercicio anterior:

$$a(x) = (x+1)(2x+3) \quad y \quad b(x) = (x+2)(4x+1) \quad \text{de } \mathbb{Z}_5[x]$$

$$a(x) = (x+1)2 \cdot 3(2x+3) = 2(x+1)(x+4)$$

$$b(x) = (x+2)4 \cdot 4(4x+1) = 4(x+2)(x+4)$$

$$\text{u.c.d}\{a(x), b(x)\} = x+4$$

$$\text{u.c.m}\{a(x), b(x)\} = (x+1)(x+2)(x+4)$$

• Propiedad de la división:

Si  $a(x), b(x) \in K[x]$  y  $b(x) \neq 0$  entonces existen únicos únicos  $q(x), r(x) \in K[x]$  tales que  $a(x) = q(x)b(x) + r(x)$  con  $\text{gr}(r(x)) < \text{gr}(b(x))$

A  $q(x)$  y  $r(x)$  los llamaremos el cociente y el resto de dividir  $a(x)$  entre  $b(x)$ , y lo denotaremos  $a(x) \text{ div } b(x)$  y  $a(x) \text{ mod } b(x)$ .

Ejercicio:

Calcular el cociente y el resto de dividir  $3x^3 + 4x^2 + 2x + 3$  entre  $2x+4$  en  $\mathbb{Z}_5[x]$

$$\begin{array}{r} 3x^3 + 4x^2 + 2x + 3 \\ 2x^3 + 4x^2 \\ \hline 0 \quad 3x^2 + 2x + 3 \\ 2x^2 + 4x \\ \hline 0 \quad x^2 + 3 \\ 4x + 3 \\ \hline 0 \quad 1 \end{array} \rightarrow \begin{array}{l} \frac{2x+4}{4x^2+4x+3} \rightarrow q(x) \\ r(x) \end{array}$$

## • Algoritmo de Euclides

Entrada:  $a(x), b(x) \in \mathbb{K}[x] - \{0\}$  (distintos de cero)

Salida: un m.c.d. de  $a(x)$  y  $b(x)$ .

$$(a_0(x), a_1(x)) = (a(x), b(x))$$

Mientras  $a_i(x) \neq 0$

$$(a_0(x), a_1(x)) = (a_i(x), a_0(x) \text{ mod } a_1(x))$$

Devuelve  $a_0(x)$ .

NOTA: Si  $d(x)$  es un m.c.d. de  $a(x)$  y  $b(x)$ , entonces

$(a(x)b(x)) \text{ mod } d(x) = 0$ , y además  $(a(x)b(x)) \text{ div } d(x)$  es un m.c.m. de  $a(x)$  y  $b(x)$

Ejercicio:

$$\text{Sea } a(x) = x^4 + x + 1 \text{ y } b(x) = x^2 + 2x + 3 \in \mathbb{Z}_5[x]$$

Calcular m.c.d.  $\{a(x), b(x)\}$  y m.c.m.  $\{a(x), b(x)\}$ .

$$(a(x), b(x)) = (x^4 + x + 1, x^2 + 2x + 3) = (x^2 + 2x + 3, 3) = (3, 0)$$

Por el alg. de Euclides, 3 es un m.c.d de  $a(x), b(x)$ , ahora bien, sabemos entonces que  $1 \cdot 3, 2 \cdot 3, 3 \cdot 3$  y  $4 \cdot 3$  también son m.c.d de  $a(x)$  y  $b(x)$ .

El único es  $2 \cdot 3 = 1$ .

Por lo tanto  $\rightarrow$  m.c.d  $\{a(x), b(x)\} = 1$ .

Como  $a(x) \neq 0$  ( $a(x) \text{ div } 1$ ) es único;

$$\text{m.c.m. } \{a(x), b(x)\} = a(x) \cdot b(x)$$

$$\begin{array}{r} x^4 + x + 1 \\ 4x^4 + 3x^3 + 2x^2 \\ \hline 3x^3 + 2x^2 + x + 1 \\ 2x^2 + 4x^2 + x \\ \hline x^2 + 2x + 1 \\ 4x^2 + 3x + 2 \\ \hline 1 \end{array}$$

Sea  $a(x) = a_0 + a_1 x + \dots + a_n x^n \in K[x]$ . Un elemento  $\alpha \in K$  diremos que es una raíz del polinomio  $a(x)$  si  $a(\alpha) = a_0 + a_1 \alpha + \dots + a_n \alpha^n = 0$

Ejemplo:

Sea  $a(x) = x^3 + 2x^2 + x + 2 \in \mathbb{Z}_5[x]$

$$\begin{array}{lll} a(0) = 2 & a(2) = 0 & a(4) = 2 \\ a(1) = 1 & a(3) = 0 & \end{array}$$

$$\text{Raíces} = \{2, 3\}$$

### • Teorema del factor.

Sea  $a(x) \in K[x]$  y  $\alpha \in K$ , entonces  $\alpha$  es una raíz de  $a(x)$  si y sólo si  $x - \alpha \mid a(x)$

→ Corolario:

Un polinomio  $a(x) \in K[x]$  es múltiplo de un polinomio de grado 1 si y sólo si el polinomio tiene una raíz.

→ Corolario:

Un polinomio de grado 2 o de grado 3 es irreducible si y sólo si no tiene raíces.

Ejercicio:

Estudiar la irreducibilidad de los siguientes polinomios en  $\mathbb{Z}_3$ :

1)  $2x+1 \rightarrow$  irreducible, ya que, tiene grado 1.

2)  $x^2+x+1 \rightarrow$  reducible, ya que tiene raíz

3)  $x^2+x+2 \rightarrow$  irreducible, ya que no tiene raíces y es de grado 2

4)  $x^3+x+1 \rightarrow$  irreducible, ya que no tiene raíces y es de grado 3

5)  $x^4+x+1 \rightarrow$  reducible, ya que tiene una raíz y por tanto es producto de un polinomio de grado 1 y de grado 3.

6)  $x^4+x+2 \rightarrow$  No sabemos todavía responder a este tipo de polinomios.

# PRÁCTICAS 31/11/15

1. Calcula el cociente y el resto de dividir  $2x^4 + 3x^3 + x^2 + 6x + 1$  entre  $3x^2 + 1$  en  $\mathbb{Z}_7[x]$  y en  $\mathbb{Z}_{10}[x]$ .

En  $\mathbb{Z}_7$ :

$$\begin{array}{r} 2x^4 + 3x^3 + x^2 + 6x + 1 \\ 5x^4 \quad 4x^2 \\ \hline \end{array}$$

$$\begin{array}{r} | 3x^2 + 1 \\ 3x^2 + 8x + 4 \\ \hline \end{array}$$

$$\begin{array}{r} 3x^3 + 5x^2 + 6x + 1 \\ 4x^3 \quad 6x \\ \hline 9x^2 + 5x + 1 \\ 2x^2 \quad 3 \\ \hline 0 \quad 5x + 4 \end{array}$$

$$\begin{array}{l} \text{COCIENTE} \rightarrow 3x^2 + x + 4 \\ \text{RESTO} \rightarrow 5x + 4 \end{array}$$

En  $\mathbb{Z}_{10}$ :

$$\begin{array}{r} 2x^4 + 3x^3 + x^2 + 6x + 1 \\ 8x^4 \quad 6x^2 \\ \hline 3x^3 + 7x^2 + 6x + 1 \\ 7x^3 \quad 9x \\ \hline 7x^2 + 5x + 1 \\ 3x^2 \quad 1 \\ \hline 5x + 2 \end{array}$$

$$\begin{array}{l} \text{COCIENTE} \rightarrow 4x^2 + x + 9 \\ \text{RESTO} \rightarrow 5x + 2 \end{array}$$

2. Sean  $p(x) = x^4 + 2x^2 + 2x + 1$ ,  $q(x) = x^3 + 2x^2 + x + 2$  polinomios en  $\mathbb{Z}_3[x]$

Sean  $r(x) = p(x) \bmod q(x)$  y  $s(x) = q(x) \bmod r(x)$

a) - Calcula todos los divisores de  $p(x)$  (hay 8, 4 de ellos unitarios)  
de  $q(x)$  (hay 8), de  $r(x)$  (hay 6) y de  $s(x)$  (hay 4)

b) - Calcula todos los divisores comunes de  $p(x)$  y  $q(x)$ ;  
 $q(x)$  y  $r(x)$ ;  $r(x)$  y  $s(x)$

c) - Calcula el mínimo común múltiplo de  $p(x)$  y  $q(x)$ .

1º Vamos a calcular  $r(x) = p(x) \bmod q(x)$  y  $s(x) = q(x) \bmod r(x)$

$$\begin{array}{r} r(x) : \quad x^4 + 2x^2 + 2x + 1 \quad | x^3 + 2x^2 + x + 2 \\ \underline{2x^4 + x^3 + 2x^2 + x} \quad x+1 \\ x^3 + 2x^2 + x + 1 \\ \underline{2x^3 + x^2 + 2x + 1} \\ 2x^2 + 2 \rightarrow 2x^2 + 2x + 2 \Rightarrow r(x). \end{array}$$

$$\begin{array}{r} s(x) : \quad x^3 + 2x^2 + x + 2 \quad | 2x^2 + 2x + 2 \\ \underline{2x^3 + 2x^2 + 2x} \quad 2x \\ x^2 + 2 \\ \cancel{x^2 + 2} \\ s(x) = 2x + 1 \quad \cancel{s(x)} = \cancel{2x + 2} \end{array}$$

a) Divisores de  $p(x)$

Las raíces pueden ser 0, 1, 2.

$$p(0) = 1 \rightarrow \text{No es raíz}$$

$$p(1) = 0 \rightarrow \text{es raíz} \rightarrow x+1 \text{ es divisor de } p(x).$$

$$p(2) = 1 \rightarrow \text{No es raíz}$$

Dividimos  $p(x)$  entre  $x+1 \rightarrow x^3 + x^2 + 2 = p'(x)$

$$p'(1) = 1 \rightarrow 1 \text{ no es raíz de } x^3 + x^2 + 2$$

Sabemos que  $p(x) = (x+1) p'(x)$

$p'(x)$  no tiene divisores de grado 1  $\Rightarrow p'(x)$  es irreducible

Porque  $\exists p'(x) = a(x) \cdot b(x)$ , donde  $\text{gr}(a(x)), \text{gr}(b(x)) \geq 1$

$$\text{Entonces } \text{gr}(a(x)) + \text{gr}(b(x)) = 3$$

Por lo tanto, los divisores son

$$\{1, 2, x+1, 2(x+1), x^3 + x^2 + 2, 2(x^3 + x^2 + 2), x^4 + 2x^2 + 2x + 1, 2(x^4 + 2x^2 + 2x + 1)\}$$

• Teorema:

Sea  $a(x) \in K[x]$ :

- 1) Si el grado de  $a(x) \geq 2$  y  $a(x)$  tiene una raíz, entonces  $a(x)$  es reducible.
- 2) Si el grado de  $a(x)$  es 2 o 3, entonces  $a(x)$  es irreducible si y solamente si no tiene raíces.
- 3) Si el grado de  $a(x)$  es 4 o 5 entonces  $a(x)$  es irreducible si y solamente si no tiene raíces y además ningún polinomio monóico e irreducible de grado 2 lo divide.
- 4) Si  $a(x)$  tiene grado 6 o 7, entonces  $a(x)$  es irreducible si y solamente si no tiene raíces y además no existe ningún polinomio monóico e irreducible de grado 2 o 3 que lo divida.

Ejemplo:

Es irreducible el polinomio  $x^4 + x^2 + 2 \in \mathbb{Z}_3[x]$ ?

El polinomio NO tiene raíces.

Polinomios monóicos de grado 2:

$$x^2 + ax + b \rightarrow \text{En } \mathbb{Z}_3 \text{ hay 9 diferentes.}$$

$$\{x^2, x^2+1, x^2+2, x^2+x, x^2+x+1, x^2+x+2, x^2+2x, x^2+2x+1, x^2+2x+2\}$$

Tachamos los reducibles

Los polinomios monóicos e irreducibles grado 2 = { $x^2+1, x^2+x+2, x^2+2x+2$ }

Ahora dividimos nuestro polinomio entre los tres hallados.

$$\begin{array}{r} x^4 + x^2 + 2 \\ \hline 2x^4 + 2x^2 \\ \hline 2 \end{array} \quad \begin{array}{r} x^4 + x^2 + 2 \\ \hline x^2 \\ \hline x^2 + x + 2 \\ \hline 2x^3 + 2x^2 + 2 \\ \hline x^3 + x^2 + 2x \\ \hline 2x + 2 \end{array}$$

$$\begin{array}{r} x^4 + x^2 + 2 \\ \hline 2x^4 + x^3 + x^2 \\ \hline x^3 + 2x^2 + 2 \\ \hline 2x^3 + x^2 + x \\ \hline x + 2 \end{array}$$

Como no hay ningún polinomio monóico de grado 2 que lo divida, el polinomio  $x^4 + x^2 + 2$  es IRREDUCIBLE.

## Ejemplos:

1) ¿Es irreducible el polinomio  $x^5 + x^4 + x^3 + 2 \in \mathbb{Z}_3[x]$ ?

- El polinomio NO tiene raíces.

- Tenemos que comprobar que ningún monómico irreducible de grado 2 lo divide.

Los polinomios monómicos e irreducibles de grado 2 de  $\mathbb{Z}_3[x]$

son  $\{x^2+1, x^2+x+2, x^2+2x+2\}$  (Sacado ej anterior)

$$\begin{array}{r} x^5 + x^4 + x^3 + 2 \\ 2x^5 \quad 2x^3 \\ \hline x^4 + 2 \\ 2x^4 + 2x^2 \\ \hline 2x^2 + 2 \\ x^2 + 1 \\ \hline 10 \end{array}$$

Como el resto da cero,

el polinomio  $x^5 + x^4 + x^3 + 2 \in \mathbb{Z}_3[x]$   
es REDUCIBLE.

## • Teorema del resto:

Sea  $a(x) \in K[x]$  y  $\alpha \in K$ , entonces  $a(x) \bmod x - \alpha = a(\alpha)$

Ejercicio:

Calcular en  $\mathbb{Z}_5[x]$  el resto de dividir  $x^{1002} + x^{77} + 1$  entre  $x + 3$

Nos piden  $(x^{1002} + x^{77} + 1) \bmod (x+3)$

$$(x+3) = (x-2) \text{ en } \mathbb{Z}_5$$

$$(x^{1002} + x^{77} + 1) \bmod (x-2) = 2^{1002} + 2^{77} + 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 3$$

$$2^4 = 1$$

$$77 \quad |4 \quad \Rightarrow 77 = 4 \cdot 19 + 1$$

$$37 \quad |19 \quad 2^{77} = (2^4)^{19} + 2 = 2$$

$$\text{Por lo tanto } 2^{1002} + 2^{77} + 1 = 4 + 2 + 1 = 2$$

## \*Multiplicidad de una raíz

Si  $\alpha$  es una raíz de  $a(x) \in K[x]$ , entonces aplicando reiteradamente el teorema del factor obtenemos que  $a(x) = (x - \alpha)^m \cdot b(x)$ . Con  $m \in \mathbb{N} - \{0\}$ ,  $b(x) \in K[x]$  y  $b(\alpha) \neq 0$ .

Al número  $m$  lo llamaremos "la multiplicidad de la raíz  $\alpha$ ", si  $m=1$  diremos que  $\alpha$  es una raíz simple y si  $m \geq 2$ , diremos que  $\alpha$  es una raíz múltiple.

### • Proposición:

Si  $a(x) \in K[x] - \{0\}$  entonces la suma de las multiplicidades de las raíces de  $a(x)$  es  $\leq$  que el grado de  $a(x)$ .

- Ejercicio:

Calcular las raíces y sus multiplicidades del polinomio  $x^3 + 2x + 3 \in \mathbb{Z}_5[x]$

Raíces =  $\{2, 4\}$ , ahora calcularemos las multiplicidades de cada una:

- Raíz 2: 
$$\begin{array}{r} x^3 + 2x + 3 \\ \hline x+3 \end{array} \Rightarrow x^3 + 2x + 3 = (x-2)(x^2 + 2x + 1)$$
  
$$\begin{array}{r} 4x^3 + 2x^2 \\ \hline 2x^2 + 2x + 3 \end{array}$$
  
$$\begin{array}{r} 3x^2 + 4x \\ \hline x + 3 \end{array}$$
  
$$\begin{array}{r} 4x + 2 \\ \hline 0 \end{array}$$

No se anula en 2  
Por lo tanto,  
la multiplicidad de la raíz 2  
vale 1.

- Raíz 4: 
$$\begin{array}{r} x^3 + 2x + 3 \\ \hline x+1 \end{array} \Rightarrow x^3 + 2x + 3 = (x-4)(x^2 + 4x + 3)$$
  
$$\begin{array}{r} 4x^3 + 4x^2 \\ \hline 4x^2 + 4x \end{array}$$
  
$$\begin{array}{r} 3x^2 + 3 \\ \hline 2x + 2 \end{array}$$
  
$$\begin{array}{r} 10 \\ \hline 0 \end{array}$$

Se anula en 4  
(seguimos dividiendo)  
$$\begin{array}{r} x^2 + 2x + 3 \\ \hline x+3 \end{array}$$
  
$$\begin{array}{r} x^2 + x \\ \hline 3x + 3 \end{array}$$
  
$$\begin{array}{r} 2x + 2 \\ \hline 10 \end{array}$$

$\Rightarrow x^3 + 2x + 3 = (x-4)(x-4)(x+3)$   
 $= (x-4)^2(x+3)$   
No se anula en 4  
Por lo tanto,

la multiplicidad de la raíz 4  
vale 2.

• Teorema:

Sea  $\alpha$  una raíz de  $a(x) \in K[x]$  entonces  $\alpha$ , una raíz múltiple si y solamente si  $\alpha$  es también raíz de  $a'(x)$  (donde  $a'(x)$  es la derivada de  $a(x)$ )

Ejercicio:

1) Calcular las raíces múltiples del polinomio

$$a(x) = x^3 + 4x^2 + 5x + 2 \in \mathbb{R}[x]$$

$$a'(x) = 3x^2 + 8x + 5$$

Vamos a ver donde se anula la derivada.

$$x = \frac{-8 \pm \sqrt{64-60}}{6} = \frac{-8 \pm 2}{6} \quad \begin{cases} x = -1 \\ x = -\frac{5}{3} \end{cases}$$

Las raíces de la derivada son }  $-1, -\frac{5}{3}$

$a(-1) = 0 \rightarrow$  Raíz múltiple

$$a\left(-\frac{5}{3}\right) = \frac{-125}{27} + \frac{100}{9} - \frac{27}{3} + 2 \neq 0$$

La única raíz múltiple de  $x^3 + 4x^2 + 5x + 2$  es  $-1$

2) Demuestra que el polinomio  $x^{70}-1 \in \mathbb{R}[x]$  no tiene raíces múltiples.

$$a'(x) = 70x^{69} \rightarrow$$
 sólo se anula en cero.

El 0 es la única raíz de la derivada, además,

$a(0) = -1$ , por tanto,  $a(x)$  no tiene raíces múltiples.

→ Corolario:

Sea  $a(x) \in K[x]$  y  $\alpha \in K$  entonces  $\alpha$  es una raíz de multiplicidad  $m$  del polinomio  $a(x)$  si y solamente si  $a(\alpha) = 0, a'(\alpha) = 0, a''(\alpha) = 0, \dots, a^{m-1}(\alpha) = 0$  y  $a^m(\alpha) \neq 0$

### Ejercicios:

1) Calcula las raíces y sus multiplicidades del polinomio

$$a(x) = x^3 + 2x + 3 \in \mathbb{Z}_5[x]$$

$$\text{Raíces} = \{2, 4\}$$

Vamos a calcular la multiplicidad de la raíz 2.

$$a'(x) = 3x^2 + 2$$

El 2 es una raíz de multiplicidad 1

$$a'(2) = 4 \neq 0$$

Vamos a calcular la multiplicidad de la raíz 2

$$a''(x) = 6x$$

El 4 es una raíz de multiplicidad 2.

$$a''(4) = 4 \neq 0$$

→ Corolario:

Sea  $a(x) \in K[x] \setminus \{0\}$  entonces las raíces múltiples de  $a(x)$  son justamente las raíces del polinomio m.c.d.  $\{a(x), a'(x)\}$ .

### Ejercicio:

1) Calcular las raíces múltiples del polinomio

$$a(x) = x^4 - 6x^3 + 13x^2 + 12x + 4 \in \mathbb{R}[x]$$

$$(a_0(x), a_1(x)) = (x^4 - 6x^3 + 13x^2 + 12x + 4, 4x^3 + 18x^2 + 26x + 12) =$$

$$= (4x^3 + 18x^2 + 26x + 12, -\frac{1}{4}x^2 - \frac{3}{4}x - \frac{1}{2}) \cong$$

$$\cong (2x^3 + 9x^2 + 12x + 6, x^2 + 3x + 2) =$$

$$= (\underline{x^2 + 3x + 2}, 0)$$

$$x = \frac{-3 \pm \sqrt{9-8}}{2} = \frac{-3 \pm 1}{2} \quad \begin{cases} x = -2 \\ x = -1 \end{cases}$$

5) Calcular la multiplicidad de lo anterior  
 La multiplicidad es 2.  
 Ver explicación  
 en Teorema.

Tiene que ser  $\leq$  grado polinomio.

### \* Corpos finitos

Sea  $m(x)$  un polinomio  $\in K[x] \setminus \{0\}$ , denotaremos por

$$K[x]_{m(x)} = \{a(x) \in K[x] \text{ tq } \text{gr}(a(x)) < \text{gr}(m(x))\}$$

El conjunto anterior es un anillo conmutativo con las siguientes operaciones:

$$a(x) \oplus b(x) = (a(x) + b(x)) \text{ mod } m(x)$$

$$a(x) \odot b(x) = (a(x) \cdot b(x)) \text{ mod } m(x)$$

Ejemplo:

Calcular  $\mathbb{Z}_3[x]_{x^2+x+1}$

$$\mathbb{Z}_3[x]_{x^2+x+1} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Ahora, calcula  $(x+1) \odot (x+2)$

$$(x+1) \odot (x+2) = (x^2 + 2) \text{ mod } (x^2 + x + 1) = 2x + 1$$

$$= 2x + 2 - 2x = 2$$

$$(0, 1, 2, x, x+1, x+2)$$

• Proposición:

Sea  $a(x) \in K[x]_{m(x)}$  entonces  $a(x)$  es una unidad si y solo si  $\text{u.c.d.}\{a(x), m(x)\} = 1$ .

Ejercicio:

¿Es  $x+3$  una unidad de  $\mathbb{Z}_5[x]_{x^2+x+1}$ ?

$$(a_0(x), a_1(x)) = (x^2 + x + 1, x + 3) = (x + 3, 2) = (2, 0)$$

2 es un máximo común divisor,

por lo tanto:  $2 \cdot 1, 2 \cdot 2, 2 \cdot 3, 2 \cdot 4$

son también máximos comunes divisores

$$2 \cdot 3 = 1 \text{ (en } \mathbb{Z}_5\text{)}.$$

$$\text{u.c.d.}\{x^2+x+1, x+3\} = 1$$

Por lo tanto  $x+3$  es una unidad.

→ Corolario:

$K[x]_{m(x)}$  es un cuerpo  $\Leftrightarrow m(x)$  es irreducible.

• Proposición:

El cardinal de un cuerpo finito es siempre la potencia de un no primo. Además, si  $p$  es un no primo positivo y  $m(x)$  pertenece a  $\mathbb{Z}_p[x]$ , entonces el cardinal

$$\text{de } \mathbb{Z}_p[x]_{m(x)} \text{ es } p^{\text{gr}(m(x))}$$

Ejercicio:

1)  $\mathbb{Z}_5$  → conti 5 elementos

2)  $\mathbb{Z}_3[x]_{x^2+x+1}$  es un anillo conmutativo con 9 elementos pero no es un cuerpo porque  $m(x)$  no es irreducible.

3) Sin embargo:  $\mathbb{Z}_3[x]_{x^2+1}$

3) Dar un cuerpo con 10 elementos.

No hay cuerpo de 10 elementos porque

10 NO es la potencia de un nº primo.

4) Dar un cuerpo con 16 elementos:

$\mathbb{Z}_2[x]_{x^4+x+1}$ , Vamos a ver que es cierto calculando si  $x^4+x+1$  es irreducible:

1º Raíces: no tiene

2º Polinomios monicos de grado 2.

$$\{x^2, x^3+1, x^2+x, x^2+x+1\}$$

Tachamos los 3º irreducibles

$x^2+x+1$  es el único polinomio monico irreducible de grado 2 de  $\mathbb{Z}_2[x]$

$$\begin{array}{r} x^4 + x + 1 \\ \underline{-} x^2 - x \\ \hline 1 \end{array}$$

Resto 1 por lo tanto

$x^4+x+1$  es irreducible.

• Proposición:

Sea  $a(x) \in K[x]_{m(x)}$ , si  $a(x) u(x) + m(x) v(x) = 1$   
entonces  $s(x) \bmod m(x)$  es el inverso para el producto  
de  $a(x)$ .

\* Algoritmo extendido de Euclides

Entrada:  $a(x), b(x) \in K[x] \setminus \{0\}$

Salida:  $s(x), t(x), d(x) \in K[x]$  tq  $d(x)$  es un  
m.c.d de  $a(x)$  y  $b(x)$ , y  $a(x)s(x) + b(x)t(x) = d(x)$ .

$$(a_0(x), a_1(x)) = (a(x), b(x))$$

$$(s_0(x), s_1(x)) = (1, 0)$$

$$(t_0(x), t_1(x)) = (0, 1)$$

Mientras  $a_i(x) \neq 0$

$$q(x) = a_0(x) \text{ div } a_i(x)$$

$$(a_0(x), a_i(x)) = (a_i(x), a_0(x) - a_i(x) \cdot q(x))$$

$$(s_0(x), s_i(x)) = (s_i(x), s_0(x) - s_i(x) \cdot q(x))$$

$$(t_0(x), t_i(x)) = (t_i(x), t_0(x) - t_i(x) \cdot q(x))$$

Devuelve  $d(x) = a_0(x)$ ,  $s(x) = s_0(x)$  y  $t(x) = t_0(x)$

Ejercicio: Calcular el inverso para el producto de  $x+3$   
en  $\mathbb{Z}_5[x]_{x^2+x+1}$

Por un ejercicio anterior, sabemos que m.c.d  $\{x^2+x+1, x+3\} = 1$   
por tanto existe  $(x+3)^{-1}$

$$(a_0(x), a_1(x)) = (x^2+x+1, x+3) = (x+3, 2) = (2, 0)$$

$$(s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, -)$$

$$(t_0(x), t_1(x)) = (0, 1) = (1, 4x+2) = (4x+2, -)$$

$$(x^2+x+1) \cdot 1 + (x+3)(4x+2) = 2 \quad \text{multiplico por 3}$$

$$(x^2+x+1) \cdot 3 + (x+3)(2x+1) = 1$$

$$(x+3)^{-1} = (2x+1) \bmod (x^2+x+1) = 2x+1$$

→ Comprobación: Si el ejercicio está bien,

$$(x+3)(2x+1) = 1$$

$$\Rightarrow (x+3)(2x+1) \bmod (x^2+x+1) =$$

$$(2x^2+2x+3) \bmod (x^2+x+1) = \underline{\underline{1}}$$

# PRACTICAS 10/11/15

Continuación ejercicio anterior sesión.

$$p(x) = x^4 + 2x^2 + 2x + 1$$

$$r(x) = 2x^4 + 2x^2 + 2$$

$$q(x) = x^3 + 2x^2 + x + 2$$

$$s(x) = \frac{\text{_____}}{2x+1}$$

en  $\mathbb{Z}_3[x]$

a) Ya tenemos los divisores de  $p(x)$ , vamos con los demás.

• Divisores de  $q(x)$ :

¿Tiene raíces?

$$q(0) = 2$$

$$q(1) = 0 \rightarrow x-1 = x+2 \text{ divide a } q(x).$$

$$q(2) = 2$$

Dividimos  $q(x)$  entre  $x+2 \rightarrow$  cociente  $x^2+1$

$$\Rightarrow q(x) = (x^2+1)(x+2)$$

Volvemos a comprobar si 1 es raíz de  $q(x)$ :

$$q(1) \neq 0 \rightarrow x^2+1 \text{ es irreducible.}$$

Por lo tanto, los divisores de  $q(x)$  =

$$\{1, 2, x+2, 2(x+2) = 2x+1, x^2+1, 2x^2+2, \dots\}$$

Grado 0: 1, 2

Grado 1:  $x+2, 2(x+2) = 2x+1$

Grado 2:  $x^2+1, 2(x^2+1) = 2x^2+2$

Grado 3:  $q(x), 2q(x)$

• Divisores de  $r(x)$

1 es la única raíz.  $\Rightarrow x+2$  divide a  $r(x) \Rightarrow$   
1 es raíz doble

$$r(x) = 2(x+2)^2$$

Por lo tanto sus divisores son:

Grado 0: 1, 2

Grado 1:  $x+2, 2x+1$

Grado 2:  $r(x), 2r(x)$

• Divisores de  $s(x)$ :

Grado 0: 1, 2

Grado 1:  $s(x), 2s(x)$

b) Calcula todos los divisores comunes de  $p(x)$  y  $q(x)$ ;  $q(x)$  y  $r(x)$ ;  $r(x)$  y  $s(x)$ .

c) Divisores comunes  $p(x)$  y  $q(x)$

Grado 0: 1, 2

1:  $x+2, 2x+1$

d) Divisores comunes  $q(x)$  y  $r(x)$

Grado 0: 1, 2

1:  $x+2, 2x+1$

e) Divisores comunes  $r(x)$  y  $s(x)$

Grado 0: 1, 2

1:  $x+2, 2x+1$

Ejercicio: calcular el resto de dividir en  $\mathbb{Z}_7[x]$

$$1. x^7 + x^2 + 1 \text{ entre } x-1$$

$$2. x^n + 1 \text{ entre } x-1$$

$$\begin{array}{r} x^7 + x^2 + 1 \\ \hline 6x^7 + 6x^6 \\ \hline 6x^6 + x^2 + 1 \\ \hline x^6 + 6x^5 \\ \hline 6x^5 + x^2 + 1 \\ \hline x^5 + 6x^4 \\ \hline 6x^4 + x^2 + 1 \\ \hline x^4 + 6x^3 \\ \hline 6x^3 + x^2 + 1 \\ \hline x^2 + 6x^1 \\ \hline \end{array}$$

$$\begin{array}{r} | x-1 \\ \hline x^6 + 6x^5 + 6x^4 + 6x^3 + 6x^2 \\ \hline \end{array}$$

Resto  $\rightarrow \cancel{3}$

$$x^n + 1 = q(x)(x-1) + r(x)$$

$$\cancel{x^n + 1} = \cancel{(x-1)}(x-1) + r(x)$$

Teorema del resto:

$$1^7 + 1^2 + 1 = 3$$

2) ~~Verificar que  $(x-1) + r(x)$  es un  $\mathbb{Z}_2[x]$~~

$x^n + 1$  entre  $x - 1$

$$a(x) \bmod (x - \alpha) = a(\alpha)$$

$$a(x) \in \mathbb{Z}_2[x], \alpha \in K$$

$$1^n + 1 = 1 + 1 = 2.$$

Ejercicio:

Sea  $A = \mathbb{Z}_2[x]_{x^3+1} \rightarrow$  n° elementos  $\mathbb{Z}_p[x]_{\text{gr}(x)} \rightarrow p^{\text{gr}(x)}$

1. Calcular las unidades de  $A$  y dar, en su caso, su inverso.  
2. ¿Es la suma de dos unidades una unidad? y el producto?

2. Calcula los divisores ~~distintos~~ de cero. Para cada uno de ellos, encuentra un elemento no nulo de  $A$  al multiplicarlo por él da cero. ¿Es la suma de dos divisores de cero un divisor de cero? y el producto?

1) Posibles raíces:  $0, 1, x, x+1, x^2, x^2+1, \cancel{x^3+1}, x^2+x+1, x^2+x$

Unidades:  $\{1, x, x^2\}$

Inverso de 1: 1

$$x : x^2 \text{ porque } x \cdot x^2 = x^3 \bmod x^3 + 1 = 1$$

$$x^2 : x$$

La suma de dos unidades no tiene por qué ser una unidad: Ejemplo  $\rightarrow x$  y 1 son unidades pero  $x+1$  no lo es.

El producto de dos unidades es siempre una unidad.

Demostración:

Si  $P(x), Q(x)$  son unidades en  $K[x]$ , entonces,

si  $P'(x)$  es el inverso de  $P(x)$  y si  $Q'(x)$  es el inverso de  $Q(x)$ , entonces  $P'(x) \cdot Q'(x)$  es el inverso de  $P(x) \cdot Q(x)$ .

$$P(x) \cdot Q(x) \cdot Q'(x) \cdot P'(x) = P(x) \cdot P'(x) = 1$$

2)  $(x+1)(x^2+x+1) = x^3+1 \bmod x^3+1 = 0$

Z2

Divisores de cero:  $\{0, x+1, x^2+x, x^2+1, x^2+x+1\}$

• Para  $x^2+x$ , se cumple que  $(x^2+x)(x^2+x+1) = x(x+1)(x^2+x+1)$   
 $= x(x^3+1) \bmod x^3+1 = 0$

• Para  $x^2+1$ ,  $\rightarrow (x^2+1)(x^2+x+1) = (x+1)^2(x^2+x+1)$   
 $= (x+1)(x^3+1) \bmod x^3+1 = 0$

• Para  $x^2+x+1$ ,  $\rightarrow (x^2+x+1)(x+1)$

La suma de dos divisores de cero no tiene  
que ser divisor de cero:  
 $x^2+x+1, x+1$  son divisores de cero pero  
 $x^2+x+1 + x+1 = x^2$  que es una  
unidad, y por tanto no es un divisor de cero.

El producto de dos divisores de cero NO es  
divisor de cero:

$x+1, x^2+x+1$  son divisores de cero:

pero  $(x+1)(x^2+x+1)$  NO es divisor de cero.

porque  $= 0$

## Ejercicios

1) Calcular la descomposición en irreducibles del polinomio

$$x^5 + x + 1 \in \mathbb{Z}_2[x]. \text{ ¿Es } \mathbb{Z}_2[x]_{x^5+x+1} \text{ un cuerpo?}$$

→ 1º Se buscan las posibles raíces, no tiene raíces.

→ 2º Buscar monóico de grado 2 que lo divida:

Por un ejercicio anterior, sabemos que  $x^2+x+1$  es el único polinomio monóico e irreducible de grado 2 de  $\mathbb{Z}_2[x]$

→ 3º Dividimos  $x^5+x+1$  entre  $x^2+x+1$ . Si el resto lo es distinto de cero, el polinomio  $x^5+x+1$  es irreducible.

$$\begin{array}{r} x^5 & & & & \\ \underline{x^5 + x^3 + x^3} & & & & \\ & x^3 & + x & + 1 & | x^2 + x + 1 \\ & \underline{x^3 + x^2 + x^2} & & & \\ & & x^2 & + x & + 1 \\ & & \underline{x^2 + x + 1} & & \\ & & & & 0 \end{array}$$

Por lo tanto:

$$(x^5 + x + 1) = (x^2 + x + 1)(x^3 + x + 1)$$

IRREDUCIBLE IRREDUCIBLE

DECOMPOSICIÓN EN  
IRREDUCIBLES.

→ ¿Es  $\mathbb{Z}_2[x]_{x^5+x+1}$  un cuerpo?

No es cuerpo ya que  $x^5+x+1$  no es irreducible,  $\mathbb{Z}_2[x]_{x^5+x+1}$  es un anillo conmutativo y tiene cardinal  $2^5 = 32$ .

→ ¿Es  $x+1$  una unidad de ese anillo?

$$\text{u.c.d}\{x^5+x+1, x+1\} = 1$$

$x+1$  es una unidad ya que  $\text{u.c.d}\{x^5+x+1, x+1\} = 1$ .

lo hemos visto rápidamente, observando las descomposiciones en irreducibles.

→ Calcular  $(x+1)^{-1}$

Aplicamos Algor. Ext. Euclides.

$$\begin{array}{l} q(x) = x^4 + x^3 + x^2 + x \\ (a_0(x), a_1(x)) = (x^5 + x + 1, x + 1) = (x + 1, 1) = (1, 0) \\ (s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, -) \\ (t_0(x), t_1(x)) = (0, 1) = (1, x^4 + x^3 + x^2 + x) = (x^4 + x^3 + x^2 + x, -) \end{array}$$

$$(x^5 + x + 1) \cdot 1 + (x + 1)(x^4 + x^3 + x^2 + x) = 1$$

$$(x + 1)^{-1} = (x^4 + x^3 + x^2 + x) \bmod (x^5 + x + 1) = x^4 + x^3 + x^2 + x$$

→ ¿Tiene  $\mathbb{Z}_2[x]_{x^5+x+1}$  divisores de cero? En caso afirmativo, da uno.

Como  $(x^2 + x + 1) \circ (x^3 + x^2 + 1)$  vale cero

[NOTA: En  $K[x]$ , los divisores de cero son los elementos de  $K$  que no son cero ni unidad.]

2) Resuelve en  $\mathbb{Z}_3[x]_{x^2+x+2}$  la ecuación  $(2x+1)Y + x + 2 = 2x$ .

$$(2x+1)Y + x + 2 = 2x$$

$$(2x+1)Y = x + 1$$

$$Y = (2x+1)^{-1}(x+1)$$

Para calcular  $(2x+1)^{-1}$  aplicamos algoritmo ext. Euclides.

$$\begin{array}{l} q(x) = \\ (a_0(x), a_1(x)) = (x^2 + x + 2, 2x + 1) = (2x + 1, 1) = (1, 0) \\ (s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, -) \\ (t_0(x), t_1(x)) = (0, 1) = (1, x^2 + x + 2) = (x^2 + x + 2, -) \end{array}$$

$$\Leftrightarrow (x^2 + x + 2) \cdot 1 + (2x + 1)(x + 2) = 1$$

$$(2x+1)^{-1} = x + 2, \text{ Por lo tanto:}$$

$$Y = (x+2) \cdot (x+1) = (x^2 + 2) \bmod (x^2 + x + 2) = \underline{\underline{2x}}$$

3) ¿Existen cuerpos de cardinal 343? En caso afirmativo, da uno.

Un cardinal de un cuerpo es siempre la potencia de un primo, ademas  $\mathbb{Z}_p[x]_{m(x)}$  tiene  $p^{\text{gr}(m(x))}$  elementos.

Como  $343 = 7^3$ , entonces 343 es la potencia de un primo y por tanto, existen cuerpos de cardinal 343.

Vamos a dar ahora un ejemplo:

$\mathbb{Z}_7[x]$   $x^3 + x + 1$  es un cuerpo porque  $x^3 + x + 1$  es irreducible.

4) Calcula las raíces y sus multiplicidades del polinomio  $a(x) = x^4 + 3x^2 + 1 \in \mathbb{Z}_5[x]$ .

$$\text{Raíces} = \{1, 4\}$$

$$a'(x) = 4x^3 + 6x$$

$$a'(1) = 0$$

$$a''(x) = 12x^2 + 1$$

$a''(1) = 3 \neq 0 \rightarrow$  El 1 es raíz de multiplicidad 2

$$\overset{\text{es}}{a'(4)} = 0$$

$a''(4) = 3 \neq 0 \rightarrow$  El 4 es raíz de multiplicidad 2.

## Tema 4 → MATRICES CON COEFICIENTE EN UN CUERPO

Sean los conjuntos  
Sean la matriz  $I = \{1, 2, \dots, m\}$  y  $J = \{1, 2, \dots, n\}$ ,

una matriz de orden  $m \times n$  con coeficientes en un cuerpo  $K$   
es una aplicación  $A: I \times J \rightarrow K$   
 $(i, j) \rightarrow a_{ij}$

Normalmente a la aplicación  $A$  se le representa de la siguiente forma:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Y diremos que la matriz tiene  $m$  filas y  $n$  columnas.

Denotaremos así:  $M_{m \times n}(K)$  al conjunto formado por todas las matrices de orden  $m \times n$  y con coeficiente en  $K$ .

Ejemplo:  $M_{2 \times 3}(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right\}$

$\# M_{2 \times 3}(\mathbb{Z}_2) = 2^6 = 64 //$

### \* Suma de matrices

Si  $A, B \in M_{m \times n}(K)$ , entonces  $A + B \in M_{m \times n}(K)$ ,  
además el elemento que ocupa la posición  $(i, j)$  en la matriz  $A + B$  es  $a_{ij} + b_{ij}$ . donde  $a_{ij}$  y  $b_{ij}$  son los elementos que ocupan la posición  $(i, j)$  en las matrices  $A$  y  $B$  respectivamente.

#### • Proposición:

$M_{m \times n}(K)$  con la operación suma es un grupo ABELIANO (o commutativo), es decir, la operación suma de matrices es asociativa, commutativa, tiene elemento neutro y tiene elemento inverso.

Ejercicio:

$$\text{Sea } A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 1 \end{pmatrix} \text{ y } B = \begin{pmatrix} 3 & 4 & 3 \\ 2 & 3 & 2 \end{pmatrix} \in M_{2 \times 3}(\mathbb{Z}_5)$$

a) Calcular  $A+B$

$$A+B = \begin{pmatrix} 4 & 1 & 1 \\ 2 & 2 & 3 \end{pmatrix}$$

b) ¿Quién es el elemento neutro de  $M_{2 \times 3}(\mathbb{Z}_5)$ ?

La matriz nula  $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

c) ¿Quién es el inverso de  $A$ ?

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

### \* Producto de matrices

Si  $A \in M_{n \times m}(\mathbb{K})$  y  $B \in M_{m \times p}(\mathbb{K})$  entonces

$A \cdot B \in M_{n \times p}(\mathbb{K})$ . Además, si  $(a_{11}, a_{12}, \dots, a_{1m})$  es la

fila  $i$  de la matriz  $A$  y  $\begin{pmatrix} b_{1,j} \\ b_{2,j} \\ \vdots \\ b_{n,j} \end{pmatrix}$  es la columna

$j$  de la matriz  $B$  entonces, el elemento

que ocupa la posición  $(ij)$  en la matriz  $A \cdot B$  es

$$a_{11}b_{1,j} + a_{12}b_{2,j} + \dots + a_{1n}b_{n,j}$$

Ejemplo:

$$\text{Sea } A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix}_{2 \times 3} \text{ y } B = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \\ 3 & 2 & 3 & 1 \end{pmatrix}_{3 \times 4}, \in \mathbb{Z}_7$$

Calcular  $A \cdot B$

$$A \cdot B = \begin{pmatrix} 6 & 4 & 1 & 5 \\ 2 & 1 & 1 & 3 \end{pmatrix}$$

Una matriz de orden  $n \times n$  diremos que es una matriz cuadrada de orden  $n$

• Proposición:

$(M_{n \times n}[K], +, \cdot)$  es un anillo (no conmutativo), además el elemento neutro del producto es la matriz:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \rightarrow \text{MATRIZ IDENTIDAD de orden } n$$

la denotaremos  $I_n$

Ejercicio:

sea  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$  y  $B = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$  dos matrices con coeficientes en  $\mathbb{Q}$

Comprobar que  $A \cdot B \neq B \cdot A$ .

$$A \cdot B = \begin{pmatrix} 5 & 2 \\ 11 & 6 \end{pmatrix} \quad B \cdot A = \begin{pmatrix} 7 & 10 \\ 2 & 4 \end{pmatrix}$$

\* Determinantes

Dada una matriz cuadrada  $A$ , definimos el determinante de  $A$ , que lo denotaremos:  $|A|$  ó  $\det(A)$ :

$$|a_{11}| = a_{11}$$

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

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{23}a_{32}a_{11}$$

### Ejercicio:

Calcular los determinantes de las matrices

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$  y  $B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 2 & 3 & 2 \end{pmatrix}$  cuyos coeficientes están en  $\mathbb{Z}_5$ .

$$|A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 3$$

$$|B| = \begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 2 & 3 & 2 \end{vmatrix} = 4 + 1 + 4 - 2 - 4 - 2 = 1$$

Sea la matriz  $A \in M_{n \times m}(\mathbb{K})$

denotaremos por  $A_{ij}$  a la matriz que se obtiene a partir de la matriz  $A$  quitándole la fila  $i$  y la columna  $j$

Llamaremos adjunto del elemento  $a_{ij}$  a  $(-1)^{1+i} |A_{ij}|$   
y lo denotaremos  $\alpha_{ij}$

### \* Desarrollo de Laplace

Sea  $A$  una matriz cuadrada  $A \in M_{n \times n}(\mathbb{R})$

1) Desarrollarlo por la fila  $i$ :

$$|A| = a_{11}\alpha_{11} + a_{12}\alpha_{12} + \dots + a_{1n}\alpha_{1n}$$

2) Desarrollarlo por la columna  $j$ :

$$|A| = a_{1j}\alpha_{1j} + a_{2j}\alpha_{2j} + \dots + a_{nj}\alpha_{nj}$$

Ejemplo:

Calcular el siguiente determinante cuyos coeficientes están en  $\mathbb{Z}_7$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 0 & 1 & 3 \\ 3 & 4 & 1 & 1 \\ 2 & 0 & 3 & 2 \end{vmatrix} = 2(-1)^{1+2} \cdot \begin{vmatrix} 2 & 1 & 3 \\ 3 & 1 & 1 \\ 2 & 3 & 2 \end{vmatrix} + 0 + 4(-1)^{2+2} \cdot \begin{vmatrix} 1 & 3 & 4 \\ 2 & 1 & 3 \\ 2 & 3 & 2 \end{vmatrix} + 0 =$$
$$= 5(4+2+6-8-6-6) + 3 \cdot (2+1+3-8-9-12) =$$
$$= 5+3 = 1$$

$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$  Si  $A$  es una matriz de orden  $n \times n$   $[M_{n \times n}(K)]$

Entonces llamaremos matriz traspuesta de  $A$ , a:

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix} \in M_{m \times n}(K)$$

Una matriz cuadrada, diremos que es simétrica si coincide con su traspuesta.

## \* Propiedades de los determinantes

Sea  $A$  una matriz cuadrada,  $A \in M_{n \times n}(K)$ :

1) ~~tales que~~  $|A| = |A^t|$

2) Si intercambiamos dos filas (o dos columnas) de la matriz  $A$ , obtenemos una nueva matriz cuyo determinante es  $-|A|$

3) Si multiplicamos todos los elementos de una fila (o de una columna) de la matriz  $A$  por  $\alpha \in K$  obtenemos una nueva matriz cuyo determinante es  $\alpha \cdot |A|$

4) Si a una fila de la matriz  $A$  le sumamos otra fila multiplicada por un elemento de  $K$  entonces obtenemos una nueva matriz cuyo determinante coincide con el determinante de la matriz  $A$ . (Lo mismo ocurre si hacemos esta operación por columnas).

5) Si  $B \in M_{n \times n}(K)$  entonces, el determinante

$$|A \cdot B| = |A| \cdot |B|$$

Ejercicio:

Calcular el siguiente determinante cuyos coeficientes están en  $\mathbb{Z}_5$

$$\begin{vmatrix} 2 & 3 & 4 & 1 & 2 \\ 3 & 2 & 4 & 1 & 1 \\ 1 & 3 & 2 & 1 & 2 \\ 4 & 1 & 2 & 3 & 4 \\ 2 & 3 & 3 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 3 & 4 & 1 & 2 \\ 0 & 0 & 3 & 2 & 3 \\ 0 & 4 & 0 & 3 & 1 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 1 & 4 \end{vmatrix} = 2(-1)^{1+1} \cdot \begin{vmatrix} 0 & 3 & 3 \\ 4 & 0 & 3 \\ 0 & 4 & 1 \end{vmatrix} =$$

$$= 2(-1)^2 \cdot 4(-1)^{2+1} \cdot \begin{vmatrix} 3 & 2 & 3 \\ 4 & 1 & 0 \\ 4 & 1 & 4 \end{vmatrix} = 2(2+0+2-2-0-2) = 0$$

Una matriz cuadrada  $A \in M_{n \times n}(\mathbb{K})$  diremos que es regular si tiene inversa para el producto, es decir, si existe  $B \in M_{n \times n}(\mathbb{K})$  tq  $A \cdot B = B \cdot A = I_n$  ( $I_n$  = Matriz Identidad). En dicho caso, a la matriz  $B$  la denotaremos por  $A^{-1}$ . La matriz adjunta de  $A$  es la matriz  $\bar{A}$

$$\bar{A} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{vmatrix} \quad \text{NOTA: } a_{ij} \text{ es el adjunto de } A_{ij}.$$

### \* Teorema

Sea  $A$  una matriz cuadrada,  $A \in M_{n \times n}(\mathbb{K})$ , entonces  $A$  es regular  $\Leftrightarrow$  el determinante de  $A$  es distinto de cero. Además en dicho caso,  $A^{-1} = |A|^{-1} (\bar{A})^t$

Ejemplo:

Calcular la inversa, si existe, de la siguiente matriz

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in M_{3 \times 3} (\mathbb{Z}_5)$$

$|A| = -1 - 1 = 3$  como es  $\neq 0$ , tiene inversa.

$$\bar{A} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 4 & 1 \\ 4 & 1 & 4 \\ 1 & 4 & 4 \end{pmatrix}$$

$$(\bar{A})^{t\ddagger} = \begin{pmatrix} 4 & 4 & 1 \\ 4 & 1 & 4 \\ 1 & 4 & 4 \end{pmatrix}$$

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

Comprobación:  $A \cdot A^{-1} = I_n$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 3 & 2 \\ 3 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

# Prácticas 17/11/15

- ) ¿Cuántos elementos tiene  $\mathbb{Z}_3[x]/x^4+x^2+x+1$ ?  
¿Cuántos de ellos tienen inverso?

$$3^4 = \cancel{81} \text{ elementos. } (3^{\text{grado}} \cancel{7})$$

Solución: 81

1º Probar si  $x^4+x^2+x+1$  es irreducible

- No tiene raíces
- Calcular los polinomios de grado dos irreducibles  
 $\{x^2+1, x^2+2, \dots\}$

Los irreducibles son  $\{x^2+1, x^2+x+2, x^2+2x+2\}$

- Comprobar si cada uno de los irreducibles divide al polinomio  $x^4+x^2+x+1$ .  
Niuguno lo divide.

Por lo tanto  $x^4+x^2+x+1$  es irreducible y por consiguiente, todos los elementos de  $\mathbb{Z}_3[x]/x^4+x^2+x+1$  son unidades.

## Ejercicios

1) Calcular la inversa de la siguiente matriz.  $A^{-1} = |A|^{-1} (\bar{A})^t$

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix} \in M_{2 \times 2}(\mathbb{Z}_7)$$

$|A| = 4 - 2 = 2$  Por lo tanto,  $|A| \neq 0$  tiene inversa.

$$\bar{A} = \begin{pmatrix} 4 & 5 \\ 5 & 1 \end{pmatrix}$$

$$(\bar{A})^t = \begin{pmatrix} 4 & 5 \\ 5 & 1 \end{pmatrix}$$

$$4 \begin{pmatrix} 4 & 5 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 3 & 4 \end{pmatrix} = A^{-1}$$

$$\begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix} \underbrace{\begin{pmatrix} 2 & 6 \\ 3 & 4 \end{pmatrix}}_{A^{-1}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2) Sean  $A$  y  $B$  dos matrices  $\in M_{2 \times 2}(\mathbb{R})$  tq  $A+B = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$

$$A-B = \begin{pmatrix} -1 & -2 \\ 0 & 3 \end{pmatrix} \text{ Calcular } A^2 - B^2$$

$$2A = A+B + A-B \Rightarrow 2A = \begin{pmatrix} 2 & -2 \\ 2 & 4 \end{pmatrix} \Rightarrow A = \frac{1}{2} \begin{pmatrix} 2 & -2 \\ 2 & 4 \end{pmatrix} \Rightarrow$$

$$\Rightarrow A = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$$

$$B = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} \Rightarrow B = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 2 & -2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -3 \\ 3 & 3 \end{pmatrix}$$

$$B^2 = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix}$$

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

- 3) Para qué valores de  $x$  es la matriz  $A = \begin{pmatrix} 4 & 2 & 1 \\ 1 & 1 & 1 \\ 0 & x & 2 \end{pmatrix} \in M_{3 \times 3}(\mathbb{Z}_5)$  regular.

$$|A| =$$

La matriz será regular para aquellos valores de  $x$  en los que el det sea distinto de cero.

$$\begin{vmatrix} 4 & 2 & 1 \\ 1 & 1 & 1 \\ 0 & x & 2 \end{vmatrix} = 3x^2 - 4x - 24$$

$$= 3x^2 + 2x - 8x - 24 \quad \cancel{-1}$$

$$\rightarrow = 2x + 4$$

$$2x + 4 = 0 \rightarrow 2x = 1 \Rightarrow x = 2^{-1} \cdot 1 \Rightarrow \underline{\underline{x = 3}}$$

La matriz es regular  $\Leftrightarrow x \neq 3$ ,  $x = \begin{smallmatrix} 0 \\ 1 \\ 2 \\ 4 \end{smallmatrix}$

- 4) ~~la siguiente~~ Resuelve la siguiente ecuación en  $M_{3 \times 3}(\mathbb{Z}_5)$ :

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

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

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{vmatrix} = 2 \neq 0$$

$$\Rightarrow X = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 4 & 0 & 4 \\ 4 & 0 & 4 \\ 1 & 4 & 3 \end{pmatrix}$$

$$\xrightarrow{\text{I} \leftrightarrow \text{II}} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 4 & 4 & 1 \end{pmatrix} \dots = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix}$$

$$X = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 0 & 4 \\ 4 & 0 & 4 \\ 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 2 \\ 1 & 3 & 0 \\ 3 & 2 & 4 \end{pmatrix}$$

5) ¿de qué cardinal tiene el conjunto  $M_{m \times n}(\mathbb{Z}_p)$ ?

$$P^{m \times n}$$

6) Dar un ejemplo de anillo no commutativo con 512 elementos.

$$M_{n \times n}(\mathbb{Z}_p) \rightarrow$$

$$p^{n \times n} = 512 \rightarrow 2^{3 \times 3} = 512$$

7) Encuentra una matriz  $A \in M_{2 \times 2}(\mathbb{Z}_2)$  tq  $A \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  pero  $A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

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

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

## Tema 5 : Espacios Vectoriales

Sea  $K$  un cuerpo, diremos que un conjunto  $V$  tiene estructura de espacio vectorial sobre el cuerpo  $K$ , si verifica lo siguiente:

1) En  $V$  hay una operación  $+$  de forma que  $(V, +)$  es un grupo abeliano (es decir, la operación  $+$  es asociativa, commutativa, tiene elemento neutro e inverso). Denotaremos  $\vec{0}$  al elemento neutro y  $-\vec{v}$  al inverso de  $\vec{v}$ .

2) Existe una aplicación  $K \times V \rightarrow V$  verificando lo siguiente:  $(a, \vec{v}) \rightarrow a\vec{v}$

$$i) a(\vec{u} + \vec{v}) = a\vec{u} + a\vec{v} \quad \forall a \in K \text{ y } \forall \vec{u}, \vec{v} \in V$$

$$ii) (a+b)\vec{u} = a\vec{u} + b\vec{u} \quad \forall a, b \in K \text{ y } \forall \vec{u} \in V$$

$$iii) a(b\vec{u}) = (ab)\vec{u} \quad \forall a, b \in K \text{ y } \forall \vec{u} \in V$$

$$iv) 1 \cdot \vec{u} = \vec{u} \quad \forall \vec{u} \in V$$

→ A los elementos ~~elementos~~ del conjunto  $V$  los llamaremos "vectores", a los elementos de  $K$  los llamaremos "escalares" y a la aplicación  $K \times V \rightarrow V$  diremos que es un producto por escalares.

Ejemplos:

1) Si  $K$  es un cuerpo y  $n$  es un entero positivo, entonces  $K^n$  es un espacio vectorial sobre el cuerpo  $K$  definiendo la suma

$$(a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) = (a_1 + b_1, a_2 + b_2, \dots)$$

y el producto de escalares:

$$a(a_1, a_2, a_3, \dots) = (aa_1, aa_2, aa_3, \dots)$$

2) Si  $K$  es un cuerpo y  $m, n$  son enteros positivos entonces  $M_{m \times n}(K) \Rightarrow$  es un espacio vectorial sobre el cuerpo  $K$  con la operación suma de matrices y con productos por escalares

$$a \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} a \cdot a_{11} & a \cdot a_{12} & \dots & a \cdot a_{1n} \\ a \cdot a_{21} & a \cdot a_{22} & \dots & a \cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a \cdot a_{m1} & a \cdot a_{m2} & \dots & a \cdot a_{mn} \end{pmatrix}$$

3) Si  $K$  es un cuerpo y  $n$  es un entero positivo, entonces  $K[x]_n = \{a(x) \in K[x] \text{ tq } \text{gr}(a(x)) \leq n\}$  es un espacio vectorial sobre el cuerpo  $K$  con la operación ~~grado~~ suma de polinomios y con producto por escalares

$$a \cdot (a_n x^n + \dots + a_1 x + a_0) = a \cdot a_n x^n + \dots + a \cdot a_1 x + a \cdot a_0$$

Vamos a tratar fundamentalmente los del conjunto 1)

## • Propiedades

- 1)  $0 \cdot \vec{u} = \vec{0}$   $\forall \vec{u} \in V$
- 2)  $a \cdot \vec{0} = \vec{0}$   $\forall a \in K$
- 3) Si  $a \cdot \vec{u} = \vec{0}$  entonces  $a=0$  ó  $\vec{u} = \vec{0}$
- 4)  $-(a \cdot \vec{u}) = (-a) \vec{u} = a(-\vec{u})$
- 5)  $a(\vec{u} - \vec{v}) = a\vec{u} - a\vec{v}$
- 6)  $(a-b)\vec{u} = a\vec{u} - b\vec{u}$
- 7) Si  $a\vec{u} = a\vec{v}$  y  $a \neq 0$  entonces  $\vec{u} = \vec{v}$
- 8) Si  $a\vec{u} = b\vec{u}$  y  $\vec{u} \neq \vec{0}$  entonces  $a = b$

\*NOTA: De adelante  $V$  denotará un espacio vectorial sobre el cuerpo  $K$

→ Un subconjunto no vacío  $U$  de  $V$  diremos que es un subespacio vectorial de  $V$  si verifica lo siguiente:

- 1) Si  $\vec{u}$  y  $\vec{v} \in U$  entonces  $\vec{u} - \vec{v} \in U$
- 2) Si  $a \in K$  y  $\vec{u} \in U$  entonces  $a\vec{u} \in U$

\*NOTA: Los subespacios vectoriales de  $V$  son también espacios vectoriales sobre el cuerpo  $K$

Ejercicio:

1) Dar un espacio vectorial de cardinal 81

$$81 = 3^4 \rightarrow M_{2 \times 2}(\mathbb{Z}_3)$$

$$\rightarrow \mathbb{Z}_3^4 = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\rightarrow \mathbb{Z}_3 [x]_3$$

2) Demostrar que  $\mathcal{U} = \{(x, y, z) \in \mathbb{Q}^3 \mid x + y + z = 0\}$

es un subespacio vectorial  $\mathbb{Q}^3$ .

$$(0, 0, 0) \in \mathcal{U} \quad (1, 2, 3) \notin \mathcal{U}$$

$$(1, -1, 0) \in \mathcal{U}$$

$$1) (x_1, x_2, x_3), (y_1, y_2, y_3) \in \mathcal{U}$$

$$\Rightarrow (x_1, x_2, x_3) - (y_1, y_2, y_3) \in \mathcal{U}$$

$$= (x_1 - y_1, x_2 - y_2, x_3 - y_3)$$

$$x_1 - y_1 + x_2 - y_2 + x_3 - y_3 = \underline{x_1 + x_2 + x_3} - \underline{(y_1 + y_2 + y_3)} =$$

$$2) (x, y, z) \in \mathcal{U} \text{ y } a \in \mathbb{K}$$

$$a(x, y, z) = (ax, ay, az)$$

$$ax + ay + az = a(x + y + z)$$

$$\rightarrow a \cdot 0 = 0 \in \mathcal{U}$$

3) Encuentra todos los elementos de  $\mathcal{U} = \{(x, y) \in \mathbb{Z}_3^2 \mid x + y = 0\}$

$\mathbb{Z}_3^2$  es un espacio vectorial de cardinal 9.

Si procedemos como en el ejercicio anterior, veríamos que  $\mathcal{U}$  es un espacio vectorial de  $\mathbb{Z}_3^2$ .

$$\mathcal{U} = \{(0, 0), (1, 2), (2, 1)\}$$

• Proposición:

La intersección de subespacios vectoriales de  $V$  es también un subespacio vectorial de  $V$ .

Sea  $S$  un subconjunto no vacío de  $V$ . El subespacio vectorial de  $V$  generado por  $S$  es la intersección de todos los subespacios vectoriales de  $V$  que contienen a  $S$ . A dicho subespacio, lo denotaremos  $\langle S \rangle$ .

NOTA:  $\langle S \rangle$  es el menor (con el orden inclusión) subespacio vectorial de  $V$  que contiene a  $S$ .

• Proposición:

Si  $S' = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ , entonces  $\langle S' \rangle = \{a_1\vec{u}_1 + a_2\vec{u}_2 + \dots + a_n\vec{u}_n \mid a_1, a_2, \dots, a_n \in K\}$ .

Ejercicio:

Calcular todos los elementos del subespacio vectorial de  $\mathbb{Z}_2^3$  generado por  $\{(1,1,0), (0,1,1)\} = V$ .

Nos pide calcular  $\langle \{(1,1,0), (0,1,1)\} \rangle = \{a(1,1,0) + b(0,1,1) \mid a, b \in \mathbb{Z}_2\}$

$$a=0, b=0; a=0, b=1; a=1, b=0; a=1, b=1 \quad \text{tg } a, b \in \mathbb{Z}_2$$

$$\langle V \rangle = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\}$$

Sea  $U_1, U_2, \dots, U_n$  subespacios vectoriales de  $V$ , llamaremos subespacio vectorial suma de todos ellos a  $U_1 + U_2 + \dots + U_n = \{ \vec{u}_1 + \vec{u}_2 + \dots + \vec{u}_n \mid \vec{u}_1 \in U_1, \vec{u}_2 \in U_2, \dots, \vec{u}_n \in U_n \}$

- Proposición

$$1) U_1 + U_2 + \dots + U_n = \langle U_1 \cup U_2 \cup \dots \cup U_n \rangle$$

$$2) \text{ Si } U_1 = \langle S_1 \rangle, U_2 = \langle S_2 \rangle, \dots, U_n = \langle S_n \rangle$$

$$\text{entonces } U_1 + U_2 + \dots + U_n = \langle S_1 \cup S_2 \cup \dots \cup S_n \rangle$$

### Ejercicio:

Sean  $U_1$  y  $U_2$  los subespacios vectoriales de  $\mathbb{Z}_3^3$

generados por  $V = \{(1, 2, 0)\}$  y  $S = \{(0, 1, 2)\}$

respectivamente. Calcular todos los elementos de  $U_1 + U_2$ .

Sabemos que  $U_1 = \langle \{(1, 2, 0)\} \rangle$  y  $U_2 = \langle \{(0, 1, 2)\} \rangle$

Por tanto aplicando el punto dos de la proposición anterior, tenemos que  $U_1 + U_2 = \langle \{(1, 2, 0), (0, 1, 2)\} \rangle$

Por consiguiente  $U_1 + U_2 = \{ a(1, 2, 0) + b(0, 1, 2) \mid a, b \in \mathbb{Z}_3 \}$

$$U_1 + U_2 = \{ (0, 0, 0), (0, 1, 2), (0, 2, 1), (1, 2, 0), (1, 0, 2), (1, 1, 1),$$

$$\text{dando valores } (2, 1, 0), (2, 2, 2), (2, 0, 1) \}$$

$$\begin{matrix} 0, 1, 2 \\ a \text{ y } b \end{matrix}$$

Sean  $U$  y  $W$  subespacios vectoriales de  $V$ , diremos que  $V$  es suma directa de  $U$  y  $W$  (y lo denotaremos  $V = U \oplus W$ ) si todo vector de  $V$  se puede poner de forma única como suma de un vector de  $U$  y otro de  $W$ . En dicho caso diremos que los subespacios vectoriales  $U$  y  $W$  son complementarios.

• Proposición:

$V = U \oplus W \iff$  se verifican las siguientes condiciones:

$$1) V = U + W$$

$$2) \text{eu } U \cap W = \{\vec{0}\}$$

Ejercicio:

Sea  $U = \{(x, y) \in \mathbb{R}^2 \mid x+y=0\}$  y  $W = \{(x, y) \in \mathbb{R}^2 \mid x-y=0\}$ . Demostrar que  $\mathbb{R}^2$  es la suma directa de  $U$  y  $W$ :  $\mathbb{R}^2 = U \oplus W$ .

Para la demostración vamos a utilizar la proposición anterior:

1)  $\mathbb{R}^2 = U + W$ : debemos probar que todo vector de  $\mathbb{R}^2$  se puede poner como suma de un vector de  $U$  y un vector de  $W$ .

$$\text{Sea } (x, y) \in \mathbb{R}^2 \Rightarrow (x, y) = \left( \frac{x-y}{2}, \frac{y-x}{2} \right) + \left( \frac{x+y}{2}, \frac{x+y}{2} \right)$$

$$2) U \cap W = \{(x, y) \in \mathbb{R}^2 \mid x+y=0, x-y=0\}$$

$$\begin{aligned} x+y &= 0 \\ x-y &= 0 \end{aligned} \quad \left\{ \begin{array}{l} x=0 \\ y=0 \end{array} \right. \Rightarrow \begin{cases} x=0 \\ y=0 \end{cases}$$

Un conjunto de vectores ~~forman~~  $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\} \subseteq V$   
 es linealmente dependiente si existe  
 $(a_1, a_2, \dots, a_n) \in K^n \setminus \{(0, 0, \dots, 0)\}$  tq  $a_1 \vec{v}_1 + a_2 \vec{v}_2 + \dots + a_n \vec{v}_n = \vec{0}$

En caso contrario, diremos que el conjunto de vectores es  
 linealmente independiente.

Ejercicio:

¿Son los vectores  $(1, 1, 0), (0, 1, 1), (1, 0, 1)$  de  $\mathbb{R}^3$   
 linealmente independiente?

$$a(1, 1, 0) + b(0, 1, 1) + c(1, 0, 1) = (0, 0, 0)$$

$$\Rightarrow (a+c, a+b, b+c) = (0, 0, 0) \Rightarrow$$

$$\begin{array}{l} a+c=0 \\ a+b=0 \\ b+c=0 \end{array} \quad \begin{array}{l} c-b=0 \\ b+c=0 \end{array} \quad \Rightarrow \begin{array}{l} c=0 \\ b=0 \end{array} \quad \begin{array}{l} a=0 \end{array}$$

Los vectores son L.I.

¿Son los vectores  $(2, 3, 4), (4, 1, 3)$  de  $\mathbb{Z}_5^3$  L.I?

$$a(2, 3, 4) + b(4, 1, 3) = (0, 0, 0)$$

$$(2a+4b, 3a+b, 4a+3b) = (0, 0, 0)$$

$$2a+4b=0$$

$$3a+b=0$$

$$4a+3b=0$$

$$4b=0$$

$$\boxed{b \neq 0}$$

$$\left\{ \begin{array}{l} \rightarrow b = -2a \\ \star \end{array} \right\} \quad \left\{ \begin{array}{l} 2a+4(-2a)=0 \\ 2a+3a=0 \\ \star a=0 \end{array} \right\}$$

$$\boxed{b = 2a}$$

$$\boxed{a \neq 0}$$

Tiene 5 sol.

L.D

Ejercicios con matrices:

1) Prueba que la matriz  $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_2(\mathbb{Q})$  satisface una ecuación de la forma  $A^2 + \alpha A + \beta Id = 0$  donde  $\alpha, \beta \in \mathbb{Q}$ .

Utiliza este hecho para ver que  $A$  es regular y calcula su inversa.

$$A^2 + \alpha A + \beta Id = 0$$

$$A^2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix} + \alpha \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} + \beta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

$$\begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix} + \alpha \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}$$

$$\begin{pmatrix} \alpha & 2\alpha \\ 2\alpha & \alpha \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = - \begin{pmatrix} -5 & -4 \\ -4 & -5 \end{pmatrix}$$

$$\alpha + \beta = -5$$

$$2\alpha = -4$$

$$2\alpha = -4$$

$$\alpha + \beta = -5$$

$$\alpha + \beta = -5$$

$$2\alpha = -4$$

$$\boxed{\alpha = -2}$$

$$\boxed{\beta = -3}$$

Sabemos que

$$A^2 - 2A - 3Id = 0 \Rightarrow A^2 - 2A = 3Id \Rightarrow \frac{1}{3}A^2 - \frac{2}{3}A = Id$$

$$\Rightarrow A \left( \frac{1}{3}A - \frac{2}{3}Id \right) = Id \Rightarrow \begin{matrix} A \text{ es regular} \\ A^{-1} = \frac{1}{3}A - \frac{2}{3}Id \end{matrix}$$

$$\Rightarrow \det A \cdot \det \left( \frac{1}{3}A - \frac{2}{3}Id \right) = 1 \Rightarrow \det A \neq 0$$

### \* Proposición

- 1)  $S'$  es un conjunto de vectores linealmente dependiente si y solo si existe  $\vec{v} \in S$  tq  $\vec{v} \in \langle S \setminus \{\vec{v}\} \rangle$
- 2) Cualquier conjunto de vectores que contenga al vector  $\vec{0}$  es linealmente dependiente.
- 3) Si un conjunto de vectores linealmente dependiente le añadimos un vector, obtenemos un nuevo conjunto de vectores L.D.
- 4) Si un conjunto de vectores linealmente independiente, le quitamos un vector, obtenemos un nuevo conjunto de vectores linealmente independiente.

### \* Base

Un subconjunto no vacío  $B$  de  $V$  diremos que es una base de  $V$  si verifica lo siguiente:

- 1)  $V = \langle B \rangle$
- 2)  $B$  es L.I.

### \* Proposición

Si  $B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  es una base de  $V$  y  $\vec{v} \in V$  entonces existe una única  $n$ -tupla  $(a_1, a_2, \dots, a_n) \in \mathbb{K}^n$  tq  $\vec{v} = a_1 \vec{v}_1 + a_2 \vec{v}_2 + \dots + a_n \vec{v}_n$ .

Al  $n$ -tupla  $(a_1, a_2, \dots, a_n)$  se le llama las coordenadas del vector  $\vec{v}$  respecto de la base  $B$ , y lo denotaremos

$$\vec{v} \equiv_B (a_1, a_2, \dots, a_n)$$

### Ejercicio:

Dada la base  $B = \{(1, 2), (1, 3)\}$  de  $\mathbb{Z}_5^2$ , calcular las coordenadas del vector  $(2, 4)$  respecto de la base  $B$ .

$$(2, 4) = a(1, 2) + b(1, 3) \Rightarrow \begin{cases} a+b=2 \\ 2a+3b=4 \end{cases}$$

$$a+b=2 \rightarrow a=2-b$$

$$2(2-b)+3b=4$$

$$4-2b+3b=4$$

$$4+b=4$$

$$\underline{b=0} \rightarrow \underline{a=2}$$

$$\Rightarrow (2, 4) \equiv_B (2, 0)$$

### • Teorema de la base:

Todo espacio vectorial  $V \neq \{\vec{0}\}$  tiene al menos una base, además todas las bases de  $V$  tienen el mismo cardinal.

Al cardinal de una base de  $V$  lo llamaremos la dimensión de  $V$  y lo denotaremos  $\dim(V)$ . Por definición diremos que la dimensión del espacio vectorial  $\dim(\{\vec{0}\}) = 0$ .

• P

### \* Proposición.

1) La dimensión de  $K^n = \dim(K^n) = n$  y además  $\{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 0, 1)\}$  es una base de  $K^n$  a la que llamaremos base canónica.

2)  $\dim(M_{m \times n}(K)) = m \cdot n$  y además

$$\left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$$

es una base de  $M_{m \times n}(K)$ .

3)  $\dim(K[x]_n) = n+1$  y además  $\{1, x, x^2, \dots, x^n\}$  es una base de  $K[x]_n$ .

### • Teorema de ampliación de la base

Si la  $\dim(V) = n$  y  $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_r\}$  es un conjunto de vectores linealmente independiente de  $V$ , entonces  $r \leq n$ , además, si  $r = n$  entonces  $\{\vec{v}_1, \dots, \vec{v}_r\}$  es una base de  $V$  y si  $r < n$  entonces existen  $\vec{v}_{r+1}, \dots, \vec{v}_n \in V$  tq  $\{\vec{v}_1, \dots, \vec{v}_r, \vec{v}_{r+1}, \dots, \vec{v}_n\}$  es una base de  $V$ .

→ Corolario:

si  $\dim(V) = n$  entonces  $n$  vectores linealmente independientes de  $V$  son una base de  $V$ .

Ejercicio:

¿Es  $B = \{(1, 2, 3), (0, 1, 1)\}$  una base de  $\mathbb{Z}_7^3$ ?

Como la dimensión de  $\mathbb{Z}_7^3$  es igual a 3, entonces todas las bases de  $\mathbb{Z}_7^3$  tienen cardinal 3 y por tanto,  $B$  no puede ser una base de  $\mathbb{Z}_7^3$  (tiene cardinal 2).

¿Es  $B = \{(1, 2, 3), (0, 1, 1), (0, 0, 1)\}$  una base de  $\mathbb{Z}_7^3$ ?

Para responder a esta pregunta utilizando el corolario anterior, me bastará ver si son o no L.I.

$$a(1, 2, 3) + b(0, 1, 1) + c(0, 0, 1) = (0, 0, 0)$$

$$\begin{array}{l} a=0 \\ 2a+b=0 \\ 3a+b+c=0 \end{array} \left\{ \begin{array}{l} a=0 \\ b=0 \\ c=0 \end{array} \right.$$

Los vectores son linealmente independientes y por tanto,  $B$  es una base de  $\mathbb{Z}_7^3$ .

Ejercicio:

Ampliar el conjunto  $\{(1,1,1)\}$  a una base de  $\mathbb{R}^3$

$$B = \{(1,1,1), (\dots), (\dots)\}$$

Siempre se puede ampliar con vectores de base canónica.

$$B = \{(1,1,1), (0,1,0), (0,0,1)\}$$

$$a(1,1,1) + b(0,1,0) + c(0,0,1) = (0,0,0)$$

$$\begin{array}{l} a=0 \\ a+b=0 \\ a+c=0 \end{array} \quad \parallel \quad \begin{array}{l} a=0 \\ b=0 \\ c=0 \end{array}$$



\*Método para calcular una base de un subespacio vectorial a partir de un sistema de generadores de él.

- 1) Se quitan los vectores que son combinación lineal de los anteriores y el conjunto resultante, es una base del subespacio
- 2) Triangularizando la matriz cuyas filas son los vectores del sistema de generadores del subespacio las filas distintas de cero de esta matriz forman una base del subespacio.

Ejercicio:

Sea  $\mathcal{U}$  el subespacio vectorial de  $\mathbb{R}^3$  generado por  $\{(1, 2, 1), (2, 4, 2), (1, 3, 2), (2, 5, 3)\}$  y calcular una base de  $\mathcal{U}$ .

Ver método:

$$B_{\mathcal{U}} = \{(1, 2, 1), (1, 3, 2)\}$$

2º método: (recomendado)

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 3 & 2 \\ 2 & 5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad B_{\mathcal{U}} = \{(1, 2, 1), (0, 1, 1)\}$$

• Corolario:

Sea  $\mathcal{U}$  un subespacio vectorial de  $V$  entonces

$$\mathcal{U} = V \text{ si y solo si } \dim(\mathcal{U}) = \dim(V)$$

que es equivalente a que los vectores

forman una base.

Ejercicio:

Sea  $U = \langle (1, 1, 1), (1, 2, 1) \rangle$  y  $W = \langle (1, 2, 3), (0, 0, 2) \rangle$  dos subespacios vectoriales de  $\mathbb{Z}_5^3$ . ¿Es  $\mathbb{Z}_5^3$  la suma de  $U$  y  $W$ ?

Sabemos que  $U + W = \langle (1, 1, 1), (1, 2, 1), (1, 2, 3), (0, 0, 2) \rangle$

Vamos a calcular una base de  $U + W$ .

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$B_{U+W} = \{(1, 1, 1), (0, 1, 0), (0, 0, 2)\}$$

Por tanto  $U + W$  es un subespacio vectorial de  $\mathbb{Z}_5^3$  y  $\dim(U + W) = 3$ . Por consiguiente, aplicando el corolario anterior podemos afirmar que  $\mathbb{Z}_5^3 = U + W$

\* Método para calcular el complementario de un subespacio vectorial

(Recuérdese que si  $V = U \oplus W$  entonces los subespacios  $U$  y  $W$  son complementarios).

Sea  $U$  un subespacio vectorial de  $V$ :

1. Calculamos una base de  $U$
2. Ampliamos la base de  $U$  a una base de  $V$
3. El subespacio generado por los vectores que hemos añadido en la ampliación, es un complementario de  $U$

Ejercicio:

Sea  $U$  el subespacio vectorial de  $\mathbb{Q}^3$  generado por

$\{(1, 1, 1), (2, 1, 3), (4, 3, 5)\}$ . Calcular un complementario de  $U$ .

1)  $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 3 \\ 4 & 3 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$

$B_U = \{(1, 1, 1), (0, -1, 1)\}$

2)  $B_{Q^3} = \{(1, 1, 1), (0, -1, 1), (0, 0, 1)\}$

$a(1, 1, 1) + b(0, -1, 1) + c(0, 0, 1) = (0, 0, 0)$

$a = 0$

$a - b = 0$

$a + b + c = 0$

$a = 0$

$b = 0$

$c = 0$

3)  $W = \langle (0, 0, 1) \rangle$

Ejercicio:

Calcular la dimensión del subespacio vectorial de  $\mathbb{Z}^4$  generado por  $\{(2, 4, 3, 4), (4, 1, 6, 1), (3, 3, 3, 3), (5, 0, 6, 0)\}$ .

$$\left( \begin{array}{cccc} 2 & 4 & 3 & 4 \\ 4 & 1 & 6 & 1 \\ 3 & 3 & 3 & 3 \\ 5 & 0 & 6 & 0 \end{array} \right) \sim \left( \begin{array}{cccc} 2 & 4 & 3 & 4 \\ 0 & 0 & 0 & 1 \\ 0 & 4 & 2 & 4 \\ 0 & 4 & 2 & 4 \end{array} \right) \sim \left( \begin{array}{cccc} 2 & 4 & 3 & 4 \\ 0 & 4 & 2 & 4 \\ 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{array} \right) \sim$$

$$\left( \begin{array}{cccc} 2 & 4 & 3 & 4 \\ 0 & 4 & 2 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right) \quad \{(2, 4, 3, 4), (0, 4, 2, 4)\} \rightarrow \text{Base del Subespacio}$$

Por lo tanto, el subespacio tiene dimensión 2.

Sea  $B = \{(1, 1, 0), (1, 2, 1), (1, 1, 2)\} \subset \mathbb{Z}^3$  y  $B' = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\} \subset \mathbb{Z}^3$ . Si las coordenadas de un vector  $\vec{v}$  respecto a la base  $B$  son  $(1, 2, 3)$ . Calcular las coordenadas de ese mismo vector respecto a la base  $B'$ .

$$\text{Si } \vec{v} \equiv_B (1, 2, 3) \Rightarrow \vec{v} = 1(1, 1, 0) + 2(1, 2, 1) + 3(1, 1, 2)$$

$$\Rightarrow \vec{v} \equiv_{B'} (1, 3, 3)$$

$$\vec{v} \equiv_{B'} a(1, 1, 0) + b(1, 0, 1) + c(0, 1, 1) = (1, 3, 3)$$

$$a + b = 1 \rightarrow b = 1 - a$$

$$a + c = 3 \rightarrow c = 3 - a$$

$$b + c = 3 \rightarrow b + (3 - a) = 3$$

$$b - 3 + a = 3$$

$$b + a = 6 \rightarrow b = 6 - a$$

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

$$a + 1 - a = 1$$

$$2a = 1 \Rightarrow a = \frac{1}{2}$$

$$\boxed{\begin{array}{l} a = \frac{1}{2} \\ b = \frac{5}{2} \\ c = \frac{3}{2} \end{array}}$$

$$\boxed{\vec{v} \equiv_{B'} (3, 0, 3)}$$

## \* Operaciones del cambio de base

Sea  $B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  y  $B' = \{\vec{v}'_1, \vec{v}'_2, \dots, \vec{v}'_n\}$

dos bases de  $V$ . Supongamos que  $\vec{v}_1 \equiv_B (a_{11}, a_{12}, \dots, a_{1n})$

$\vec{v}_2 \equiv_B (a_{21}, a_{22}, \dots, a_{2n})$ ,  $\vec{v}_n \equiv_B (a_{n1}, a_{n2}, \dots, a_{nn})$ .

Sea  $\vec{x} \in V$  y supongamos que  $\vec{x} \equiv_B (x_1, x_2, \dots, x_n)$

y  $\vec{x} \equiv_{B'} (x'_1, x'_2, \dots, x'_n)$ , entonces

$$(x'_1, x'_2, \dots, x'_n) = (x_1, x_2, \dots, x_n)$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Expresión matricial del cambio  
de base de  $B$  a  $B'$

matriz del  
cambio de  
base de  $B$  a  $B'$ .

La matriz del cambio de base es  
siempre regular, además, su inversa es  
justamente la matriz del cambio de base  
de  $B'$  a  $B$ .

$$(x'_1, x'_2, \dots, x'_n) = (a_{11}, a_{12}, \dots, a_{1n}) \cdot (x_1, x_2, \dots, x_n)$$

$$x'_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$$

$$x'_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n$$

$$\vdots$$

$$x'_n = a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n$$

escribiendo en forma de

$$(x'_1, x'_2, \dots, x'_n)$$

$$\begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Sean  $B = \{(1,1,0), (1,2,1), (1,1,2)\}$  y  $B' = \{(1,1,0), (1,0,1), (0,1,1)\}$  dos bases de  $\mathbb{Z}^3$

a) Calcular las ecuaciones del cambio de base de  $B$  a  $B'$ .

$$(1,1,0) \equiv_{B'} (1,0,0)$$

$$(1,2,1) \equiv_{B'} (1,0,1)$$

$$(1,1,2) \equiv_{B'} (0,1,1)$$

$$\rightarrow (1,1,0) = a(1,1,0) + b(1,0,1) + c(0,1,1) \Rightarrow$$

De aquí sacamos un sistema y lo resolvemos  
obteniendo:  $\Rightarrow a=1, b=0, c=0$

$$\rightarrow (1,2,1) = a(1,1,0) + b(1,0,1) + c(0,1,1) \Rightarrow \\ \Rightarrow a=1, b=0, c=1$$

$$\rightarrow (1,1,2) = a(1,1,0) + b(1,0,1) + c(0,1,1) \Rightarrow \\ \Rightarrow a=0, b=1, c=1$$

La expresión matricial del cambio de base  
de  $B$  a  $B'$  es

$$(x', y', z') = (x, y, z) \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$x' = x + y$   
 $y' = z$   
 $z' = y + z$

b) Si las coordenadas de un vector  $\vec{v}$  respecto de la base  $B$  son  $(1,2,4)$ . Calcula las coordenadas de  $\vec{v}$  respecto de la base  $B'$

$$(1,2,4) \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (3,4,1)$$

c) Calcular las ecuaciones del cambio de base,  
de  $B'$  a  $B$ .

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 1 \\ 4 & 1 & 0 \end{pmatrix}$$

$$\det A = -1$$

$$[Adj(A)]^t = \begin{pmatrix} 4 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}^t = \begin{pmatrix} 4 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

La expresión matricial del cambio de base  
de  $B'$  a  $B$  es

$$(x^*, y^*, z^*) = (x^1, y^1, z^1) \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 1 \\ 4 & 1 & 0 \end{pmatrix}$$

d) Si la coordenada de un vector  $v$  respecto de  
la base  $B'$  son  $(1, 1, 1)$ . Calcula las coordenadas  
del vector  $v$  respecto de la base  $B$ .

$$(1, 1, 1) \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 1 \\ 4 & 1 & 0 \end{pmatrix} = (1, 0, 1) //$$

Las coordenadas del vector  $v$  respecto de  
la base  $B' = (1, 0, 1)$

## \* Ecuaciones paramétricas de un subespacio vectorial.

Sea  $U$  un subespacio vectorial de  $V$ ,  $B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  una base de  $V$  y  $B_U = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_r\}$  una base de  $U$ . Supongamos que: ~~las coordenadas de  $u$  respecto~~

$$\vec{u}_1 \in_B (a_{11}, a_{12}, \dots, a_{1n})$$

$$\vec{u}_2 \in_B (a_{21}, a_{22}, \dots, a_{2n})$$

$$\vdots$$

$$\vec{u}_r \in_B (a_{r1}, a_{r2}, \dots, a_{rn})$$

Sea  $\vec{x} \in V$  y supongamos que  $\vec{x} \in_B (x_1, x_2, \dots, x_n)$ . Entonces  $\vec{x} \in U \Leftrightarrow (x_1, x_2, \dots, x_n) = \lambda_1 (a_{11}, a_{12}, \dots, a_{1n}) + \lambda_2 (a_{21}, a_{22}, \dots, a_{2n}) + \dots + \lambda_r (a_{r1}, a_{r2}, \dots, a_{rn})$

Para algún  $\lambda_1, \lambda_2, \dots, \lambda_r \in K$ . Por tanto  $\vec{x} \in U \Leftrightarrow$

$$x_1 = a_{11}\lambda_1 + a_{12}\lambda_2 + \dots + a_{1n}\lambda_r$$

$$x_2 = a_{21}\lambda_1 + a_{22}\lambda_2 + \dots + a_{2n}\lambda_r$$

$$\vdots$$

$$x_n = a_{n1}\lambda_1 + a_{n2}\lambda_2 + \dots + a_{nn}\lambda_r$$

Ecuaciones paramétricas de  $U$  respecto a la base  $B$

**NOTA:** Las ecuaciones paramétricas de un subespacio siempre van referidas respecto a una base del espacio. Cuando nos pidan las ec. paramétricas de un subespacio y no nos especifiquen respecto de qué base supondremos que es respecto de la base ~~canónica~~ canónica.

Ejercicio:

Dada la base  $B = \{(1,1,0), (1,0,1), (0,1,1)\}$  de  $\mathbb{Q}^3$

y  $U$  es subespacio vectorial generado por

$\{(1,2,1), (1,3,2), (2,5,3)\}$  calcular las ecuaciones

paramétricas de  $U$  respecto de la base  $B$

1) Vamos a calcular la base de  $U$ , para ello

triangularizaremos la siguiente matriz

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$B_U = \{(1,2,1), (0,1,1)\}$$

2) Calculamos las coordenadas de los vectores  
de la base de  $U$  respecto de la base  $B$ .

$$(1,2,1) \in B \quad a(1,1,0) + b(1,0,1) + c(0,1,1) = (1,2,1)$$

$$(0,1,1) \in B \quad a(1,1,0) + b(1,0,1) + c(0,1,1) = (0,1,1)$$

$$\rightarrow a = 1, b = 0, c = 1 \Rightarrow (1,0,1)$$

$$\rightarrow a = 0, b = 0, c = 1 \Rightarrow (0,0,1)$$

$$3) (x, y, z) = \lambda(1,0,1) + \mu(0,0,1)$$

$$\boxed{\begin{array}{l} x = \lambda \\ y = 0 \\ z = \lambda + \mu \end{array}}$$

Ejercicio:

Calcular las ec. paramétricas del subespacio vectorial  $\mathbb{Z}_7^3$  generado por  $\{(2, 3, 5), (3, 1, 4), (2, 3, 1)\}$

1) Calculamos una base de  $\alpha$ . Para ello, triángularizaremos la matriz:

$$\begin{pmatrix} 2 & 3 & 5 \\ 3 & 1 & 4 \\ 2 & 3 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 5 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto:  $B_{\alpha} = \{(2, 3, 5), (0, 0, 3)\}$

2) Calculamos:

$$(2, 3, 5) \equiv_{B_C} (2, 3, 5)$$

$\downarrow$   
base canónica.

$$(0, 0, 3) \equiv_{B_C} (0, 0, 3)$$

3)  $(x, y, z) = \lambda(2, 3, 5) + \mu(0, 0, 3)$

$$\boxed{\begin{aligned} x &= 2\lambda \\ y &= 3\lambda \\ z &= 5\lambda + 3\mu \end{aligned}}$$

# PRACTICAS 11/12/15

1) Sea  $U = \{(x, y, z) \in \mathbb{Q}^3 : x+y+z=1\}$

¿Es un subespacio vectorial?

No, porque no es cerrado para la suma.

$$(0, 0, 1) \in U$$

$$(0, 1, 0) \in U$$

$$(0, 0, 1) + (0, 1, 0) = (0, 1, 1) \notin U$$

2)  $V_1 = (1, 2, 1)$

$$V_2 = (1, 0, 1)$$

$$V_3 = (2, 0, 1)$$

$$V_4 = (1, 0, 2)$$

$$\left. \begin{array}{c} \\ \\ \\ \end{array} \right\} \mathbb{R}^3$$

¿Son linealmente dependientes?

Sí:

$$(1, 0, 1) = a(1, 2, 1) + b(2, 0, 1) + c(1, 0, 2)$$

$$\Rightarrow a=0, b=\frac{1}{3}, c=\frac{1}{3}$$

$V_1$  no es combinación lineal.

$V_2$  sí es comb.

$$\text{lineal } V_2 = \frac{1}{3} V_3 + \frac{1}{3} V_4$$

$V_3$  sí es comb.

$$\text{lineal. } V_3 = 3V_2 - \frac{1}{3} V_4$$

$V_4$  sí es comb.

$$\text{lineal } V_4 = 3V_2 - \frac{1}{3} V_3$$

3) ¿Es  $B = \{(1,1,1), (1,2,2), (1,1,2)\}$  base de  $\mathbb{Q}^3$ ?

Para que lo sea:

$$\langle B \rangle = \mathbb{Q}^3 \quad y \quad B \text{ es L.I.}$$

Si  $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$  es regular,  $B$  es L.I.

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

Por lo tanto,  $B$  es L.I.

4)  $B' = \{(1,1,1), (0,1,1), (0,0,1)\}$

Ecuaciones del cambio de base de  $B$  a  $B'$   
( $B$  está en el ej. anterior)

$$u = (3, 5, 7)$$

\* Calculamos coordenadas de  $u$  en  $B$

\*\* Calculamos coordenadas de  $u$  en  $B'$

$$*(3, 5, 7) = a(1, 1, 1) + b(1, 2, 2) + c(1, 1, 2)$$

$$5) \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

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

$$\begin{array}{l} a=0 \\ b=0 \\ c=0 \\ d=0 \end{array} \quad \begin{array}{l} \parallel \text{ Son linealmente} \\ \parallel \text{ Independiente.} \end{array}$$

$$6) \text{ Eu } (\mathbb{Z}_5^3)$$

Calcula una base del espacio generado por:

$$\left\{ (2, 1, 3), (4, 4, 1), (4, 3, 1) \right\}$$

$$\begin{pmatrix} 2 & 1 & 3 \\ 4 & 4 & 1 \\ 4 & 3 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 4 \\ 4 & 4 & 1 \\ 4 & 3 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 4 \\ 0 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$B = \{(1, 3, 4), (0, 1, 0)\}$$

$x = a$ $y = 3a + b$ $z = 4a$
-------------------------------------

## \* Aplicaciones lineales

Sean  $V$  y  $V'$  dos espacios vectoriales sobre el mismo cuerpo  $K$ .

Una aplicación  $f: V \rightarrow V'$  diremos que es lineal

(o un ~~homomorfismo~~ homomorfismo) si verifica lo siguiente:

$$1) f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v}) \quad \forall \vec{u}, \vec{v} \in V$$

$$2) f(a \cdot \vec{v}) = a \cdot f(\vec{v}) \quad \forall a \in K \quad y \quad \forall \vec{v} \in V$$

Ejercicio:

Demuestra que la aplicación  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ ,

$f(x, y, z) = (x+y, x+z)$  es lineal.

$$\begin{aligned} 1) f((x, y, z) + (\bar{x}, \bar{y}, \bar{z})) &= f(x+\bar{x}, y+\bar{y}, z+\bar{z}) = \\ &= (x+\bar{x}+y+\bar{y}, x+\bar{x}+z+\bar{z}) = (x+y, x+z) + (\bar{x}+\bar{y}, \bar{x}+\bar{z}) = \\ &= f(x, y, z) + f(\bar{x}, \bar{y}, \bar{z}) \end{aligned}$$

Se conserva la suma.

$$\begin{aligned} 2) f(a(x, y, z)) &= f(ax, ay, az) = (ax+ay, ax+az) = \\ &= a(x+y, x+z) = a f(x, y, z) \end{aligned}$$

Se conserva el producto.

Por lo tanto, la aplicación es lineal.

• Proposición.

Si  $f: V \rightarrow V'$  es una aplicación lineal, entonces:

$$1) f(\vec{0}) = \vec{0}$$

$$2) f(-\vec{v}) = -f(\vec{v})$$

$$3) N(f) = \{\vec{v} \in V \text{ tq } f(\vec{v}) = \vec{0}\}$$

Que llamaremos núcleo de  $f$ , es un subespacio vectorial de  $V$ .

4)  $\text{Im}(f) = \{f(\vec{v}) \text{ tq } \vec{v} \in V\}$  es un subespacio vectorial de  $V'$  y que llamaremos imagen de  $f$ .

Ejercicio:

Dada la aplicación lineal  $f: \mathbb{Z}_5^3 \rightarrow \mathbb{Z}_5^2$

definida por  $f(x, y, z) = (2x + y + z, x + y + z)$ .  
Calcular todos los elementos del núcleo de  $f$ .

$$N(f) = \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } f(x, y, z) = (0, 0)\}$$

$$= \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } (2x + y + z, x + y + z) = (0, 0)\}$$

$$= \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } \begin{cases} 2x + y + z = 0 \\ x + y + z = 0 \end{cases}\}$$

$$= \{(0, 0, 0), (0, 4, 1), (0, 1, 4), (0, 2, 3), (0, 3, 2)\}$$

## \*Tipos especiales de aplicaciones lineales

- 1) Un "monomorfismo" es una aplicación lineal inyectiva.
- 2) Un "epimorfismo" es una aplicación lineal sobreyectiva.
- 3) Un "isomorfismo" es una aplicación lineal biyectiva

### • Proposición

Sea  $f: V \rightarrow V'$  una aplicación lineal:

- 1) Si  $f$  es un isomorfismo, entonces  $f^{-1}$  es también un isomorfismo.

- 2)  $f$  es un monomorfismo si y solo si

$$N(f) = \{0\}$$

- 3) Si  $V = \langle \vec{v}_1, \vec{v}_2, \vec{v}_3, \dots, \vec{v}_n \rangle$ , entonces  $\text{Im}(f) = \langle f(\vec{v}_1), f(\vec{v}_2), \dots, f(\vec{v}_n) \rangle$

- 4) Si  $f$  es un monomorfismo y  $\{\vec{v}_1, \dots, \vec{v}_n\}$  es un conjunto de vectores linealmente independientes, entonces  $\{f(\vec{v}_1), \dots, f(\vec{v}_n)\}$  es también un conjunto de vectores L.I.

### Ejercicio:

Dada la aplicación lineal  $f: \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^3$   $f(x, y) = (x, y, x+y)$

- a) Calcular una base de la imagen

Como  $\mathbb{Z}_7^2 = \langle (1, 0), (0, 1) \rangle$  entonces aplicando el punto 3 de la proposición anterior, tenemos que  $\text{Im}(f) = \langle f(1, 0), f(0, 1) \rangle$ .

Por tanto,  $\text{Im}(f) = \langle (1, 0, 1), (0, 1, 1) \rangle$

triangularizamos:

$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ , como ya está triangularizada,

una base de la imagen sería:

$$B_{\text{Im}(f)} = \{(1, 0, 1), (0, 1, 1)\}$$

b) ¿Es  $f$  un epimorfismo?

$$\text{Im}(f) \neq \mathbb{Z}_7^3$$

No, porque la dimensión de la imagen es 2  
y la imagen de  $\mathbb{Z}_7^3$  es 3.

Por tanto,  $f$  no es sobreyectiva y por consiguiente  
no es un ~~iso~~ epimorfismo.

c) ¿Es  $f$  un monomorfismo?

$$\begin{aligned} N(f) &= \{(x, y) \in \mathbb{Z}_7^2 \mid \text{tg } f(x, y) = (0, 0, 0)\} \\ &= \{(x, y) \in \mathbb{Z}_7^2 \mid (x, y, x+y) = (0, 0, 0)\} \\ &= \{(x, y) \in \mathbb{Z}_7^2 \mid \begin{array}{l} x=0 \\ y=0 \\ x+y=0 \end{array}\} = \{(0, 0)\} \\ &= \{\vec{0}\} \end{aligned}$$

Por tanto, aplicando el punto ~~2~~ 2 de la proposición anterior, tenemos que  $f$  es un monomorfismo

Ejercicio:

Dada la aplicación lineal  $f: \mathbb{R}^4 \rightarrow \mathbb{R}^3$

$$f(x, y, z, t) = (x+y, x+z, x+t)$$

a) Calcular una base de la imagen

Como  $\mathbb{R}^4 = \langle (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1) \rangle$

entonces  $\text{Im}(f) = \langle f(1, 0, 0, 0), f(0, 1, 0, 0), f(0, 0, 1, 0), f(0, 0, 0, 1) \rangle$

Por tanto:

$$\text{Im}(f) = \langle (1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1) \rangle$$

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

$$B_{\text{Im}f} = \{ (1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1) \}$$

b) ¿Es  $f$  un epimorfismo?

Como  $\text{Im}(f)$  es un subespacio vectorial de  $\mathbb{R}^3$  de dimensión 3, entonces  $\mathbb{R}^3 = \text{Im}(f)$ .

Por tanto,  $f$  es sobreyectiva y por consiguiente,  $f$  es un epimorfismo.

c) ¿Es  $f$  un monomorfismo?

$$\begin{aligned} N(f) &= \{ (x, y, z, t) \in \mathbb{R}^4 \mid \begin{cases} x+y=0 \\ x+z=0 \\ x+t=0 \end{cases} \} \\ &= \{ (0, 0, 0, 0), (-1, 1, 1, 1), (1, -1, -1, -1), \dots \} \end{aligned}$$

Como  $(1, -1, -1, -1) \in N(f)$  entonces,  $f$  no es inyectiva y por consiguiente,  $f$  no es un monomorfismo.

### • Teorema

Sea  $B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  una base de  $V$  y

$\{\vec{v}'_1, \vec{v}'_2, \dots, \vec{v}'_n\}$  un subconjunto de  $V'$ .

Entonces existe una única aplicación lineal

$f: V \rightarrow V'$  verificando que  $\{f(\vec{v}_1) = \vec{v}'_1, f(\vec{v}_2) = \vec{v}'_2, \dots, f(\vec{v}_n) = \vec{v}'_n\}$

además  $f$  es un isomorfismo si y solamente si

el conjunto  $\{\vec{v}'_1, \vec{v}'_2, \dots, \vec{v}'_n\}$  es una base de  $V'$ .

**NOTA:** El teorema anterior nos dice que una aplicación lineal queda perfectamente determinada si conocemos las imágenes de los vectores de una base de  $V$ , además dicha aplicación lineal es un isomorfismo, si y solamente si las imágenes de los vectores de la base de  $V$  son una base de  $V'$ .

- Dos espacios vectoriales  $V$  y  $V'$  diremos que son isomorfos si existe un isomorfismo  $f: V \rightarrow V'$ .

→ **Corolario:**

Dos espacios vectoriales sobre el mismo cuerpo son isomorfos si y solamente si tienen la misma dimensión.

Ejercicio:

- ¿Son los espacios vectoriales  $\mathbb{R}^2$  y  $\mathbb{Z}_5^2$  isomorfos?

No, ya que no son espacios vectoriales sobre el mismo cuerpo.

- ¿Son los espacios vectoriales  $M_{2 \times 2}(\mathbb{Z}_5)$  y  $\mathbb{Z}_5^4$  isomorfos?

Sí, porque son espacios vectoriales sobre el mismo cuerpo y tienen la misma dimensión: 4.

- ¿Son isomorfos los espacios vectoriales  $\mathbb{Q}[x]_3$  y  $\mathbb{Q}^3$ ?

No, ya que la dimensión de  $\mathbb{Q}[x]_3$  es 4 y  $\mathbb{Q}^3$  es 3.



Ejercicio:

Sea  $\mathcal{U}$  el subespacio vectorial de  $\mathbb{Z}_5^3$  generado por  $\{(1, 2, 3), (0, 1, 2), (1, 3, 0)\}$ . Calcular el cardinal de  $\mathcal{U}$ .

1º Vamos a calcular una base de  $\mathcal{U}$ , para ello triangulizaremos la matriz:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 1 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$B_{\mathcal{U}} = \{(1, 2, 3), (0, 1, 2)\}$$

$\mathcal{U}$  es un espacio vectorial sobre el cuerpo  $\mathbb{Z}_5$  de dimensión 2, y por tanto,  $\mathcal{U}$  es isomorfo a  $\mathbb{Z}_5^2$ . Por consiguiente el cardinal de  $\mathcal{U}$  coincide con el cardinal de  $\mathbb{Z}_5^2$  y en consecuencia el cardinal de  $\mathcal{U}$  es

25

## \*Ecuaciones de una aplicación lineal:

Sea  $f: V \rightarrow V'$  una aplicación lineal,

$B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  una base de  $V$  y

$B' = \{\vec{v}'_1, \vec{v}'_2, \dots, \vec{v}'_m\}$  una base de  $V'$ .

Supongamos que  $f(\vec{v}_1) =_{B'} [a_{11}, a_{12}, \dots, a_{1m}]$

$$f(\vec{v}_2) =_{B'} [a_{21}, a_{22}, \dots, a_{2m}]$$

$$f(\vec{v}_n) =_{B'} [a_{n1}, a_{n2}, \dots, a_{nm}]$$

Sea  $\vec{x} \in V$   $\vec{x} =_{B} (x_1, x_2, \dots, x_n)$  y  $\vec{x} =_{B'} (x'_1, x'_2, \dots, x'_m)$

Entonces:  $(x'_1, x'_2, \dots, x'_m) = (x_1, x_2, \dots, x_n) \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$

↓  
Expresión matricial de  $f$  respecto de la base  
 $B$  de  $V$  y la base  $B'$  de  $V'$ .

A la matriz se la llama, matriz asociada a  $f$   
respecto de la base  $B$  de  $V$  y la base  $B'$  de  $V'$ .

$$x'_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_n$$

$$x'_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_n$$

:

$$x'_m = a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mm}x_n$$

} Ecuaciones de  $f$   
respecto de la base  
 $B$  de  $V$  y la base  
 $B'$  de  $V'$ .

NOTA:

1)  $f$  es un isomorfismo si y solo si su matriz asociada es regular

2) La expresión matricial de una aplicación lineal siempre se refiere a una base  $B$  de  $V$  y una base  $B'$  de  $V'$ .

Cuando nos pidan calcular la expresión matricial de una aplicación lineal y no nos especifiquen respecto de qué base, supondremos que es respecto de la base canónica de  $V$  y la base canónica de  $V'$ .

Ejercicio:

Si  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}$  es la matriz asociada a una aplicación lineal  $f: \mathbb{Z}_5^2 \rightarrow \mathbb{Z}_5^3$  respecto de la base  $B = \{(2,1), (3,1)\}$  y  $B' = \{(1,1,0), (0,0,1), (0,1,1)\}$ . Calcular  $f(2,3)$ .

La expresión matricial de  $f$  respecto de las bases  $B$  y  $B'$  es  $(x', y', z') = (x, y) \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}$

$$(2, 3) \equiv_B ($$

$$(2, 3) = a(2, 1) + b(3, 1) \rightarrow \begin{cases} 2a + 3b = 2 \\ a + b = 3 \end{cases} \begin{cases} a = 2 \\ b = 1 \end{cases}$$

$$\Rightarrow (2, 3) \equiv_{B'} (2, 1)$$

$$(2, 1) \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix} = (4, 0, 0)$$

$$f(2, 3) \equiv_{B'} (4, 0, 0).$$

$$f(2, 3) = 4(1, 1, 0) + 0(1, 0, 1) + 0(0, 1, 1) =$$

$$\Rightarrow \boxed{f(2, 3) = (4, 0, 0)}$$

Ej.: Sea  $f: \mathbb{Q}^2 \rightarrow \mathbb{Q}^3$  la aplicación lineal definida por:

$$f(x, y) = (x, x+y, x-y). \text{ Calcular la expresión matricial}$$

de  $f$  respecto de las bases  $B = \{(1,1), (1,2)\}$  y  $B' = \{(1,1,0), (1,0,1), (0,1,1)\}$ .

$$f(1, 1) \equiv_B \left(\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}\right)$$

$$f(1, 2) \equiv_B \left(\frac{5}{2}, -\frac{3}{2}, \frac{1}{2}\right)$$

$$f(1, 1) = (1, 2, 0)$$

$$f(1, 2) = (1, 3, -1)$$

$$a(1, 1, 0) + b(1, 0, 1) + c(0, 1, 1) = (1, 2, 0) \rightarrow a = \frac{3}{2}, b = -\frac{1}{2}, c = \frac{1}{2}$$

$$a(1, 1, 0) + b(1, 0, 1) + c(0, 1, 1) = (1, 3, -1) \Rightarrow a = \frac{5}{2}, b = -\frac{3}{2}, c = \frac{1}{2}$$

La expresión matricial de  $f$  respecto de la base  $B$  y  $B'$

es:

$$(x', y', z') = (x, y) \begin{pmatrix} \frac{3}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{5}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$$

$$\boxed{\begin{aligned} x' &= \frac{3}{2}x + \frac{5}{2}y \\ y' &= -\frac{1}{2}x - \frac{3}{2}y \\ z' &= \frac{1}{2}x + \frac{1}{2}y \end{aligned}}$$

Ecuaciones de la aplicación  
lineal

Ejercicio:

Calcular una aplicación lineal  $f: \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^3$   
verificando que  $f(1,2) = (2,3,1)$  y  $f(2,5) = (3,4,2)$

Puesto que  $\{(1,2), (2,5)\}$  es una base de  $\mathbb{Z}_7^2$  entonces  
por el teorema anterior, sabemos que existe  
una única aplicación lineal verificando lo  
que queremos.

$$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} A = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \end{pmatrix} \Rightarrow A = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \end{pmatrix} \Rightarrow A = \boxed{\begin{pmatrix} 4 & 0 & 1 \\ 6 & 5 & 0 \end{pmatrix}}$$

$$A = \begin{pmatrix} 5 & 5 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \end{pmatrix} \Rightarrow A = \boxed{\begin{pmatrix} 4 & 0 & 1 \\ 6 & 5 & 0 \end{pmatrix}}$$

$$f(x, y) = (x, y) \begin{pmatrix} 4 & 0 & 1 \\ 6 & 5 & 0 \end{pmatrix} \Rightarrow f(x, y) = (4x+6y, 5y, x)$$

Comprobación:

$$f(1,2) = (2, 3, 1)$$

$$f(2,5) = (3, 4, 2)$$

Calcular una aplicación lineal de  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$  verificando que  $(1,0,0) \in N(f)$  y que  $\text{Im}(f) = \langle (2,3,1) \rangle$

$$f(1,0,0) = (0,0,0)$$

$$f(0,1,0) = (2,3,1)$$

$$f(0,0,1) = (8,12,4) \rightarrow \text{múltiplos de } (2,3,1).$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 3 & 1 \\ 8 & 12 & 4 \end{pmatrix} \Rightarrow A = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 3 & 1 \\ 8 & 12 & 4 \end{pmatrix}$$

$$f(x,y,z) = (x,y,z) \begin{pmatrix} 0 & 0 & 1 \\ 2 & 3 & 1 \\ 8 & 12 & 4 \end{pmatrix}$$

$$f(x,y,z) = (2y + 8z, 3y + 12z, y + 4z)$$

### \* Espacio vectorial cociente

Sea  $U$  un subespacio vectorial de  $V$  definidos sobre  $K$ . La relación binaria  $\vec{u} R \vec{v}$  si  $\vec{u} - \vec{v} \in U$ . Entonces  $R_U$  es una relación de equivalencia, y al conjunto cociente  $\frac{V}{R_U}$  lo denotaremos  $\frac{V}{U}$  ( $V$  sobre  $U$ ).

El conjunto  $\frac{V}{U}$  es también un espacio vectorial sobre el cuerpo  $K$  definiendo la suma como  $[\vec{u}] + [\vec{v}] = [\vec{u} + \vec{v}]$  y definiendo el producto por escalar como  $a[\vec{v}] = [a \cdot \vec{v}]$ .

A dicho espacio vectorial, lo llamaremos espacio vectorial cociente de  $V$  sobre  $U$  ( $\frac{V}{U}$ )

### • Proposición

Si  $\{\vec{u}_1, \dots, \vec{u}_r\}$  es una base de  $U$  y  $\{\vec{u}_1, \dots, \vec{u}_r, \vec{u}_{r+1}, \dots, \vec{u}_n\}$  una base de  $V$ . Entonces  $\{[\vec{u}_{r+1}], \dots, [\vec{u}_n]\}$  es una base de  $\frac{V}{U}$ .

→ Corolario:

$$\dim \frac{V}{U} = \dim V - \dim U$$

Ejercicio:

Sea  $U$  el subespacio vectorial de  $\mathbb{Z}_5^3$  generado por  $\{(2, 3, 4), (1, 4, 2)\}$ . Calcular una base del espacio vectorial cociente  $\frac{\mathbb{Z}_5^3}{U}$ .

Vamos a calcular una base de  $U$ . y para ello triangulizaremos la matriz:

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 \\ 0 & 0 & 0 \end{pmatrix} \quad B_U = \{(2, 3, 4)\}$$

Vamos a ampliar la base de  $U$  a una base de  $\mathbb{Z}_5^3$ :

$B = \{(2, 3, 4), (0, 1, 0), (0, 0, 1)\}$  entonces por la proposición anterior tenemos que  $\frac{\mathbb{Z}_5^3}{U}$   $\{[0, 1, 0], [0, 0, 1]\}$  es una base de  $\frac{\mathbb{Z}_5^3}{U}$ .

## \* 1er teorema de isomorfía

Si  $f: V \rightarrow V'$  es una aplicación lineal entonces los espacios vectoriales  $\frac{V}{N(f)}$  y  $I\text{m}(f)$  son isomorfos

→ Corolario:

Si  $f: V \rightarrow V'$  es una aplicación lineal, entonces  $\dim V = \dim N(f) + \dim I\text{m}(f)$ .

Ejercicio:

Dada la aplicación lineal  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^2$  definida por  $f(x, y, z) = (2x+y, 3x+z)$ . Hallar una base del núcleo

$$N(f) = \{(x, y, z) \in \mathbb{R}^3 \mid \begin{array}{l} 2x+y=0 \\ 3x+z=0 \end{array}\}$$

$$\dim \mathbb{R}^3 = \dim N(f) + \dim I\text{m}(f)$$

$$3 = \dim N(f) + \dim I\text{m}(f)$$

$$I\text{m}(f) = \langle f(1, 0, 0), f(0, 1, 0), f(0, 0, 1) \rangle$$

$$I\text{m}(f) = \langle (2, 3), (1, 0), (0, 1) \rangle$$

$$B_{I\text{m}(f)} = \{(1, 0), (0, 1)\} \Rightarrow \dim I\text{m}(f) = 2$$

Por lo tanto:

$$\dim N(f) = 1$$

$$B_{N(f)} = \{(1, -2, -3)\}$$

\* Segundo teorema de isomorfía:

Si  $U_1$  y  $U_2$  son subespacios vectoriales de  $V$ , entonces los espacios vectoriales  $\frac{U_2}{U_1 \cap U_2}$  y  $\frac{U_1 + U_2}{U_1}$  son isomorfos.

→ Corolario:

Si  $U_1$  y  $U_2$  son subespacios vectoriales de  $V$ , entonces  $\dim U_1 + \dim U_2 = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$

Ejercicio:

Sean  $U$  y  $W$  los subespacios vectoriales de  $\mathbb{Z}^3$  generados por  $\{(1, 1, 2), (1, 2, 3)\}$  y  $\{(1, 0, 0), (2, 1, 3)\}$  respectivamente. Calcular la dimensión de  $U \cap W$ .

$$\dim U + \dim W = \dim U + W + \dim(U \cap W)$$

$$U = \langle (1, 1, 2), (1, 2, 3) \rangle$$

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix} \Rightarrow \dim U = 2$$

$$W = \langle (1, 0, 0), (2, 1, 3) \rangle$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \end{pmatrix} \Rightarrow \dim W = 2$$

$$U + W = \langle (1, 1, 2), (1, 2, 3), (1, 0, 0), (2, 1, 3) \rangle$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 3 \\ 1 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 4 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \Rightarrow \dim U + W = 3$$

Por lo tanto:

$$\boxed{\dim(U \cap W) = 1}$$

## Tema 6: "Sistemas de ecuaciones lineales"

Sea  $A \in M_{n \times m}(K)$ , el rango por fila de la matriz  $A$  es la dimensión del subespacio vectorial de  $K^n$  generado por la fila de la matriz.

El rango por columna de la matriz  $A$ , es la dimensión del subespacio vectorial de  $K^m$  generado por la columna de la matriz.

Ejercicio:

Calcular el rango por fila y el rango por columna de la matriz.

$$A = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in M_{3 \times 4}(\mathbb{Z}_5)$$

$$R.F(A) = \dim (\langle (2, 3, 4, 1), (3, 3, 2, 4), (0, 1, 1, 0) \rangle) = \underline{\underline{2}}$$

$$\begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$R.C(A) = \dim (\langle (2, 3, 0), (3, 3, 1), (4, 2, 1), (1, 4, 0) \rangle) = \underline{\underline{2}}$$

$$\begin{pmatrix} 2 & 3 & 0 \\ 3 & 3 & 1 \\ 4 & 2 & 1 \\ 1 & 4 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

\* Teorema:

El rango por fila siempre coincide con el rango por columna. A dicha cantidad la llamaremos rango de la matriz  $A$  y la denotaremos  $\text{rang}(A)$

Sea una matriz  $A$ , entonces una matriz que se obtiene a partir de la matriz  $A$  quitándole alguna fila y alguna columna, se dice que es una submatriz de  $A$ .

\* Teorema:

El rango de una matriz es el máximo de los órdenes de sus submatrices cuadradas regulares.

Ejercicios:

1) Calcular el rango de la matriz  $A = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in M_{3 \times 4}(\mathbb{Z}_5)$

$$\begin{vmatrix} 2 & 3 & 4 \\ 3 & 3 & 2 \\ 0 & 1 & 1 \end{vmatrix} = 0 \quad \begin{vmatrix} 2 & 3 & 1 \\ 3 & 3 & 4 \\ 0 & 1 & 0 \end{vmatrix} = 0$$

$$\boxed{\text{rang}(A)=2}$$

2) ¿Es  $\{(1, 2, 1), (2, 3, 2), (4, 3, 3)\}$  una base de  $\mathbb{Z}_7^3$ ?

$$\begin{vmatrix} 1 & 2 & 1 \\ 2 & 3 & 2 \\ 4 & 3 & 3 \end{vmatrix} = 2 + 6 + 2 - 2 - 6 - 2 = 11$$

$$\text{rang} = 3 \quad \text{Por lo que son una base de } \mathbb{Z}_7^3.$$

## \* Expresión matricial de un sistema de ecuaciones lineales

Un sistema de  $m$  ecuaciones lineales con  $n$  incógnitas sobre un cuerpo  $K$  es una expresión de la forma:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned} \quad \left. \right\}$$

Una solución del sistema es una  $n$ -tuple  $(s_1, s_2, \dots, s_n) \in K^n$  tal que si  $x_1 = s_1, x_2 = s_2, \dots, x_n = s_n$  se verifican las  $n$  igualdades del sistema.

Las  $m$  igualdades del sistema se pueden expresar como una única igualdad entre matrices de la siguiente forma:

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}}_{\text{matriz de los coeficientes}} \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\text{matriz incógnita}} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_{\text{matriz de los términos independientes}}$$

Expresión matricial del sistema.

llamaremos "matriz ampliada":

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

## \* Tipos especiales de sistemas:

Si un sistema tiene solución diremos que es compatible y en caso contrario diremos que es incompatible.

Si tiene una única solución diremos que es compatible determinado, y si tiene al menos dos soluciones diremos que es compatible indeterminado

Dos sistemas de ecuaciones sobre el mismo cuerpo, diremos que son equivalentes si tienen la misma solución.

## \* Proposiciones:

- 1) Si intercambiamos de posición dos ecuaciones en un sistema, obtenemos un sistema equivalente.
- 2) Si multiplicamos una ecuación por un elemento del cuerpo distinto de cero, obtenemos un sistema equivalente
- 3) Si a una ecuación le sumamos otra ecuación multiplicada por un elemento del cuerpo, obtenemos un sistema equivalente.

## \* MÉTODO DE GAUSS

Resolver el siguiente sistema cuyos coeficientes están en  $\mathbb{Z}_7$

$$\begin{array}{l} x + 2y + 3z = 1 \\ x + y + 2z = 0 \\ 2x + y + 4z = 3 \end{array} \left\{ \Rightarrow \begin{array}{l} x + 2y + 3z = 1 \\ 6y + 6z = 6 \\ 4y + 5z = 1 \end{array} \right\} \Rightarrow$$

$$\begin{array}{l} x + 2y + 3z = 1 \\ y + z = 1 \\ 4y + 5z = 1 \end{array} \left\{ \Rightarrow \begin{array}{l} x + 2y + 3z = 1 \\ y + z = 1 \\ z = 4 \end{array} \right\}$$

$$\boxed{y \mid z=4} \quad \boxed{y=4} \quad \boxed{x=2}$$

Ejercicio:

Resolver el siguiente sistema con coeficientes en  $\mathbb{Z}_5$

$$\begin{cases} x + y + z = 1 \\ 2x + y + 3z = 0 \\ x + 4y + 3z = 2 \end{cases} \Rightarrow \begin{cases} x + y + z = 1 \\ 4y + 2z = 3 \\ 3y + 2z = 1 \end{cases} \Rightarrow \begin{cases} x + y + z = 1 \\ 4y + z = 3 \\ 0 = 0 \end{cases}$$

$$\begin{cases} x + y = 1 - z \\ 4y = 3 - z \end{cases} \quad |z = \lambda| \quad \Rightarrow \quad y = 4^{-1}(3 - \lambda) = 4(3 - \lambda)$$
$$\Rightarrow x = 1 - \lambda - 2 - \lambda = 4 + 3\lambda$$
$$x = 4 + 3\lambda$$

Ejercicio:

Resolver el siguiente sistema con coeficientes en  $\mathbb{Q}$

$$\begin{cases} x + y + z = 1 \\ x + 2y + z = 2 \\ 2x + y + 4z = 0 \end{cases} \Rightarrow \begin{cases} x + y + z = 1 \\ y - 2z = 1 \\ -y + 2z = 2 \end{cases} \Rightarrow \begin{cases} x + y + z = 1 \\ y - 2z = 1 \\ 0 = 1 \end{cases}$$

El sistema es incompatible

$\Rightarrow$  No tiene solución.

Cuando se pida estudiar un sistema, hay que resolverlo  
y e juzgar de qué tipo es

## \* Teorema de ROUCHE - FROBENIUS

Un sistema es compatible si y solamente si el rango de la matriz de los coeficientes coincide con el de la matriz ampliada. Además es compatible determinado si y solamente si dicho rango coincide con el número de incógnita.

Ejercicio:

Estudiar el siguiente sistema con coeficientes en  $\mathbb{Z}_5$

$$\begin{array}{l} 2x + 4y + 4z = 1 \\ 3x + y + 2z = 2 \\ 4y + z = 3 \end{array} \left\{ \begin{array}{l} \text{rang} \begin{pmatrix} 2 & 4 & 4 \\ 3 & 1 & 2 \\ 0 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 4 \\ 0 & 0 & 1 \\ 0 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 4 \\ 0 & 4 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ \text{rang} \begin{pmatrix} 2 & 4 & 4 & 1 \\ 0 & 4 & 1 & ? \\ 0 & 0 & 1 & ? \end{pmatrix} = 3 \end{array} \right.$$

$$\text{rang} \begin{pmatrix} 2 & 4 & 4 & 1 \\ 3 & 1 & 2 & 2 \\ 0 & 4 & 1 & 3 \end{pmatrix} = 3$$

El sistema es compatible determinado.

Estudiar el siguiente sistema con coeficientes en  $\mathbb{Z}_7$  y que depende del parámetro  $a$ .

$$\begin{array}{l} ax + y + z = 1 \\ x + ay + z = 0 \\ x + y + az = a \end{array} \quad \left| \begin{array}{ccc|c} a & 1 & 1 & 1 \\ 1 & a & 1 & 0 \\ 1 & 1 & a & a \end{array} \right| = a^3 + 4a + 2$$

$$a^3 + 4a + 2 = 0 \Leftrightarrow a \in \{1, 5\}$$

Si  $a \notin \{1, 5\}$  el determinante es distinto de cero y el rango de la matriz de los coeficientes vale 3.

Por consiguiente el rango de la matriz ampliada vale 3, y por consiguiente el sistema es compatible determinado

Ahora estudiamos los casos  $a=1$  y  $a=5$

$a=1$

$$\text{rang} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 1 \quad \text{rang} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} = 2$$

Por lo tanto, para  $a=1$ , el sistema es incompatible

$a=5$

$$\text{rang} \begin{pmatrix} 5 & 1 & 1 \\ 1 & 5 & 1 \\ 1 & 1 & 5 \end{pmatrix} = 2 \quad \text{rang} \begin{pmatrix} 5 & 1 & 1 & 1 \\ 1 & 5 & 1 & 0 \\ 1 & 1 & 5 & 5 \end{pmatrix} = 3$$

$$\begin{pmatrix} 5 & 1 & 1 \\ 1 & 5 & 1 \\ 1 & 1 & 5 \end{pmatrix} = 5+1-5-5$$

Por lo tanto, para  $a=5$ , el sistema es incompatible

Resolver el siguiente sistema con coeficientes en  $\mathbb{R}$  y que depende de los parámetros  $a$  y  $b$ .

$$\left. \begin{array}{l} ax + y + z = 1 \\ x + by + z = b \\ ax + by + z = 1 \end{array} \right\} \quad \left| \begin{array}{ccc|c} a & 1 & 1 & 1 \\ 1 & 1 & 1 & b \\ a & b & 1 & 1 \end{array} \right| = a + a + b - a - ab - 1 = \\ = a + b - ab - 1 \\ = a(1 - b) + b - 1 = \\ = a(1 - b) - (1 - b) = \\ = (1 - b)(a - 1)$$

$$(1 - b)(a - 1) = 0 \Leftrightarrow \begin{cases} a = 1 \\ b = 1 \end{cases}$$

Si  $a \neq 1$  y  $b \neq 1$  el determinante es distinto de cero, el rango es 3 y el de la matriz auxiliar es 3 por lo que el sistema es compatible determinado.

$$\boxed{a=1}$$

$$\text{rang} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & b & 1 \end{pmatrix} = \begin{cases} 1 & \text{si } b \neq 1 \\ 2 & \text{si } b = 1 \end{cases}$$

$$\text{rang} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & b \\ 1 & b & 1 & 1 \end{pmatrix} = \begin{cases} 1 & \text{si } b = 1 \\ 3 & \text{si } b \neq 1 \end{cases}$$

$$\left| \begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 1 & b & b \\ 1 & b & 1 & 1 \end{array} \right| = \cancel{b^2} - 2b + 1 = \\ = (b-1)^2$$

Por lo tanto, si  $a = 1$  y  $b = 1 \rightarrow$  S.C. I

si  $a = 1$  y  $b \neq 1 \rightarrow$  S. I

$$\boxed{b=1 \text{ y } a \neq 1}$$

$$\text{rang} \begin{pmatrix} a & 1 & 1 \\ 1 & 1 & 1 \\ a & 1 & 1 \end{pmatrix} = 2 \quad \text{rang} \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ a & 1 & 1 & 1 \end{pmatrix} = 2$$

Por lo tanto, si  $a \neq 1$  y  $b=1 \rightarrow \text{S.C.I.}$

→ Estudiar el siguiente sistema con coeficientes en  $\mathbb{Z}_5$  y que depende del parámetro  $a$ .

$$\begin{cases} ax + y + z = 1 \\ x + y + z = 2 \end{cases} \quad \text{rang} \begin{pmatrix} a & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{cases} 1 & \text{si } a=1 \\ 2 & \text{si } a \neq 1 \end{cases}$$

$$\text{rang} \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix} = 2$$

Por lo tanto, si  $a=1 \rightarrow \text{S.I.}$   
 $a \neq 1 \rightarrow \text{S.C.I.}$

→ Estudiar el siguiente sistema con coeficientes en  $\mathbb{IR}$  y que depende del parámetro.

$$\begin{cases} ax + y + z = 1 \\ x - y + z = 1 \end{cases} \quad \text{rang} \begin{pmatrix} a & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} = 2$$

$$\text{rang} \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix} = 2$$

Por lo tanto el sistema es C.I.

→ Estudiar el siguiente sistema con coeficientes en  $\mathbb{Z}_7$  y que depende del parámetro  $a$ .

$$\begin{cases} ax + y + z = 1 \\ x + 2y + az = 2 \end{cases} \quad \text{rang} \begin{pmatrix} a & 1 & 1 \\ 1 & 2 & a \end{pmatrix} = 2$$

$$\text{rang} \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 2 & a & 2 \end{pmatrix} = 2$$

Por lo tanto → S. C. I

### \* CRAMER

• Fórmula.

Un sistema es de Cramer si su matriz de coeficientes es cuadrada y regular.

Si  $AX=B$  es la expresión matricial de un sistema de Cramer, entonces el sistema es compatible determinado y su única solución es  $|A|^{-1}(|M_1|, |M_2|, \dots, |M_n|)$  donde  $M_i$  es la matriz que se obtiene a partir de la matriz  $A$  quitándole la columna  $i$  y colocando en su lugar, la columna  $B$ .

Ejercicio :

Probar que el siguiente sistema es de Cramer y calcular su solución usando la fórmula de Cramer.

coeficientes en  $\mathbb{R}$ .

$$\begin{cases} x + y + z = 1 \\ x - y + z = 0 \\ x + y - z = 2 \end{cases} \quad \begin{vmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{vmatrix} = 1+1+1+1-1-1 = 4$$

$$x = \frac{1}{4} \cdot \begin{vmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 1 & -1 \end{vmatrix} = \frac{1}{4} \cdot 4 = 1 \Rightarrow \boxed{x=1}$$

$$y = \frac{1}{4} \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \end{vmatrix} = \frac{1}{4} \cdot \frac{1}{2} \Rightarrow \boxed{y = \frac{1}{2}}$$

$$z = \frac{1}{4} \begin{vmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 0 \end{vmatrix} = -\frac{1}{2} \Rightarrow \boxed{z = -\frac{1}{2}}$$

Ejercicio:

Resolver el siguiente sistema con coeficientes en  $\mathbb{Z}_5$

$$\begin{array}{l} x+y+z=3 \\ x+y+2z=1 \end{array} \quad \text{rang } \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix} = 2$$

$$\text{rang } \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 1 & 2 & 1 \end{pmatrix} = 2$$

Sistema compatible indeterminado.

$$\begin{array}{l} y+z=3-x \\ y+2z=1-x \end{array} \quad \Rightarrow \quad \begin{array}{l} y+z=3+4x \\ y+2z=1+4x \end{array}$$

$$\boxed{x=\lambda}$$

$$\begin{array}{l} y+z=3+4\lambda \\ y+2z=1+4\lambda \end{array} \quad \left| \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 2 & 1 \end{array} \right| = 1$$

$$y = \lambda^{-1} \cdot \begin{vmatrix} 3+4\lambda & 1 \\ 1+4\lambda & 2 \end{vmatrix} = \lambda + 3\lambda - 1 - 4\lambda = 4\lambda$$

$$\boxed{y=4\lambda}$$

$$z = \lambda^{-1} \cdot \begin{vmatrix} 1 & 3+4\lambda \\ 1 & 1+4\lambda \end{vmatrix} = 3$$

$$\boxed{z=3}$$

Resuelve el siguiente sistema con coeficientes en  $\mathbb{Z}_7$

$$\begin{cases} x + y + z + t = 1 \\ x + y + 2z + 3t = 2 \end{cases} \quad \text{rang} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 \end{pmatrix} = 2$$

$$\begin{cases} x + t = 1 + 6y + 6z \\ x + 3t = 2 + 6y + 5z \end{cases} \quad \begin{cases} y = \lambda \\ z = \mu \end{cases}$$

$$\begin{cases} x + t = 1 + 6\lambda + 6\mu \\ x + 3t = 2 + 6\lambda + 5\mu \end{cases} \quad \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} = 2$$

$$x = 2^{-1} \cdot \begin{vmatrix} 1+6\lambda+6\mu \\ 1+6\lambda+5\mu \end{vmatrix} = 4 \cdot (3 + 4\lambda + 4\mu + 5 + \lambda + 2\mu) \\ = 4(1 + 5\lambda + 6\mu) \\ = 4 + 6\lambda + 3\mu$$

$$t = 5^{-1} \begin{vmatrix} 1 & 1+6\lambda+6\mu \\ 1 & 2+6\lambda+5\mu \end{vmatrix} = 4(2 + 6\lambda + 5\mu - 1 - 6\mu - 6\lambda) \\ = 4(1 + 6\mu) = 4 + 3\mu$$

Tiene  $7^2$  soluciones = 49.

## \* Ecuaciones cartesianas de un subespacio vectorial

Sea  $U$  un subespacio vectorial de  $V$ , sea  $B = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$  una base de  $V$  y  $B_U = \{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_r\}$  una base de  $U$ .

Supongamos que  $\vec{u}_1 \equiv_B (a_{11}, a_{12}, \dots, a_{1n})$

$\vec{u}_2 \equiv_B (a_{21}, a_{22}, \dots, a_{2n})$

$\vec{u}_r \equiv_B (a_{r1}, a_{r2}, \dots, a_{rn})$

Sea  $\vec{x} \in V$  y supongamos que  $\vec{x} \equiv_B (x_1, x_2, \dots, x_n)$ , entonces

$\vec{x} \in U \Leftrightarrow$  el rango de

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & x_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & x_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{rn} & a_{rn} & \cdots & a_{rn} & x_n \end{pmatrix} = r$$

Para que esto ocurra, ciertos determinantes deben ~~llegar~~ <sup>valer</sup> el cero. El desarrollo de dichos determinantes igualados a cero, nos proporciona  $n-r$  ecuaciones linealmente independientes de la forma:

$$b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n = 0$$

$$b_{n-r+1}x_1 + b_{n-r+2}x_2 + \dots + b_{n-r+n}x_n = 0$$

A dichas ecuaciones las llamaremos ecuaciones cartesianas de  $U$  respecto de la base  $B$ .

NOTA:

1)  $U$  está determinado por  $\dim V - \dim U$  ecuaciones cartesianas L.I (linealmente independientes)

2) Si nos piden calcular las ecuaciones cartesianas de  $U$  y no nos dicen respecto de qué base, supondremos que es respecto de la base Cartónica.

## 10 EJERCICIOS MUY IMPORTANTES

① Dada la base  $B = \{(1,1,0), (1,0,1), (0,1,1)\}$  de  $\mathbb{R}^3$ , calcular las ecuaciones cartesianas de  $U = \langle (1,2,1) \rangle$  respecto de la base  $B$

1º necesitamos una base de  $U$

$$B_U = \{(1,2,1)\}$$

2º Calculamos las coordenadas de los vectores de la base de  $U$  respecto de la base  $B$ .

$$(1,2,1) \equiv_B (1,0,1)$$

$$(1,2,1) = a(1,1,0) + b(1,0,1) + c(0,1,1)$$

$$\begin{aligned} a+b &= 1 \\ a+c &= 2 \\ b+c &= 1 \end{aligned} \quad \left\{ \begin{array}{l} a=1 \\ b=0 \\ c=0 \end{array} \right.$$

3º.  $U$  viene dado por  $\dim \mathbb{R}^3 - \dim U = 3 - 1 = 2$  ecuaciones cartesianas linealmente independiente que se obtienen al imponer el

Para ello,

$$\begin{aligned} \begin{vmatrix} 1 & 1 & x \\ 0 & 1 & y \\ 1 & 0 & z \end{vmatrix} &= 0 \Rightarrow \boxed{y=0} \quad \text{rang} \begin{pmatrix} 1 & x \\ 0 & y \\ 1 & z \end{pmatrix} = \cancel{\dim U = 1} \\ \begin{vmatrix} 1 & x \\ 1 & z \end{vmatrix} &= 0 \Rightarrow \boxed{z-x=0} \quad \text{ec. cartesianas de } U \text{ resp. de la base } B. \end{aligned}$$

- ② Calcular las ecuaciones cartesianas del subespacio vectorial  $\mathbb{Q}^4$  generado por  $\{(1, 2, 3, 1), (1, 1, 1, 1), (3, 5, 7, 3)\}$

Sea  $U$  dicho subespacio:

1º Calculamos una base de  $U$ :

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 1 & 1 & 1 \\ 3 & 5 & 7 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & -1 & -2 & 0 \\ 0 & -1 & -2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$B_U = \{(1, 2, 3, 1), (0, -1, -2, 0)\}$$

2º Calculamos las coordenadas de los vectores de la base  $U$  respecto de la base canónica.

$$(1, 2, 3, 1) \equiv_{B_C} (1, 2, 3, 1)$$

$$(0, -1, -2, 0) \equiv_{B_C} (0, -1, -2, 0)$$

3º  $U$  viene dado por  $\dim \mathbb{Q}^4 - \dim U = 4 - 2 = 2$  ecuaciones cartesianas que se obtienen al imponer que

$$\text{rang} \begin{pmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 3 & -2 & z \\ 1 & 0 & t \end{pmatrix} = \dim U = 2 \quad \text{Para ello,}$$

$$\begin{vmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 3 & -2 & z \end{vmatrix} = 0 \rightarrow -z - 4x + 3x + 2y = 0 \Rightarrow \boxed{-x + 2y - z = 0}$$

$$\begin{vmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 1 & 0 & t \end{vmatrix} = 0 \rightarrow -t + x = 0$$

Las ecuaciones son:

$$\boxed{\begin{aligned} -x + 2y - z &= 0 \\ -t + x &= 0 \end{aligned}}$$

- ③ Dado los subespacios vectoriales de  $\mathbb{Z}_5^3$   $U = \{(1,1,1), (1,2,1)\}$   
 y  $W = \{(1,4,3), (0,0,4)\}$ , calcular una base de  $U \cap W$

1º Vamos a calcular las ecuaciones cartesianas de  $U$

$B_U = \{(1,1,1), (1,2,1)\}$  Por tanto,  $U$  viene dada por  $3-2=1$  ecuación. Dicha ecuación se obtiene al imponer:

$$\text{rang} \begin{pmatrix} 1 & 1 & x \\ 1 & 2 & y \\ 1 & 1 & z \end{pmatrix} = \dim U = 2$$

$$\begin{vmatrix} 1 & 1 & x \\ 1 & 2 & y \\ 1 & 1 & z \end{vmatrix} = 0 \Rightarrow 2x + y + x - 2x - y - z = 0 \\ 4x + z = 0$$

Entonces  $U = \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } 4x + z = 0\}$

2º Vamos a calcular las ecuaciones cartesianas de  $W$ .

$B_W = \{(1,4,3), (0,0,4)\}$   $W$  viene dada

por  $3-2=1$  ecuaciones, que se obtiene imponiendo:

$$\text{rang} \begin{pmatrix} 1 & 0 & x \\ 4 & 0 & y \\ 3 & 4 & z \end{pmatrix} = 2 \quad \begin{vmatrix} 1 & 0 & x \\ 4 & 0 & y \\ 3 & 4 & z \end{vmatrix} = 0 \Rightarrow x + y = 0$$

Entonces  $W = \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } x + y = 0\}$

$$U \cap W = \{(x, y, z) \in \mathbb{Z}_5^3 \text{ tq } \begin{cases} 4x + z = 0 \\ x + y = 0 \end{cases}\}$$

Las ecuaciones son L.I.

$U \cap W$  es un subespacio vectorial de  $\mathbb{Z}_5^3$  que viene dado por dos ecuaciones L.I. Por tanto  $U \cap W$  es un espacio vectorial de dimensión  $\dim \mathbb{Z}_5^3 - \text{nº ec. L.I.} = 3-2 = 1$

~~U ∩ W~~

Por consiguiente, una base de  $U \cap W$  es:

$$B_{U \cap W} = \{(1, 4, 1)\}$$

④ Sea  $U = \{(x, y, z, t) \in \mathbb{Z}_5^4 \text{ tq } \begin{cases} 2x + 3y + 2z + t = 0 \\ x + 4y + z + 3t = 0 \end{cases}\}$

Calcular una base de  $U$ .

1º Vemos cuántas ecuaciones hay L.I.

$$\begin{pmatrix} 2 & 3 & 2 & 1 \\ 1 & 4 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ No son L.I.}$$

Por lo tanto la ec.  $x + 4y + z + 3t = 0$  no sirve para nada.

$U$  es un subespacio vectorial de  $\mathbb{Z}_5^4$  que viene dada por una ecuación L.I. Por tanto  $\dim U = 4 - 1 = 3$

$$2x = 2y + 3z + 4t.$$

$$y=1, z=0, t=0 \rightarrow x=1$$

$$y=0, z=1, t=0 \rightarrow x=4$$

$$y=0, z=0, t=1 \rightarrow x=2$$

$$B_U = \{(1, 1, 0, 0), (4, 0, 1, 0), (2, 0, 0, 1)\}$$

⑤ Sea  $U = \{(1,1,1,1), (1,2,3,3)\}$  y  $W = \{(x,y,z,t) \in \mathbb{Q}^4 \text{ tq } x+y-z-t=0\}$   
 Calcular una base de  $U + W$

$W$  viene dado por una ecuación, por tanto,  $\dim W = 3$ ,  
 en consecuencia,  $B_W = \{(-1,1,0,0), (1,0,1,0), (1,0,0,1)\}$   
 Por tanto:

$$U + W = \{(1,1,1,1), (1,2,3,3), (-1,1,0,0), (1,0,1,0), (1,0,0,1)\}$$

Ahora triangularizamos:

$$\begin{array}{c} \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 3 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 1 \\ 0 & -1 & 0 & -1 \\ 0 & -1 & -1 & 0 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & -3 & -3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{array} \right) \sim \\ \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & -3 & -3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & -3 & -3 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 3 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & 0 \end{array} \right) \end{array}$$

Por lo tanto:

$$B_{U+W} = \{(1,1,1,1), (0,1,2,2), (0,0,1,2), (0,0,0, -3)\}$$

- ⑥ Dada la aplicación lineal  $f: \mathbb{Z}_5^4 \rightarrow \mathbb{Z}_5^3$  definida por  $f(x, y, z, t) = (x+y+z+t, x+y+z+2t, x+y+z)$ . Calcular una base del núcleo.

$$N(f) = \{(x, y, z, t) \in \mathbb{Z}_5^4 \text{ tq } \begin{cases} x+y+z+t=0 \\ x+y+z+2t=0 \\ x+y+z=0 \end{cases}\}$$

$$\left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 1 & 1 & 0 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\Rightarrow N(f) = \{(x, y, z, t) \in \mathbb{Z}_5^4 \text{ tq } \begin{cases} x+y+z+t=0 \\ t=0 \end{cases}\}$$

Como el núcleo de  $f$  viene dado por dos ecuaciones linealmente independientes, entonces  $\dim N(f) = 4 - 2 = 2$

$$\mathcal{B}_{N(f)} = \{(4, 1, 0, 0), (4, 0, 1, 0)\}$$

$$\begin{matrix} x+t=4 \\ y=4 \\ z=0 \end{matrix}$$

- ⑦ Sea  $U$  el subespacio vectorial de  $\mathbb{Z}_7^3$  generado por  $\{(2, 3, 2), (1, 3, 3)\}$ . ¿Es  $\{(1, 1, 5), (2, 0, 5)\}$  una base de  $U$ .

Como  $\begin{pmatrix} 2 & 3 & 2 \\ 1 & 3 & 3 \end{pmatrix}$  es L.I., es una base de  $U$ . Por lo que  $\dim U = 2$ .

$\begin{pmatrix} 1 & 1 & 5 \\ 2 & 0 & 5 \end{pmatrix}$  son L.I. Para saber si son una base,

$U$  es un subespacio vectorial de  $\mathbb{Z}_7^3$  de dimensión 2, los vectores del conjunto  $\{(1, 1, 5), (2, 0, 5)\}$  son L.I. Por tanto son una base de  $U \Leftrightarrow$  los dos vectores están en  $U$

Para ver si dichos vectores están o no en  $\mathcal{U}$ , calcularé las ecuaciones cartesianas de  $\mathcal{U}$  y vereé si los vectores verifican o no dichas ecuaciones.

$\mathcal{U}$  viene determinado por 1 ecuación que se obtiene al imponer que

$$\text{rang} \begin{pmatrix} 2 & 1 & x \\ 3 & 3 & y \\ 2 & 3 & z \end{pmatrix} = \dim \mathcal{U} = 2$$

Es decir,  $\begin{vmatrix} 2 & 1 & x \\ 3 & 3 & y \\ 2 & 3 & z \end{vmatrix} = 0 \rightarrow 6x + 2y + 2x + x + y + 4z = 0$   
 $\rightarrow 3x + 3y + 3z = 0$   
 $\rightarrow x + y + z = 0$

$\therefore \mathcal{U} = \{(x, y, z) \in \mathbb{Z}^3 : x + y + z = 0\}$

Por tanto  $\{(1, 1, 5), (2, 0, 5)\} \subseteq \mathcal{U}$

Por consiguiente,  $\mathcal{U}$  es un espacio vectorial de dimensión 2 y  $\{(1, 1, 5), (2, 0, 5)\}$  son dos vectores de  $\mathcal{U}$  L.I. En consecuencia  $\{(1, 1, 5), (2, 0, 5)\}$  es una base de  $\mathcal{U}$ .

⑧ Sea  $U$  el subespacio vectorial de  $\mathbb{Z}_5^3$  generado por  $\{(1,1,1,1)\}$  y  $W = \{(x,y,z) \in \mathbb{Z}_5^3 \text{ tq } x+y+z=0\}$

a) ¿Es  $\mathbb{Z}_5^3 = U + W$ ?

$$B_U = \{(1,1,1,1)\} \quad B_W = \{(1,4,0), (1,0,4)\}$$

$$U + W = \langle (1,1,1), (1,4,0), (1,0,4) \rangle$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 4 & 0 \\ 1 & 0 & 4 \end{pmatrix} N \begin{pmatrix} 1 & 1 & 1 \\ 0 & 3 & 4 \\ 0 & 4 & 3 \end{pmatrix} N \begin{pmatrix} 1 & 1 & 1 \\ 0 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

$$B_{U+W} = \{(1,1,1), (0,3,4), (0,0,1)\}$$

$U + W$  es un subespacio vectorial de  $\mathbb{Z}_5^3$  de dimensión 3. Por tanto  $U + W = \mathbb{Z}_5^3$

b) ¿Es  $\mathbb{Z}_5^3 = U \oplus W$ ?

Sabemos que  $\mathbb{Z}_5^3 = U \oplus W \iff$  se verifican las siguientes condiciones:

$$1 - \mathbb{Z}_5^3 = U + W$$

$$2 - U \cap W = \{(0,0,0)\}$$

$$\text{Sabemos que } \dim U + \dim W = \dim(U + W) + \dim(U \cap W).$$

$$\Rightarrow \dim(U \cap W) = 0 \Rightarrow U \cap W = \{(0,0,0)\}$$

Luego se verifican ambas condiciones

⑨ Sea  $U$  el subespacio vectorial de  $\mathbb{Z}^3$  cuyas ecuaciones cartesianas respecto de la base  $B = \{(1,1,1), (1,0,0), (1,1,0)\}$  son :

$$\begin{cases} x + y + z = 0 \\ x + 2y + z = 0 \end{cases}$$

¿ Es  $(0,4,4) \in U$  ?

Calculamos :  $(0,4,4) \equiv_B ($

$$(0,4,4) = a(1,1,1) + b(1,1,0) + c(1,0,0)$$

$$\begin{array}{l} a + b + c = 0 \\ a + b = 4 \\ a = 4 \end{array} \quad || \quad \begin{array}{l} c = 1 \\ a = 4 \\ b = 0 \end{array}$$

Por lo tanto :

$$(0,4,4) \equiv_B (4,0,1)$$

Como  $(4,0,1)$  verifica las ecuaciones, entonces  $(0,4,4) \in U$

(10) Sea  $\bar{U}$  el subespacio vectorial de  $\mathbb{Z}_5^4$  generado por

$\{(1,1,1,1), (0,1,1,1), (0,0,1,1)\}$  y sea

$$W = \{(x, y, z, t) \in \mathbb{Z}_5^4 \mid x+y+z+t=0\}$$

Calcular el cardinal de  $\bar{U} \cap W$

~~Vamos a calcular las ecuaciones cartesianas de  $\bar{U}$~~

Sabemos que  $\dim \bar{U} + \dim W = \dim (\bar{U} + W) + \dim (\bar{U} \cap W)$

$$\begin{array}{c} \parallel \\ 3 \end{array} \quad \begin{array}{c} \parallel \\ 3 \end{array}$$

$$B_W = \{(4,1,0,0), (4,0,1,0), (4,0,0,1)\}$$

$$\bar{U} + W = \langle (1,1,1,1), (0,1,1,1), (0,0,1,1), (4,1,0,0), (4,0,1,0), (4,0,0,1) \rangle.$$

$$\left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 4 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \sim$$

$$\left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{array} \right) \sim \left( \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right) \rightarrow \dim \bar{U} + W = 4$$

Por lo tanto  $\rightarrow \dim (\bar{U} \cap W) = 2$ .

$\bar{U} \cap W$  es un espacio vectorial sobre el cuerpo  $\mathbb{Z}_5$  de dimensión 2, por tanto,  $\bar{U} \cap W$  es isomorfo a  $\mathbb{Z}_5^2$  por consiguiente el cardinal de

$$\bar{U} \cap W \text{ es } 5^2 = \underline{\underline{25}}$$

## Tema 7 : Diagonalización de matrices.

Una matriz diagonal es una matriz cuadrada en la que todos sus valores son cero salvo algunos de la diagonal principal.

Ejemplo:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Una matriz cuadrada  $A$  es diagonalizable si existe una matriz diagonal  $D$  y existe una matriz regular  $P$  tal que  $A = P \cdot D \cdot P^{-1}$

La diagonalización de matrices es útil para el cálculo de potencias grandes de una matriz, ya que si  $A$  es diagonalizable y  $A = P \cdot D \cdot P^{-1}$ , entonces  $A^n = A \cdot A \cdot A \cdots A = P \cdot D \cdot P^{-1} \cdot P \cdot D \cdot P^{-1} \cdots P \cdot D \cdot P^{-1} = P \cdot D \cdot D \cdots D \cdot P^{-1} = P \cdot D^n \cdot P^{-1}$

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}^n = \begin{pmatrix} d_1^n & 0 & 0 \\ 0 & d_2^n & 0 \\ 0 & 0 & d_3^n \end{pmatrix}$$

En adelante,  $A$  será una matriz cuadrada de orden  $n \times n$  con coeficientes en un cuerpo  $K$ .

Un elemento  $\lambda \in K$  diremos que es un valor propio de  $A$  si existe  $(x_1, \dots, x_n) \in K^n \setminus \{0, \dots, 0\}$

taq  $A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda (x_1, \dots, x_n)$ . En tal caso diremos que  $(x_1, \dots, x_n)$  es un vector propio asociado al valor propio  $\lambda$

### \* Teorema :

Un elemento  $\lambda \in K$  es un vector propio de la matriz  $A$  si y solamente si  $|A - \lambda I_n| = 0$  (si el determinante vale cero).

El teorema anterior nos dice que los valores propios de la matriz  $A$ , son las raíces del polinomio  $|A - \lambda I_n| \in K[\lambda]$  que se conoce como

Polinomio característico de la matriz  $A$  y que denotaremos  $P_A(\lambda)$

Notese que el grado  $P_A(\lambda)$  es  $n$ .

### Ejercicio:

Calcula el Polinomio característico y los valores propios de la matriz  $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_{2 \times 2}(\mathbb{R})$

$$\begin{aligned} P_A(\lambda) &= \left| \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right| = \left| \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right| \\ &= \begin{vmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 - 4 = \boxed{\lambda^2 - 2\lambda - 3} \end{aligned}$$

$$\lambda^2 - 2\lambda - 3 = 0 \Rightarrow \lambda = \frac{2 \pm \sqrt{4+12}}{2} = \frac{2 \pm 4}{2} \quad \begin{matrix} 3 \\ -1 \end{matrix}$$

$\boxed{\begin{matrix} \lambda = 3 \\ \lambda = -1 \end{matrix}}$  Valores propios de la matriz.

Una matriz cuadrada diremos que es triangular superior si todos los elementos que hay por debajo de la diagonal principal valen cero:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Una matriz cuadrada diremos que es triangular inferior si todos los elementos que hay por encima de la diagonal, valen cero.

\*Proposición:

- 1) Si  $A$  es una matriz triangular (sup o inf) entonces sus valores propios son justamente los valores que aparecen en la diagonal principal.
- 2) Los valores propios de  $A$  y los de  $A^t$ , coinciden.
- 3) El determinante de  $A$  es cero si y solamente si  $0$  es un valor propio de  $A$ .
- 4) Si  $A$  es regular y  $\lambda$  es un valor propio de  $A$ , entonces  $\lambda^{-1}$  es un valor propio de  $A^{-1}$ .

Si  $\lambda$  es un valor propio de la matriz  $A$ , entonces,

$$V(\lambda) = \{(x_1, \dots, x_n) \in \mathbb{K}^n \text{ tq } (A - \lambda I_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

es  
un subespacio vectorial de  $\mathbb{K}^n$  al que llamaremos  
subespacio vectorial propio asociado al valor propio  $\lambda$

Ejercicio:

Calcular los subespacios vectoriales propios asociados a los valores propios de la matriz  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_{2 \times 2}(\mathbb{R})$

Por el ejercicio anterior, sabemos que los valores propios  $\lambda = -1$  y  $\lambda = 3$ . Por lo tanto:

$$\begin{aligned} V(-1) &= \{(x, y) \in \mathbb{R}^2 \text{ tq } \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\} = \\ &= \{(x, y) \in \mathbb{R}^2 \text{ tq } \begin{cases} 2x + 2y = 0 \\ 2x + 2y = 0 \end{cases}\} \end{aligned}$$

Por tanto  $\dim V(-1) = 1$

$$\text{y } BV(-1) = \{(1, -1)\}$$

$$\begin{aligned} V(3) &= \{(x, y) \in \mathbb{R}^2 \text{ tq } \begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\} = \\ &= \{(x, y) \in \mathbb{R}^2 \text{ tq } \begin{cases} -2x + 2y = 0 \\ 2x - 2y = 0 \end{cases}\} \end{aligned}$$

Por tanto  $\dim V(3) = 1$

$$\text{y } BV(3) = \{(1, 1)\}$$

Sea  $\lambda_1, \dots, \lambda_k$  los valores propios de la matriz  $A$ , entonces a la multiplicidad de la raíz  $\lambda_i$  de polinomio  $P_A(\lambda)$  la llamaremos la multiplicidad algebraica del valor propio  $\lambda_i$ , y a la dim  $V(\lambda_i)$  la llamaremos la multiplicidad geométrica del valor propio  $\lambda_i$ .

#### • Ejemplo :

Calcular la multiplicidad algebraica y la multiplicidad geométrica de la matriz  $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ .

Sabemos por los ejercicios anteriores que

$P_A(\lambda) = \lambda^2 - 2\lambda - 3$  y que los valores propios son  $\lambda = -1$  y  $\lambda = 3$ .

También sabemos que  $\dim V(-1) = 1$  y  $\dim V(3) = 1$ .

Por tanto, los dos valores propios tienen multiplicidad geométrica 1

$$P_A'(\lambda) = 2\lambda - 2$$

$$P_A'(-1) = -4 \neq 0$$

$$P_A'(3) = 4 \neq 0$$

Tienen multiplicidad algebraica 1

#### \* Proposición :

La multiplicidad geométrica de un valor propio siempre es  $\leq$  que su multiplicidad algebraica.

#### • Criterio de diagonalización

Sea  $A \in \text{Mat}_{n \times n}(K)$ , entonces  $A$  es diagonalizable si y solamente si la suma de las multiplicidades algebraicas de sus valores propios es igual a  $n$  y además para cada valor propio, coincide su multiplicidad algebraica y su mult. geométrica.

Ejercicio:

Es  $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$  diagonalizable?

Sí, ya que la suma de las mult. algebraicas de sus valores propios es 2 que coincide con el tamaño y además, cada valor propio tiene mult. algebraica y geométrica 1.

\* COROLARIO

Si  $A \in M_{n \times n}(\mathbb{K})$  tiene n valores propios distintos, entonces la matriz A es diagonalizable

\* COROLARIO

Toda matriz cuadrada y simétrica con coeficiente en  $\mathbb{R}$  es diagonalizable.

→ Método para diagonalizar una matriz.

Sea  $A \in M_{n \times n}(\mathbb{K})$ :

- 1) Calculamos  $P_A(\lambda)$ , sus raíces  $\lambda_1, \dots, \lambda_k$  y sus multiplicidades algebraicas  $m_1, \dots, m_k$
- 2) Si  $m_1 + m_k \neq n$ , entonces la matriz no es diagonalizable.

3) Para cada  $\lambda_i$  calculamos su multiplicidad geométrica.  
 Si para algún  $i$  no coincide su mult. algebraica  
 y su mult. geométrica, entonces la matriz  $A$   
 no es diagonalizable.

4) La matriz  $A$  es diagonalizable, además  $A \overset{?}{=} P \cdot D \cdot P^{-1}$   
 donde  $D$  es la matriz diagonal que contiene en la  
 diagonal  $\lambda_1$ ,  $m_1$  veces,  $\lambda_2$   $m_2$  veces, ...,  $\lambda_k$   $m_k$  veces.  
 y la matriz  $P$  se construye colocando por  
 columnas una base de  $V(\lambda_1), V(\lambda_2), \dots, V(\lambda_k)$

Ejercicio:

$$\text{Diagonalizar } A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_{2 \times 2}(\mathbb{R})$$

$$D = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Ejercicio:

$$\text{Diagonalizar, si es posible, la matriz } A = \begin{pmatrix} 4 & 2 & 5 \\ 6 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in M_{3 \times 3}(\mathbb{Z}_7)$$

$$P_A(\lambda) = \begin{vmatrix} 4-\lambda & 2 & 5 \\ 6 & 1-\lambda & 1 \\ 0 & 0 & 2-\lambda \end{vmatrix} = (2-\lambda)(1-\lambda)(4-\lambda) - 12(2-\lambda)$$

$$= 6\lambda^3 + 5\lambda + 5$$

$\lambda = 2$  y  $\lambda = 3$  son las raíces de  $P_A(\lambda)$   
 y por tanto, 2 y 3 son los valores propios  
 de la matriz  $A$

Vamos a calcular la multiplicidad algebraica de  
 los valores propios

$$P_A'(\lambda) = 4\lambda^2 + 5 \quad P_A'(2) = 0 \quad P_A'(3) = 6 \neq 0$$

$$P_A''(\lambda) = \lambda \quad P''(2) = 2 \neq 0$$

$$\begin{aligned} \text{multip. algebraica } 3 &= 1 \\ &2 = 2 \end{aligned}$$

La suma de las mult. algebraicas es 3 = tamaño matriz. seguimos.

$$V(2) = \left\{ (x, y, z) \in \mathbb{Z}_7^3 \text{ tq } \begin{pmatrix} 2 & 2 & 5 \\ 6 & 6 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} =$$

$$= \left\{ (x, y, z) \in \mathbb{Z}_7^3 \text{ tq } \begin{array}{l} 2x + 2y + 5z = 0 \\ 6x + 6y + z = 0 \end{array} \right\}$$

Por lo tanto dim  $V(2) = 2$

multip. geométrica = 2

Pues coincide con la algebraica, seguimos.

$$B_{V(2)} = \{(1, 0, 1), (0, 1, 1)\}$$

$$V(3) = \left\{ (x, y, z) \in \mathbb{Z}_7^3 \text{ tq } \begin{pmatrix} 1 & 2 & 5 \\ 6 & 5 & 1 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} =$$

$$\left\{ (x, y, z) \in \mathbb{Z}_7^3 \text{ tq } \begin{array}{l} x + 2y + 5z = 0 \\ 6x + 5y + z = 0 \\ 6z = 0 \end{array} \right\}$$

Por lo tanto para saber cuántas ecuaciones L.I triangulizamos

$$\begin{pmatrix} 1 & 2 & 5 \\ 6 & 5 & 1 \\ 0 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{array}{l} \text{Por lo tanto} \\ \text{dim } V(3) = 1 \end{array}$$

multip. geométrica = 1

Pues coincide con la algebraica, seguimos

$$B_{V(3)} = \{(5, 1, 0)\}$$

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

# PRACTICAS 12/01/16

•) Dado el sistema de ecuaciones con coeficientes en  $\mathbb{Z}_5$

$$\begin{cases} 2x + y + 4z = 3 \\ x + 2y + az = 4 \\ 3x + (a+2)y + 2z = 2 \end{cases}$$

Discútelo según el valor de  $a$ . Si para  $a=4$  es compatible, resólvelo.

$$\left| \begin{array}{ccc|c} 2 & 1 & 4 \\ 1 & 2 & a \\ 3 & a+2 & 2 \end{array} \right| = 3a(1+a)$$

Para  $a=0 \Rightarrow$  Incompatible

Para  $a=4 \Rightarrow$  Comp. I indeterminado.

Vamos a resolverlo

para  $a=4$

$$\left( \begin{array}{ccc|c} 2 & 1 & 4 & 3 \\ 1 & 2 & 4 & 4 \\ 3 & 1 & 2 & 2 \end{array} \right) \sim \left( \begin{array}{ccc|c} 1 & 2 & 4 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 1 & 2 & 2 \end{array} \right) \sim \left( \begin{array}{ccc|c} 1 & 2 & 4 & 4 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

$$\begin{cases} 2x + y + 4z = 4 \\ 2y + z = 0 \end{cases}$$

$$\begin{cases} y = \alpha \\ z = 3\alpha \end{cases} \quad ||$$

$$\begin{cases} 2x + \alpha + 2\alpha = 3 \\ x = (3+2\alpha)/3 \end{cases}$$

•) Calcula en  $\mathbb{R}^4$   $U \cap W$

$$1. U = \{(a, b, -b, a) / a, b \in \mathbb{R}\}$$

$$W = \{(a, b, 0, c) / a, b, c \in \mathbb{R}\}$$

Son ecuaciones  
paramétricas

$$2. U = \begin{cases} x_1 = \lambda \\ x_2 = 0 \\ x_3 = \lambda + \mu \\ x_4 = \lambda + \mu + \gamma \end{cases} \quad W = \begin{cases} x_1 = \lambda + \mu + \gamma \\ x_2 = \lambda + \mu \\ x_3 = 0 \\ x_4 = \lambda \end{cases}$$

$$U = \langle (1, 0, 0, 1), (0, 1, -1, 0) \rangle$$

$$W = \langle (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 0, 1) \rangle$$

$$(x, y, z, t) \in U \Leftrightarrow$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ x & y & z & t \end{pmatrix} \text{ matriz de rango 2}$$

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ x & y & z \end{vmatrix} = 0 \quad \text{y} \quad \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ x & y & t \end{vmatrix} = 0$$

$$(x, y, z, t) \in W \Leftrightarrow \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ x & y & z & t \end{vmatrix} = 0$$

$$\rightarrow U = \begin{cases} y + z = 0 \\ -x + t = 0 \end{cases}$$

$$\rightarrow W = \{z = 0\}$$

$$|| \quad U \cap W = \begin{cases} y + z = 0 \\ -x + t = 0 \\ z = 0 \end{cases}$$

## Tema 8: "Combinatoria"

La combinatoria es la técnica de saber cuántos elementos tiene un conjunto sin necesidad de contarlos uno por uno.

\* Principio de inclusión - exclusión para dos conjuntos

Si  $A_1$  y  $A_2$  son conjuntos, entonces, el cardinal de  $A_1 \cup A_2$

$$\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#A_1 \cap A_2$$

Ejercicio:

Cuántos nº enteros entre 1 y 100 son múltiplos de 2 o de 3

$$A_1 = \{x \in \{1, \dots, 100\} \mid x \text{ es múltiplo de } 2\}$$

$$A_2 = \{x \in \{1, \dots, 100\} \mid x \text{ es múltiplo de } 3\}$$

La solución del problema es el conjunto  $\#A_1 \cup A_2$ :

$$\#A_1 + \#A_2 - \#A_1 \cap A_2$$

$$\begin{array}{r} 50 \\ 33 \\ \hline \end{array}$$

$$\begin{array}{r} 11 \\ \hline \end{array}$$

$$\begin{aligned} A_1 \cap A_2 &= \{x \in \{1, \dots, 100\} \mid x \text{ es múlt. de } 6\} \\ &= 16 \end{aligned}$$

$$50 + 33 - 16 = \boxed{67}$$

\* Principio de inclusión-exclusión general.

Si  $A_1, A_2, \dots, A_n$  son conjuntos, entonces

$$\#(A_1 \cup A_2 \cup \dots \cup A_n) = \sum_{i=1}^n \#A_i - \sum_{1 \leq i_1 \leq i_2 \leq n} \#A_1 \cap A_2 + \dots +$$
$$+ \sum_{\substack{(1) \\ 1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n}}^{K+1} \#A_1 \cap A_2 \cap \dots \cap A_k + \dots$$
$$+ (-1)^{K+1} \#(A_1 \cap A_2 \cap \dots \cap A_n) +$$

NOTA: El principio anterior quiere decir lo siguiente

$$1) \#A_1 \cup A_2 \cup A_3 = \#A_1 + \#A_2 + \#A_3 - \#A_1 \cap A_2 - \#A_1 \cap A_3 - \#A_2 \cap A_3$$
$$+ \#A_1 \cap A_2 \cap A_3$$

$$2) \#A_1 \cup A_2 \cup A_3 \cup A_4 = \#A_1 + \#A_2 + \#A_3 + \#A_4 - \#A_1 \cap A_2 -$$
$$- \#A_1 \cap A_3 - \#A_1 \cap A_4 - \#A_2 \cap A_3 -$$
$$- \#A_2 \cap A_4 - \#A_3 \cap A_4 + \#A_1 \cap A_2 \cap A_3 +$$
$$+ \#A_1 \cap A_2 \cap A_4 + \#A_1 \cap A_3 \cap A_4 +$$
$$+ \#A_2 \cap A_3 \cap A_4 - \#A_1 \cap A_2 \cap A_3 \cap A_4$$

Ejercicio:

cuántos n° entre 1 y 100 son múltiplos de 2, de 3 o de 5?

$$A_1 = \{x \in \{1, \dots, 100\} \mid x \text{ es múlt. de } 2\}$$

$$A_2 = \{x \in \{1, \dots, 100\} \mid x \text{ es múlt. de } 3\}$$

$$A_3 = \{x \in \{1, \dots, 100\} \mid x \text{ es múlt. de } 5\}$$

la solución es  $\#A_1 \cup A_2 \cup A_3$

$$\Rightarrow \#A_1 + \#A_2 + \#A_3 - \#A_1 \cap A_2 - \#A_1 \cap A_3 - \#A_2 \cap A_3 + \#A_1 \cap A_2 \cap A_3$$
$$\begin{array}{ccccccccc} " & " & " & " & " & " & " & " \\ 50 & 33 & 20 & 16 & 10 & 8 & 6 & 3 \end{array}$$

$$106 - 32 = 74$$

## \* Principio del complementario

$$\text{Si } A \subseteq X \Rightarrow \#(X \setminus A) = \#X - \#A$$

Ejercicio:

¿Cuántos nº de tres cifras no son múltiplos ni de 3 ni de 7?

$X = \{ \text{números de 3 cifras} \}$

$A = \{ x \in X \text{ tq } x \text{ es múlt. de } 3 \}$

$B = \{ x \in X \text{ tq } x \text{ es múlt. de } 7 \}$

La solución es  $\#(X \setminus (A \cup B))$

$$\#(X \setminus (A \cup B)) = \#X - \#(A \cup B) = \#X - (\#A + \#B - \#A \cap B)$$

$\begin{matrix} \#A \\ 900 \end{matrix} \quad \begin{matrix} \#B \\ 300 \end{matrix} \quad \begin{matrix} \#A \cap B \\ 128 \end{matrix} \quad \begin{matrix} \#(X \setminus (A \cup B)) \\ 43 \end{matrix}$

$$900 - (300 + 128 - 43) = 515$$

## \* Principio del producto

Si  $A_1, A_2, \dots, A_n$  son conjuntos,  $\Rightarrow \#(A_1 \times A_2 \times \dots \times A_n) =$

$$\#A_1 \cdot \#A_2 \cdot \dots \cdot \#A_n$$

Ej:

Ejercicio:

La placa de matrícula de vehículos de cierto país consta de 4 letras (elegidas entre 25) seguidas de 3 números (de 10 posibles). ¿Cuántas placas de matrículas distintas pueden formarse?

Sea  $L$  el conjunto de letras y  $N$  el conjunto de números, dar una matrícula es lo mismo que dar un elemento de  $L \times L \times L \times L \times N \times N \times N$

$$25^4 \cdot 10^3 =$$

Si  $q \in \mathbb{Q}$ , denotaremos  $\lfloor q \rfloor = \text{máximo } \{z \in \mathbb{Z} \mid q \leq z\}$  y  $\lceil q \rceil = \text{mínimo } \{z \in \mathbb{Z} \mid z \leq q\}$

Ejemplo:

$$\lfloor 6.3 \rfloor = 6 \quad \lceil 6.3 \rceil = 7$$

\*Principio de la caja (o Dirichlet)

Si se distribuyen  $n$  objetos en  $K$  cajas, entonces existe una caja que contiene al menos

$\lceil \frac{m}{K} \rceil$  objetos, y existe otra caja que contiene al menos  $\lfloor \frac{m}{K} \rfloor$

Ejercicio:

¿Cuál es el mínimo número de alumnos que debe tener una asignatura para poder asegurar que al menos 6 alumnos van a obtener la misma calificación?  
Se califican {0, 1, 2, ..., 10}

$$\lceil \frac{56}{11} \rceil = 6$$

### \* Variaciones simples

Sea  $A$  un conjunto con  $m$  elementos. Una  $K$ -tupla  $(a_1, a_2, \dots, a_K)$  diremos que es simple si ~~si~~  
 $\#\{a_1, \dots, a_K\} = K$

Ejercicios

¿Cuántas  $K$ -tuplas simples podemos formar con el conjunto  $A$ ?

• Si  $m < K$ , ninguno

• Si  $m \geq K$ ,  $V_{m,K} = \frac{m!}{(m-K)!}$

Variaciones de  $m$  elementos  
tomados de  $K$  en  $K$

El número anterior también indica el nº de aplicaciones inyectivas que hay de un conjunto de  $K$  elementos en un conjunto de  $m$  elementos

Ejercicio:

- 1) ¿De cuántos no de 3 cifras distintas podemos formar con los dígitos 5, 6, 7, 8 y 9

$$V_{5,3} = \frac{5!}{(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{2} = 60 //$$

$$\overline{5} \cdot \overline{4} \cdot \overline{3} = 60 //$$

- 2) ¿De cuántas formas se pueden sentar cuatro personas en un microbus de 15 plazas?

$$V_{15,4} = \frac{15!}{(15-4)!} = 15 \cdot 14 \cdot 13 \cdot 12$$

$$\frac{P_1}{15} \quad \frac{P_2}{14} \quad \frac{P_3}{13} \quad \frac{P_4}{12}$$

- 3) ¿De cuántos no de 3 cifras distintas podemos formar con los dígitos 0, 1, 2, 3 y 4

$$V_{5,3} - V_{4,2} = \frac{5!}{2!} - \frac{4!}{2!} = 5 \cdot 4 \cdot 3 - 4 \cdot 3 = 48 //$$

$$\overline{4} \quad \overline{4} \quad \overline{3} = 48$$

## \* Variaciones con repetición

Sea  $A$  un conjunto con  $m$  elementos, ¿cuántas  $K$ -tuplas podemos formar con los elementos de  $A$ .

$$V_{m,K}^R = m^K$$

El número anterior también indica el número de aplicaciones que hay de un conjunto de  $K$  elementos en un conjunto de  $m$  elementos.

Ejercicio:

¿Cuántos números de 3 cifras podemos construir utilizando los dígitos 1 y 2?

$$\overline{2} \cdot \overline{2} \cdot \overline{2} = 8$$

¿Cuántos números de tres cifras podemos construir utilizando los dígitos 0, 1, 2?

$$\overline{3} \cdot \overline{3} \cdot \overline{3} = 27$$

¿Cuántos polinomios tiene  $\mathbb{Z}_5[x]$  de grado  $\leq$  que 2?

$$\frac{x^2}{5} + \frac{x}{5} + \frac{1}{5} = 125$$

¿Cuántos polinomios de grado 2 hay en  $\mathbb{Z}_5[x]$ ?

$$\frac{x^2}{4} + \frac{x}{5} + \frac{1}{5} = 100$$

¿Cuántos polinomios cuadráticos de grado 2 tiene  $\mathbb{Z}_5[x]$ ?

$$\frac{x^2}{1} + \frac{x}{5} + \frac{1}{5} = 25$$

¿Cuántos polinomios monómico de grado  $\leq 2$  tiene  $\mathbb{Z}_5[x]$ ?

$$\begin{aligned} - \frac{x^2}{1} + - \frac{x}{5} + \frac{1}{5} &= 25 \\ \frac{1x}{1} + \frac{-}{5} &= 5 \\ \frac{-1}{1} &= 1 \end{aligned} \quad \left. \begin{array}{l} 30 \\ 31 \end{array} \right\}$$

~~abreviatura~~

### \* Permutaciones simples

Sea  $A$  un conjunto con  $m$  elementos, ¿cuántas  $m$ -tuplas simples podemos formar con los elementos de  $A$ ?

$$P_m = m!$$

El número anterior también indica el número de aplicaciones biyectivas que hay de un conjunto de  $m$  elementos en un conjunto de  $m$  elementos. Es además un caso particular de variación simple, cuando  $m = k$ .

Ejercicio:

¿De cuántas formas distintas se pueden colocar 5 libros en una estantería?

$$\frac{5}{ } \cdot \frac{4}{ } \cdot \frac{3}{ } \cdot \frac{2}{ } \cdot \frac{1}{ } = 5!$$

\* Permutaciones con repetición

Sea  $A$  un conjunto con  $r$  elementos y  $\alpha_1, \alpha_2, \dots, \alpha_r$  enteros positivos tales que  $\alpha_1 + \alpha_2 + \dots + \alpha_r = m$ . Cuántas  $n$ -tuplas podemos formar con los elementos del conjunto  $A$  de manera que una coordenada se repita  $\alpha_1$  veces, otra coordenada se repita  $\alpha_2$  veces, ... y otra coordenada se repita  $\alpha_r$  veces.

$$P_m^{\alpha_1, \alpha_2, \dots, \alpha_r} = \frac{m!}{\alpha_1! \cdot \alpha_2! \cdot \dots \cdot \alpha_r!}$$

Ejemplo:

¿Cuántos nros de 16 cifras se pueden formar con 3 unos, 5 doses y 8 treses.

$$P_{16}^{3, 5, 8} = \frac{16!}{3! \cdot 5! \cdot 8!}$$

Ejercicio:

¿De cuántas maneras de 16 cifras se pueden formar con 3 unos, 5 doses, 6 treses y 2 ceros?

$$P_{16}^{3,5,6,2} - P_{15}^{3,5,6,1}$$

¿De cuántas formas podemos ordenar las letras de la palabra menotretó?

$$P_9^{2,2,2,1,1,1}$$

### \* Combinaciones simples

Sea  $A$  un conjunto con  $m$  elementos, ¿cuántos subconjuntos de cardinal  $K$  tiene  $A$ ?

$$C_{m,K} = \binom{m}{K} = \frac{m!}{K!(m-K)!}$$

Ejercicio:

Se extraen 5 cartas de una baraja de 40, ¿cuántas jugadas diferentes pueden obtenerse?

$$E_{40,5} = \binom{40}{5} = \frac{40!}{5! 35!}$$

Ejercicio:

Cierto club de portavoz está formado por 15 mujeres y 12 hombres. Un comité consta\* de 4 personas.

a) ¿Cuántos comités pueden formarse?

$$C_{27,4} = \binom{27}{4} = \frac{27!}{4! \cdot 23!}$$

b) ¿Cuántos comités se pueden formar que contengan exactamente dos mujeres.

dos mujeres  
dos hombres

$$\binom{15}{2} \binom{12}{2} \Rightarrow \binom{15}{2} \cdot \binom{12}{2}$$

Ejercicio:

c) De cuántas formas se puede acertar exactamente 9 resultados en una quiniela de 14?

$$\binom{14}{9} \cdot 2^5$$

\* Combinaciones con repetición

Disponemos de bolas de 12 colores. (un nº ilimitado de cada una de ellas) ¿Cuántas cajas distintas de  $K$  bolas podemos formar?

$$C_{m,K}^R = \binom{m+K-1}{K}$$

El nº anterior también indica el cardinal del conjunto  $\{(x_1, x_2, \dots, x_n) \in \mathbb{N}^m \text{ tq } x_1 + x_2 + \dots + x_m = K\}$

### Ejercicio:

- 1) En una heladería se sirven helados de 20 sabores diferentes, ¿cuántas compras distintas de 12 helados podemos efectuar?

$$C_{20,12}^R = \binom{31}{12}$$

- 2) Se lanzan 3 dados simultáneamente, ¿cuántas jugadas distintas podemos obtener?

$$C_{6,3}^R = \binom{8}{3}$$

- 3) Calcular el cardinal del conjunto

$$\{(x_1, x_2, x_3, x_4) \in \mathbb{N}^4 \text{ tq } x_1 + x_2 + x_3 + x_4 = 24 \text{ y } x_i \geq 2 \text{ para todo } i \in \{1, 2, 3, 4\}\}$$

~~Clas.~~ 24

Este conjunto tiene el mismo cardinal que el conjunto

$$\{(x_1, x_2, x_3, x_4) \in \mathbb{N}^4 \text{ tq } x_1 + x_2 + x_3 + x_4 = 16 \text{ y } x_i \geq 0 \text{ y } i \in \{1, 2, 3, 4\}\}$$

$$C_{4,16}^R = \binom{19}{16}$$

## \* Regla del binomio de Newton.

Sea  $A$  un anillo comutativo,  
y  $a, b \in A$ .

Entonces,  $\forall n \in \mathbb{N}$  se verifica que  $(a+b)^m =$

$$\sum_{k=0}^m \binom{m}{k} a^k \cdot b^k$$

Ejercicio:

Calcular utilizando la fórmula del binomio de Newton

$$(a+b)^3 = \binom{3}{0} a^0 \cdot b^{3-0} + \binom{3}{1} a^1 \cdot b^{3-1} + \binom{3}{2} a^2 b^{3-2}$$

$$+ \binom{3}{3} a^3 b^{3-3} = b^3 + 3ab^2 + 3a^2b + a^3$$