ÁLGEBRA LINEAL Y ESTRUCTURAS MATEMÁTICAS

Apuntes anotados

Eduardo Rodríguez Hoces

Índice

1 Conjuntos y Aplicaciones

La teoría de conjuntos es la fundación de la matemática abstracta, por lo que es uno de los temas que debemos de dar antes de continuar con el resto de temas. Aunque las definiciones de los conceptos de teoría de conjuntos que se dan en este tema pueden ser poco rigurosas, siguen siendo suficientes para el contenido de este curso.
Este tema consiste en una introducción a la teoría de conjuntos, las relaciones dentro de un conjunto y aplicaciones de un conjunto en otro.

Un conjunto es una colección de objetos a los que se llama elementos del conjunto. Si x es un elemento de un conjunto A entonces se dice que x pertenece a A y se denota $x \in A$. [1]
Diremos que un conjunto A es un subconjunto de otro conjunto B, denotado $A \subseteq B$ si todos los elementos de A también están en B, es decir, si para todo $x \in A$ se cumple que $x \in B$.
Sean A y B dos conjuntos. Si se cumple que $A \subseteq B$ y $B \subseteq A$, entonces se dice que A y B son iguales ($A = B$). Existe un conjunto $\emptyset$ que no tiene elementos, o sea, $\emptyset = \{\}$. A $\emptyset$ se le llama el conjunto vacío y es subconjunto de todos los conjuntos.
Ejemplo: Sean los conjuntos $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4\}$ y $C = \{2, 4, 6\}$. Entonces se cumple lo siguiente:

- $1 \in A$, pero $6 \notin A$.
- $B \subseteq A$, pero $C \nsubseteq A$.
- $\emptyset \subseteq A$ y $\emptyset \subseteq \emptyset$, pero $\emptyset \notin A$, $\emptyset \notin \emptyset$ y $\emptyset \neq \{\emptyset\}$.
- $B = \{4, 2\}$ y $\{1\} = \{1, 1, 1, 1\}$, pero $1 \neq \{1\}$.
- $\{1, 2, 3\} = \{3, 2, 1, 1, 2, 1, 3, 2, 1, 1 + 1\}$ [2]

1.1 Operaciones con conjuntos

Sean A y B dos conjuntos.

1. **Intersección de conjuntos:**
   La intersección de A y B es $A \cap B = \{x \text{ t. q. } x \in A \text{ y } x \in B\}$[3]

2. **Unión de conjuntos:**
   La unión de A y B es $A \cup B = \{x \text{ t. q. } x \in A \text{ ó } x \in B\}$

3. **Diferencia de conjuntos:**
   La diferencia de A y B es $A \setminus B = \{x \in A \text{ t. q. } x \notin B\}$

4. **Conjunto partes:**
   El conjunto partes de A es $\mathcal{P}(A) = \{X \text{ t. q. } X \subseteq A\}$

[1] A los elementos de un conjunto se les encierra entre llaves y se les separa con comas. Por ejemplo, si A es el conjunto con los elementos 1, 2, 3, a, b y c, se escribe $A = \{1, 2, 3, a, b, c\}$

[2] Es decir, el orden de los elementos en un conjunto no importa, y si dos elementos dentro de un conjunto son iguales entonces son el mismo elemento y cuentan como uno.

[3] "t.q." es abreviación para "tal que". Entonces, $\{x \text{ t. q. } x \in A \text{ y } x \in B\}$ se refiere al conjunto de todos los elementos x tales que x pertenece a A y x pertenece a B. Esta notación se mantendrá a lo largo de los apuntes.

5. **Producto cartesiano de dos o más conjuntos:**
   El producto cartesiano de A y B es $A \times B = \{(a,b) \text{ t. q. } a \in A, b \in B\}$[4]. A los elementos de $A \times B$ se les llama pares ordenados.
   Sean $A_1, A_2, A_3, \ldots, A_n$ conjuntos. Entonces el producto cartesiano de todos ellos es

$$A_1 \times A_2 \times A_3 \times \cdots \times A_n = \Big\{(a_1, a_2, a_3, \ldots, a_n) \text{ t. q. } a_1 \in A_1, a_2 \in A_2, a_3 \in A_3, \ldots, a_n \in A_n\Big\}$$

   A los elementos de $A_1 \times A_2 \times A_3 \times \cdots \times A_n$ se les llama n-tuplas.[5]
   Al conjunto $A \times A \times A \times \overset{n \text{ veces}}{\cdots} \times A$ lo denotaremos A^n.

Ejemplo: Sean los conjuntos $A = \{1,2,3\}$, $B = \{2,3,4,5\}$ y $C = \{4,5,6\}$. Entonces se cumple lo siguiente:

- $A \cap B = \{2,3\}$, $A \cap C = \emptyset$ y $A \cup B = \{1,2,3,4,5\}$.
- $A \setminus B = \{1\}$ y $B \setminus A = \{4,5\}$.
- $\mathcal{P}(A) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\Big\}$.
- $(1,2) \in A \times B$ y $(1,6) \in A \times C$, pero $(1,6) \notin A \times B$.
- $(1,2,3) \notin A \times B \times C$, $(1,2,1) \in A^3$ y $(1,2,4) \notin A^3$

El cardinal de un conjunto es el número de elementos distintos de dicho conjunto. Si A es un conjunto entonces denotaremos al cardinal de A como $\#A$.
Ejemplo: $\#\{1,3,5,7\} = 4$ y $\#\mathbb{N} = \#\{0,1,2,3,4,\ldots\}$[6] $= \infty$

Proposición 1. [7]

- Si A es un conjunto entonces $\#\mathcal{P}(A) = 2^{\#A}$
- Si $A_1, A_2, \ldots, A_n$ son conjuntos entonces $\#(A_1 \times A_2 \times \cdots \times A_n) = \#A_1 \cdot \#A_2 \ldots \#A_n$

Ejercicio: Sea $A = \{1,2,3,4\}$. Calcular el cardinal de $\mathcal{P}(A)$.

$\#\mathcal{P}(A) = 2^{\#A} = 2^4 = 16$ $\square$

Ejercicio: Sean $A = \{1,2,3\}$, $B = \{2,3,4,5\}$ y $C = \{4,5,6\}$. Calcular el cardinal de $A \times B \times C$ y el de A^4.

Nótese que $\#A = 3 = \#C$ y $\#B = 4$. Entonces
$\#(A \times B \times C) = \#A \cdot \#B \cdot \#C = 3 \cdot 4 \cdot 3 = 36$
y $\#A^4 = \#(A \times A \times A \times A) = (\#A)^4 = 3^4 = 81$. $\square$

[4] Nótese que, generalmente, $A \times B \neq B \times A$
[5] A los elementos del producto cartesiano de tres conjuntos se les llama ternas, no 3-tuplas.
[6] A lo largo de esta asignatura se toma el conjunto de los números naturales a partir del cero.
[7] Una proposición es una declaración menos importante que un teorema.

1.2 Aplicaciones entre conjuntos

Sean A y B dos conjuntos. Una aplicación f de A en B, denotada $f : A \longrightarrow B$, es una correspondencia que a todo elemento de A le asocia un único elemento de B. Si $f : A \longrightarrow B$ es una aplicación y $a \in A$, el elemento de B que f asocia a a se denota $f(a)$ y se le llama la imagen de a.

Ejemplo: Sean los conjuntos $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c\}$.

- La correspondencia $f : A \longrightarrow B$ tal que $f(1) = a, f(2) = b$ ó $f(2) = c, f(3) = a, f(4) = a$ no es aplicación porque al elemento $2 \in A$ le asocia dos elementos de B distintos.
- La correspondencia $f : A \longrightarrow B$ tal que $f(1) = a, f(2) = b, f(4) = b$ no es aplicación porque al elemento $3 \in A$ no le asocia ningún elemento.
- La correspondencia $f : A \longrightarrow B$ tal que $f(1) = a, f(2) = b, f(3) = a, f(4) = b$ es una aplicación.

Sea $f : A \longrightarrow B$ una aplicación. A los conjuntos A y B se les llama el dominio y el codominio de f respectivamente. Además, la imagen de f se define como $\mathrm{Im}(f) = \{f(a) \text{ t. q. } a \in A\}$.

Ejemplo: Dada la aplicación $f : \{1, 2, 3, 4\} \longrightarrow \{a, b, c\}$ tal que $f(1) = a, f(2) = b, f(3) = a, f(4) = b$ tenemos que $\mathrm{Im}(f) = \{a, b\}$.

Ejercicio: Dada la aplicación $f : \mathbb{N} \longrightarrow \mathbb{Q}$ definida por $f(n)) = 2n + 1$, calcular $\mathrm{Im}(f)$

$\mathrm{Im}(f) = \{f(n) \text{ t. q. } n \in \mathbb{N}\} = \{2n + 1 \text{ t. q. } n \in \mathbb{N}\} = \{1, 3, 5, 7, 9, \dots\} =$
$\{n \in \mathbb{N} \text{ t. q. } n \text{ es impar}\}$ □

1.3 Tipos especiales de aplicaciones

Una aplicación $f : A \longrightarrow B$ se dice que es:

- inyectiva si, dados $x, y \in A$, $f(x) = f(y)$ implica que $x = y$.
- sobreyectiva si $\mathrm{Im}(f) = B$.
- biyectiva si es inyectiva y sobreyectiva.

Ejemplo:

- La aplicación $f : \{1, 2, 3\} \longrightarrow \{a, b, c, d\}$ tal que $f(1) = a, f(2) = c, f(3) = d$ es inyectiva pero no es sobreyectiva porque no hay ningún $x \in \{1, 2, 3\}$ tal que $f(x) = b$.
- La aplicación $f : \{1, 2, 3, 4\} \longrightarrow \{a, b, c\}$ tal que $f(1) = a, f(2) = c, f(3) = b, f(4) = c$ es sobreyectiva pero no inyectiva porque $f(2) = f(4) = c$.
- La aplicación $f : \{1, 2, 3\} \longrightarrow \{a, b, c\}$ tal que $f(1) = b, f(2) = c, f(3) = a$ es biyectiva.
- La aplicación $f : \{1, 2, 3, 4\} \longrightarrow \{a, b, c\}$ tal que $f(1) = a, f(2) = b, f(3) = a, f(4) = c$ no es inyectiva ni sobreyectiva.

Ejercicio: Demostrar que la aplicación $f : \mathbb{N} \longrightarrow \mathbb{Z}$ definida por $f(n) = n-5$ es inyectiva pero no sobreyectiva.

Dados $x, y \in \mathbb{N}$, si $f(x) = f(y)$ entonces $x - 5 = y - 5$. Al sumar 5 a ambos lados obtenemos que $x = y$. Por tanto f es inyectiva.
Además, no existe ningún $n \in \mathbb{N}$ tal que $n - 5 = -6$. Por tanto $-6 \notin \text{Im}(f)$, así que $\text{Im}(f) \neq \mathbb{Z}$ y f no es sobreyectiva. $\square$

Ejercicio: Demostrar que la aplicación $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definida por $f(x) = x^2$ no es inyectiva ni sobreyectiva.

$f(1) = f(-1) = 1$, así que f no es inyectiva.
Por otra parte, no existe ningún $x \in \mathbb{Z}$ tal que $x^2 = 2$. Por tanto $2 \notin \text{Im}(f)$, así que $\text{Im}(f) \neq \mathbb{N}$ y f no es sobreyectiva. $\square$

1.4 Composición de aplicaciones

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos aplicaciones. La aplicación composición de f y g es otra aplicación $g \circ f : A \longrightarrow C$ definida por $\Big(g \circ f\Big)(a) = g\big(f(a)\big)$.
Ejemplo: Sean las aplicaciones $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definida por $f(x) = x^2$ y $g : \mathbb{N} \longrightarrow \mathbb{Q}$ definida por $g(n) = \dfrac{2n+1}{3}$. Entonces $g \circ f : \mathbb{Z} \longrightarrow \mathbb{Q}$ es otra aplicación definida por

$$\Big(g \circ f\Big)(x) = g\big(f(x)\big) = g(x^2) = \frac{x^2+1}{3}$$

Proposición 2. La composición de funciones es asociativa y no conmutativa.

Nota: Decir que la composición de aplicaciones es asociativa es equivalente a decir que si $f : A \longrightarrow B$, $g : B \longrightarrow C$ y $h : C \longrightarrow D$ son aplicaciones entonces $(h \circ g) \circ f = h \circ (g \circ f) = h \circ g \circ f$.
Decir que la composición de aplicaciones es no conmutativa es equivalente a decir que si $f : A \longrightarrow A$ y $g : A \longrightarrow A$ son aplicaciones entonces, en general, $f \circ g \neq g \circ f$.
Sea A un conjunto. La aplicación identidad en A es la aplicación $1_A : A \longrightarrow A$ definida por $1_A(a) = a$ para todo $a \in A$.

Proposición 3. Si $f : A \longrightarrow B$ es una aplicación biyectiva, entonces existe una aplicación única $g : B \longrightarrow A$ t. q. $g \circ f = 1_A$ y $f \circ g = 1_B$. En dicho caso se dice que g es la aplicación inversa de f y se denota por f^{-1}.

Ejemplo: Si $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$ son conjuntos, la aplicación $f : A \longrightarrow B$ tal que $f(1) = b, f(2) = c, f(3) = a$ es claramente biyectiva, y su inversa es la aplicación $f^{-1} : B \longrightarrow A$ tal que $f^{-1}(a) = 3, f^{-1}(b) = 1, f^{-1}(c) = 2$.

Ejercicio: Demostrar que la aplicación $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ definida por $f(x) = \dfrac{2x+1}{3}$ es biyectiva, y calcular f^{-1}.

Sean $x, y \in \mathbb{Q}$ tales que $f(x) = f(y)$. Entonces

$$\frac{2x+1}{3} = \frac{2y+1}{3} \implies 2x+1 = 2y+1 \implies 2x = 2y \implies x = y$$

Por tanto f es inyectiva.
Es claro que si $x \in \mathbb{Q}$ entonces $f(x) \in \mathbb{Q}$, así que $\mathrm{Im}(f) \subseteq \mathbb{Q}$. Además, si $q \in \mathbb{Q}$, entonces $\dfrac{3q-1}{2} \in \mathbb{Q}$, y $f\left(\dfrac{3q-1}{2}\right) = q$.[8] Por tanto $\mathbb{Q} \subseteq \mathrm{Im}(f)$[9], y por consiguiente $\mathrm{Im}(f) = \mathbb{Q}$. Podemos afirmar entonces que f es sobreyectiva, y biyectiva debido a que es también inyectiva.
La aplicación inversa de f es $f^{-1} : \mathbb{Q} \longrightarrow \mathbb{Q}$ tal que $f^{-1}(q) = \dfrac{3q-1}{2}$ $\square$

1.5 Relaciones de equivalencia

Sea A un conjunto. Una relación binaria en A es un subconjunto $\mathrm{R} \subseteq A^2$. Cuando el par ordenado (a, b) pertenece a R entonces diremos que a está relacionado con b, lo cual denotaremos con a R b.
Ejemplo: Sea $A = \{1, 2, 3, 4, 5, 6\}$ y $\mathrm{R} = \big\{(1,1), (2,3), (3,2), (4,5), (3,4)\big\}$. Entonces R es una relación binaria en A. Además, tenemos que

$$4 \text{ R } 5,\ 5 \not\mathrm{R}\, 4,\ 2 \not\mathrm{R}\, 5,\ 1 \text{ R } 1,\ 2 \text{ R } 3 \text{ y } 3 \text{ R } 2$$

Una relación binaria R sobre A es una relación de equivalencia si cumple las siguientes propiedades:

1. **Reflexiva:** a R a para todo $a \in A$.
2. **Simétrica:** Si a R b, entonces b R a.
3. **Transitiva:** Si a R b y b R c, entonces a R c.

Ejemplo: Sean A y R como en el ejemplo anterior. Entonces:

- R no es reflexiva ya que $(2,2) \notin$ R y por tanto $2 \not\mathrm{R}\, 2$.
- R no es simétrica ya que $(4,5) \in$ R pero $(5,4) \notin$ R. Por tanto 4 R 5 pero $5 \not\mathrm{R}\, 4$.
- R no es transitiva ya que $(2,3), (3,4) \in$ R pero $(2,4) \notin$ R, así que tenemos que 2 R 3 R 4 [10] pero $2 \not\mathrm{R}\, 4$.

Ejemplo: Sea $A = \{1, 2, 3, 4, 5, 6\}$ y $\mathrm{R} = \big\{(1,1)(2,2), (3,3), (4,4), (5,5), (6,6),$
$(1,2), (2,1), (2,3), (3,2), (1,3), (3,1), (5,6), (6,5)\big\}$. Entonces podemos ver que R es una relación de equivalencia en A.

[8] Esto es debido a que si $\exists x$ t. q. $f(x) = q$, entonces $\frac{2x+1}{3} = q \implies 2x+1 = 3q \implies 2x = 3q-1 \implies x = \frac{3q-1}{2}$.

[9] Todos los elementos de $\mathbb{Q}$ están en $\mathrm{Im}(f)$, ya que para todo número racional q, existe otro número racional al que la aplicación f le asocia el número q como imagen, como acabamos de demostrar.

[10] a R b R c es una manera abreviada de escribir "a R b y b R c", al igual que se suelen escribir expresiones de la forma $x = y = z$ ó $1 < 2 < 3$.

Sea R una relación de equivalencia en un conjunto A, y $a \in A$. Entonces llamaremos la clase de a a $[a] = \big\{b \in A \text{ t. q. } b \mathrel{\mathrm{R}} a\big\}$, y definiremos el conjunto cociente como
$\dfrac{A}{\mathrm{R}} \coloneqq \big\{[a] \text{ t. q. } a \in A\big\}$.
Ejemplo: Sean A y R como en el ejemplo anterior. Entonces $[1] = \{1, 2, 3\}$ [11], $[2] = \{1, 2, 3\}$, $[3] = \{1, 2, 3\}$, $[4] = \{4\}$, $[5] = \{5, 6\}$ y $[6] = \{5, 6\}$. Por tanto el conjunto cociente es [12]

$$\frac{A}{\mathrm{R}} = \big\{[1], [2], [3], [4], [5], [6]\big\} = \big\{[1], [4], [5]\big\} = \big\{\{1, 2, 3\}, \{4\}, \{5, 6\}\big\}$$

Proposición 4. Sea R una relación de equivalencia sobre un conjunto A y $a, b \in A$. Entonces

1. $a \mathrel{\mathrm{R}} b$ si y solo si $[a] = [b]$. [13]
2. $a \not\mathrel{\mathrm{R}} b$ si y solo si $[a] \cap [b] = \emptyset$.

Ejercicio: En el conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ definimos la relación binaria R de la siguiente manera: $a \mathrel{\mathrm{R}} b$ si y solo si $a - b$ es múltiplo de 3.

a) Demostrar que R es una relación de equivalencia.

b) Calcular $[2]$.

c) Calcular el cardinal del conjunto cociente $\dfrac{A}{\mathrm{R}}$.

- Vamos a demostrar que R cumple las propiedades reflexiva, simétrica y transitiva:
  - Si $a \in A$ entonces $a - a = 0$ y 0 es múltiplo de 3. Por tanto $a \mathrel{\mathrm{R}} a$ para todo $a \in A$ y R cumple la propiedad reflexiva.
  - Si $a \mathrel{\mathrm{R}} b$ entonces $a - b$ es múltiplo de 3 $\implies$ $-(a - b)$ es múltiplo de 3 $\implies$ $b - a$ es múltiplo de 3 $\implies$ $b \mathrel{\mathrm{R}} a$. Por tanto R cumple la propiedad simétrica.
  - Si $a \mathrel{\mathrm{R}} b \mathrel{\mathrm{R}} c$ entonces $a - b$ y $b - c$ son múltiplos de 3. Por tanto $(a - b) + (b - c) = a - c$ es otro múltiplo de 3 y entonces $a \mathrel{\mathrm{R}} c$. Por consiguiente R cumple la propiedad transitiva.

  Por tanto R es una relación de equivalencia.
- $[2] = \big\{a \in A \text{ t. q. } a - 2 \text{ es múltiplo de } 3\big\} = \{2, 5, 8\}$
- Sabemos que $\dfrac{A}{\mathrm{R}} = \big\{[1], [2], [3], \ldots, [9]\big\}$ y por tanto $\#\dfrac{A}{\mathrm{R}} \leq 9$ [14]. Pasamos a ver cuántas de las clases son iguales:

[11] Esto se debe a que $1 \mathrel{\mathrm{R}} 1$, $1 \mathrel{\mathrm{R}} 2$ y $1 \mathrel{\mathrm{R}} 3$. Cabe señalar que para cualquier relación de equivalencia sobre un conjunto A, se cumple que $a \in [a]$ para todo $a \in A$ ya que toda relación de equivalencia es reflexiva.

[12] Nótese que el conjunto $\big\{[1], [2], [3], [4], [5], [6]\big\}$ y $\big\{[1], [4], [5]\big\}$ son iguales porque $[1] = [2] = [3]$ y $[5] = [6]$.

[13] Es decir, $a \mathrel{\mathrm{R}} b$ implica que sus clases sean iguales, y a su vez $[a] = [b]$ implica que a está relacionado con b. Esto es análogo para el segundo punto de la proposición.

[14] Ya que si algunas de las clases son iguales entonces el cardinal del conjunto no es 9 ya que no hay 9 elementos distintos.

- Como hemos visto en el apartado anterior, 2 R 5 y 2 R 8, y por tanto $[2] = [5] = [8]$.
- $[1] = \{1, 4, 7\} \implies 1 \text{ R } 4 \text{ y } 1 \text{ R } 7 \implies [1] = [4] = [7]$
- $[3] = \{3, 6, 9\} \implies 3 \text{ R } 6 \text{ y } 3 \text{ R } 9 \implies [3] = [6] = [9]$

Por tanto el conjunto cociente solo tiene 3 clases distintas y entonces $\#\dfrac{A}{\mathrm{R}} = 3$

□

Ejercicio: Sea $A = \{1, 2, 3, 4\}$. En $\mathcal{P}(A)$ definimos la relación binaria R de la siguiente manera: X R Y si y solo si $\#X = \#Y$.

a) Demostrar que R es una relación de equivalencia.

b) Calcular $\big[\{1, 2\}\big]$.

c) Calcular el cardinal de $\dfrac{\mathcal{P}(A)}{\mathrm{R}}$.

(Solución intencionalmente en blanco)

Ejercicio: Sea $A = \{-3, -1, 0, 1, 2, 3, 4\}$. Definimos en A la relación binaria R de la siguiente manera: x R y si y solo si $x^2 = y^2$.

a) Demostrar que R es una relación de equivalencia.

b) Calcular $[1]$.

c) Calcular el cardinal de $\dfrac{A}{\mathrm{R}}$.

(Solución intencionalmente en blanco)

1.6 Relaciones de orden

Sea $\leq$ una relación binaria sobre un conjunto A. Entonces $\leq$ es una relación de orden si verifica las siguientes propiedades:

1. **Reflexiva:** $a \leq a$ para todo $a \in A$.
2. **Antisimétrica:** Si $a \leq b$ y $b \leq a$, entones $a = b$.
3. **Transitiva:** Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Ejemplo: El orden usual $\underset{u}{\leq}$ [15] es una relación de orden en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$.
Ejercicio: En el conjunto de los números naturales $\mathbb{N}$ definimos una relación binaria $\underset{m}{\leq}$ de la siguiente manera: $a \underset{m}{\leq} b$ si y solo si b es múltiplo de a. Demostrar que $\underset{m}{\leq}$ es una relación de orden.

Obsérvese que $2 \underset{m}{\leq} 6$, $4 \underset{m}{\not\leq} 6$ y $5 \underset{m}{\leq} 0$. Pasamos ahora a demostrar que $\underset{m}{\leq}$ cumple las propiedades reflexiva, antisimétrica y transitiva.

[15] El orden usual ("menor o igual que") es el que se suele usar cuando se trabaja con números: $3 \leq 4$ y $2 \leq 2$ pero $4 \not\leq 3$. En esta sección trabajaremos con relaciones de orden bastante distintas al orden usual.

- Todo $a \in \mathbb{N}$ verifica que a es múltiplo de a. Por tanto $a \underset{m}{\leq} a$ para todo $a \in \mathbb{N}$ y entonces $\underset{m}{\leq}$ cumple la propiedad reflexiva.
- Si $a \underset{m}{\leq} b$ y $b \underset{m}{\leq} a$, entonces a es múltiplo de b y b es múltiplo de a. Esto lleva a que $a = b$ [16] y por tanto $\underset{m}{\leq}$ cumple la propiedad antisimétrica.
- Si $a \underset{m}{\leq} b$ y $b \underset{m}{\leq} c$, entonces c es múltiplo de b y b es a su vez múltiplo de a. Entonces tenemos que c es múltiplo de $a \implies a \underset{m}{\leq} c$. Por tanto $\underset{m}{\leq}$ cumple la propiedad transitiva.

Por consiguiente $\underset{m}{\leq}$ es una relación de orden. $\square$

Un conjunto ordenado es un par $(A, \leq)$ donde A es un conjunto y $\leq$ es una relación de orden en A. Si para todo $(a, b) \in A^2$ se cumple que $a \leq b$ o que $b \leq a$ [17], entonces diremos que $(A, \leq)$ es un conjunto totalmente ordenado.
Ejemplo: $(\mathbb{N}, \underset{u}{\leq})$ es un conjunto totalmente ordenado, pero $(\mathbb{N}, \underset{m}{\leq})$ no es un conjunto totalmente ordenado ya que el par ordenado $(3, 4) \in \mathbb{N}^2$ no cumple que $3 \underset{m}{\leq} 4$ ni que $4 \underset{m}{\leq} 3$.

1.7 Elementos notables de un conjunto ordenado

Si $(A, \leq)$ es un conjunto ordenado y $B \subseteq A$, entonces:

1. Un maximal de B es un elemento $\beta \in B$ tal que si $x \in B$ y $\beta \leq x$ entonces $\beta = x$.
2. Un minimal de B es un elemento $\beta \in B$ tal que si $x \in B$ y $x \leq \beta$ entonces $x = \beta$. [18]
3. Un elemento $\beta \in B$ es el máximo de B si $x \leq \beta$ para todo $x \in B$.
4. Un elemento $\beta \in B$ es el mínimo de B si $\beta \leq x$ para todo $x \in B$.
5. Una cota superior de B es un elemento $a \in A$ tal que $b \leq a$ para todo $b \in B$.
6. Una cota inferior de B es un elemento $a \in A$ tal que $a \leq b$ para todo $b \in B$.
7. El supremo de B es el mínimo del subconjunto $C \subseteq A$ formado por las cotas superiores de B.
8. El ínfimo de B es el máximo del subconjunto $C \subseteq A$ formado por las cotas superiores de B.

Ejercicio: Dado el conjunto ordenado $(\mathbb{N}, \underset{m}{\leq})$, calcular los elementos notables de $B = \{1, 2, 3, 4, 5\} \subseteq \mathbb{N}$.

- Como $1 \underset{m}{\leq} 2$ y $2 \underset{m}{\leq} 4$, entonces los maximales de B son 3, 4 y 5 ya que son los únicos que no tienen múltiplos en B salvo ellos mismos.

[16] Esto se puede demostrar de la siguiente manera: si a es múltiplo de b entonces $a = mb$ para algún $m \in \mathbb{Z}$, y si b es múltiplo de a entonces $b = na$ para algún otro $n \in \mathbb{Z}$. Por tanto, como $a = m \cdot b = m \cdot (na) = mna$, entonces $m \cdot n = 1$. Pero como a y b son números naturales, entonces m y n no pueden ser negativos, por lo que la única posibilidad es que $m = n = 1 \implies a = b$.
[17] O ambos, en el caso de que $a = b$
[18] Además, denotaremos por Maximales(B) y Minimales(B) a los conjuntos formados por los maximales de B y los minimales de B respectivamente.

- El único minimal de B es el 1, ya que el único $x \in B$ tal que 1 es múltiplo de x es $x = 1$.
- B no tiene máximo, ya que no existe ningún elemento en B que sea múltiplo de todos los otros.
- El mínimo de B es el 1, ya que todos los elementos de B son múltiplos de 1.
- Las cotas superiores de B son los elementos de $\mathbb{N}$ que sean múltiplos de 1, 2, 3, 4 y de 5. Por tanto, el conjunto de las cotas superiores de B es el conjunto de múltiplos naturales de 60: $C_S = \{60k \text{ t. q. } k \in \mathbb{N}\} = \{0, 60, 120, 180, \dots\}$
- Similarmente, las cotas inferiores de B son los elementos de $\mathbb{N}$ que son divisores de 1, 2, 3, 4 y de 5. Como el único número natural que cumple esto es el 1, entonces el conjunto de cotas inferiores de B es $C_I = \{1\}$.
- El supremo de B es el mínimo de $C_S = \{0, 60, 120, \dots\}$. Como C_S es el conjunto de múltiplos naturales de 60 entonces $60 \underset{m}{\leq} x$ para todo $x \in C_S$. Por tanto el mínimo de C_S (el supremo de B) es el 60.
- Claramente el 1 es el máximo de $C_I = \{1\}$. Por tanto el ínfimo de B es el 1.

□

Ejercicio: Sea X un conjunto. Demostrar que la relación binaria $\subseteq$ sobre $\mathcal{P}(X)$ es una relación de orden.

(Solución intencionalmente en blanco)

Ejercicio: Dado el conjunto ordenado $\Big(\mathcal{P}\big(\{1, 2, 3, 4, 5, 6\}\big), \subseteq\Big)$, calcular los elementos notables de $B = \big\{\{3, 4, 5\}, \{2, 4, 6\}, \{2\}\big\}$.

(Solución intencionalmente en blanco)

2 Aritmética entera y modular

La aritmética es el estudio de los números y de las operaciones entre ellos. En concreto, este tema da una base de las propiedades de la aritmética entera que luego nos servirán para abarcar problemas más complicados como ecuaciones diofánticas o congruencias.
La segunda parte del tema trata de aritmética modular, la cual será esencial para el resto de temas, ya que la mayoría de problemas que se nos presentan están basados en ella.

Denotamos por $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ al conjunto de los números enteros. Sobre $\mathbb{Z}$ hay definidas una operación suma $(+)$ y una operación producto $(\cdot)$ con las siguientes propiedades.
Propiedades de la suma:

- Conmutativa: $a + b = b + a \ \ \forall a, b \in \mathbb{Z}$ [1]
- Asociativa: $(a + b) + c = a + (b + c) = a + b + c \ \ \forall a, b, c \in \mathbb{Z}$
- Elemento neutro: $a + 0 = a \ \ \forall a \in \mathbb{Z}$
- Elemento inverso: $a + (-a) = 0 \ \ \forall a \in \mathbb{Z}$
- Cancelativa: $a + c = b + c \implies a = b \ \ \forall a, b, c \in \mathbb{Z}$

Propiedades del producto:

- Conmutativa: $a \cdot b = b \cdot a \ \ \forall a, b \in \mathbb{Z}$
- Asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c \ \ \forall a, b, c \in \mathbb{Z}$
- Elemento neutro: $a \cdot 1 = a \ \ \forall a \in \mathbb{Z}$
- Cancelativa por elementos distintos de cero: $a \cdot c = b \cdot c \implies a = b \ \ \forall a, b, c \in \mathbb{Z}, \mathbf{c \neq 0}$
- Distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c \ \ \forall a, b, c \in \mathbb{Z}$

Propiedad de la división
Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existen unos únicos $q, r \in \mathbb{Z}$ t. q. $a = bq + r$ y $0 \leq r < |b|$. A q y r se les llama el cociente y el resto de dividir a entre b, y los denotaremos a div b y a mod b respectivamente[2].
Ejemplo:
123 div $9 = 13$ y 123 mod $9 = 6$ porque $123 = 9 \cdot 13 + 6$.
(-123) div $9 = -14$ y (-123) mod $9 = 3$ porque

$$123 = 9{\cdot}13{+}6 \implies -123 = 9{\cdot}(-13){-}6 \implies -123 = 9{\cdot}(-13){-}9{+}9{-}6 \implies -123 = 9{\cdot}(-14){+}3$$

Sean $a, b \in \mathbb{Z}$. Diremos que a divide a b (o que a es divisor de b, o que b es múltiplo de a), denotado $a \mid b$, si existe $c \in \mathbb{Z}$ t. q. $b = a \cdot c$ [3]
Ejemplo: $2 \mid 6$, pero $2 \nmid 9$.

---

[1] El símbolo $\forall$ significa "para todo".
[2] Si a mod $b = 0$, entonces a div b también se puede denotar como $\frac{a}{b}$
[3] O lo que es lo mismo, si a mod $b = 0$.

Sea $p \in \mathbb{Z} \setminus \{-1, 1\}$. Entonces se dice que p es primo si sus únicos divisores son 1, -1, p y $-p$. Además, dos números enteros $a, b \in \mathbb{Z}$ son primos relativos si los únicos divisores que tienen en común son el 1 y el -1.

Ejemplo:
$2, -2, 3, -3, 5, 7, -11, 13, 23 \ldots$ son números primos.
4 y 9 son primos relativos, pero 4 y 8 no son primos relativos.

Teorema 1 (Teorema de Bézout)**.** Dos números $a, b \in \mathbb{Z}$ son primos relativos solo si existen $u, v \in \mathbb{Z}$ t. q. $au + bv = 1$.

Ejercicio: Calcular $u, v \in \mathbb{Z}$ que verifiquen que $4u + 9v = 1$.

Probando distintos valores de u y v, vemos que $4 \cdot (-2) + 9 \cdot 1 = 1$. Por tanto $u = -2, v = 1$ $\square$

Teorema 2 (Teorema fundamental de la aritmética)**.** Todo número entero mayor o igual que dos se puede expresar de forma única, salvo reordenaciones, como producto de números primos positivos.[4]

Ejercicio: Calcular la descomposición en primos de 360.

$$360 = 2 \cdot 180 = 2 \cdot 2 \cdot 90 = 2 \cdot 2 \cdot 2 \cdot 45 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 15 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5 \quad \square$$

Corolario 1. [5] Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ es la descomposición en primos de un entero $n > 1$, entonces $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1)$ es el número de divisores **positivos** de n.

Ejercicio: ¿Cuántos divisores tiene el número 360?

Como hemos dicho en el ejercicio anterior, $360 = 2^3 \cdot 3^2 \cdot 5^1$ es la descomposición en primos de 360. Por tanto, el número de divisores positivos de 360 es $(3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = 24$. Así que el número total de divisores de 360 es $2 \cdot 24 = 48$ $\square$

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

- $d \mid a$ y $d \mid b$.
- Si $\exists c \in \mathbb{Z}$ t. q. $c \mid a$ y $c \mid b$, entonces $c \mid d$. [6]

Nota: Si d es un m.c.d de a y b, entonces $-d$ también lo es. La expresión $\mathrm{m.\,c.\,d}\{a, b\}$[7] denota al máximo común divisor de a y b que sea positivo.
Ejemplo: $\mathrm{m.\,c.\,d}\{6, 10\} = 2$, $\mathrm{m.\,c.\,d}\{6, 0\} = 6$, $\mathrm{m.\,c.\,d}\{6, 6\} = 6$, $\nexists\, \mathrm{m.\,c.\,d}\{0, 0\}$.

[4] A esta forma de expresar un número se le llama su descomposición en primos.
[5] Un corolario es una consecuencia de una proposición o teorema que es lo suficientemente importante como para ser notado.
[6] O sea, que si c es divisor común de a y de b, entonces también es divisor común de d. Por eso d es el máximo de los divisores comunes de a y b.
[7] Se usan llaves porque se puede hacer el m.c.d de un conjunto con más de dos números. En el caso de haber tres o más argumentos, $\mathrm{m.\,c.\,d}\{a, b, c\} = \mathrm{m.\,c.\,d}\left\{a, \mathrm{m.\,c.\,d}\{b, c\}\right\}$

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

- $a \mid m$ y $b \mid m$.
- Si $\exists c \in \mathbb{Z}$ t. q. $a \mid c$ y $b \mid c$, entonces $m \mid c$. [8]

Nota: Si m es un m.c.m de a y b, entonces $-m$ también lo es. La expresión $\text{m. c. m}\{a, b\}$ denota al mínimo común múltiplo de a y b que sea positivo.
Ejemplo: $\text{m. c. m}\{6, 10\} = 30$, $\text{m. c. d}\{6, 0\} = 0$, $\text{m. c. d}\{6, 6\} = 6$, $\text{m. c. m}\{0, 0\} = 0$.

Proposición 1. Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $\text{m. c. d}\{a, b\} = \text{m. c. d}\{|a|, |b|\}$ y $\text{m. c. m}\{a, b\} = \text{m. c. m}\{|a|, |b|\}$

Teorema 3. Sean $p_1, p_2, \ldots, p_r$ números primos positivos y $\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_r, \beta_r \in \mathbb{N}$. Si $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ y $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$, entonces se cumple que

$$\text{m. c. d}\{a, b\} = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \ldots p_r^{\min\{\alpha_r, \beta_r\}}$$

$$\text{m. c. m}\{a, b\} = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \ldots p_r^{\max\{\alpha_r, \beta_r\}} \quad [9]\ [10]$$

Ejercicio: Calcular el m.c.d y el m.c.m de 120 y 231.

$120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0$ y $231 = 3 \cdot 7 \cdot 11 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1$
Por tanto, $\text{m. c. d}\{120, 231\} =$
$\text{m. c. d}\{2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0,\ \ 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1\} = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3$
y $\text{m. c. m}\{120, 231\} = \text{m. c. m}\{2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0,\ \ 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1\} =$
$2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 9240$ □

Proposición 2. Si a y b son enteros positivos, entonces $\text{m. c. d}\{a, b\} \cdot \text{m. c. m}\{a, b\} = a \cdot b$.

2.1 Algoritmo de Euclides

Entrada: a y b enteros positivos.
Salida: $\text{m. c. d}\{a, b\}$
Al principio, $(a_0, a_1) = (a, b)$. Mientras $a_1 \neq 0$, se sustituye (a_0, a_1) por $(a_1, a_0 \bmod a_1)$. Si $a_1 = 0$, entonces devuelve a_0 como salida.[11]
Ejercicio: Calcular el m.c.d de 282 y 134.

Usando el algoritmo de Euclides:

$$(a_0, a_1) = (282, 134) = (134, 14) = (14, 8) = (8, 6) = (6, 2) = (\mathbf{2}, \mathbf{0})$$

Por tanto, $\text{m. c. d}\{282, 134\} = 2$ □

[8] Análogo a la explicación de máximo común divisor.
[9] Las expresiones $\min\{\alpha, \beta\}$ y $\max\{\alpha, \beta\}$ denotan, como es de esperar, el menor y el mayor entre α y β.
[10] Esta es la forma matemáticamente rigurosa de la regla de "comunes y no comunes al mayor exponente" para el mínimo común múltiplo y "solo comunes al menor exponente" para el máximo común divisor.
[11] Normalmente el algoritmo de Euclides se lleva a cabo en una tabla, pero se denota de este modo a lo largo del tema 2 y 3.

2.2 Ecuaciones diofánticas lineales

Una ecuación diofántica lineal es una expresión de la forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, donde $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ y $x_1, x_2, \ldots, x_n$ son incógnitas. Una n-tupla $(c_1, c_2, \ldots, c_n) \in \mathbb{Z}^n$ es solución de dicha ecuación si la igualdad $a_1c_1 + a_2c_2 + \cdots + a_nc_n = b$ es cierta.

Teorema 4 (Teorema de Bézout generalizado)**.** Si $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ y $d = \text{m. c. d}\{a_1, a_2, \ldots, a_n\}$, entonces la ecuación diofántica $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ tiene solución si y solo si $d \mid b$. En dicho caso, esa ecuación tiene las mismas soluciones que

$$\frac{a_1}{d}x_1 + \frac{a_2}{d}x_2 + \cdots + \frac{a_n}{d}x_n = \frac{b}{d}$$

Ejemplo:

- La ecuación diofántica $9x - 6y + 15z = 22$ no tiene solución, ya que $\text{m. c. d}\{9, -6, 15\} = 3$ y $3 \nmid 22$.
- La ecuación diofántica $6x - 14y + 12z = 10$ tiene solución ya que $\text{m. c. d}\{6, -14, 2\} = 2 \mid 10$. Además, tiene las mismas soluciones que la ecuación $3x - 7y + 6z = 5$.

2.3 Ecuaciones diofánticas lineales con dos incógnitas

Sean $a, b, c \in \mathbb{Z}$ t. q. $\text{m. c. d}\{a, b\} = 1$. 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

$$\Big\{(x_0 + b \cdot k, y_0 - a \cdot k) \text{ t. q. } k \in \mathbb{Z}\Big\}^{12}$$

Ejercicio: Calcular todas las soluciones de la ecuación $10x - 8y = 14$.

Como $\text{m. c. d}\{10, -8\} = 2 \mid 14$, la ecuación del enunciado tiene solución, y tiene las mismas soluciones que la ecuación

$$5x - 4y = 7 \tag{1}$$

Nótese que $\text{m. c. d}\{5, -4\} = 1$.
Como $(3, 2)$ es una solución de (1), el conjunto de todas las soluciones de la ecuación es $S = \Big\{(3 - 4k, 2 - 5k) \text{ t. q. } k \in \mathbb{Z}\Big\}$ $\square$

2.4 Algoritmo extendido de Euclides

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

[12] Como es de esperar, si una ecuación diofántica lineal tiene solución, entonces tiene soluciones infinitas.

Al principio,

$$\begin{aligned}(a_0, a_1) &= (a, b)\\ (s_0, s_1) &= (1, 0)\\ (t_0, t_1) &= (0, 1)\end{aligned}$$

Mientras, $a_1 \neq 0$, se toma $q = a_0$ div a_1 y se sustituyen

$$\begin{aligned}(a_0, a_1) &\text{ por } (a_1, a_0 - qa_1)\\ (s_0, s_1) &\text{ por } (s_1, s_0 - qs_1)\\ (t_0, t_1) &\text{ por } (t_1, t_0 - qt_1)\end{aligned}$$

Cuando $a_1 = 0$, entonces se devuelve como salida $d = a_0, s = s_0, t = t_0$.
Ejercicio: Calcular todas las soluciones de la ecuación $120x - 93y = 6$.

m. c. d$\{120, -93\} = 3 \mid 6$. Por tanto, la ecuación del enunciado tiene solución, y tiene las mismas soluciones que

$$40x - 31y = 2. \tag{1}$$

Para hallar una solución de esta ecuación usamos el algoritmo extendido de Euclides con 40 y 31 como entrada:

$$\begin{array}{ccccccccccc}(a_0, a_1) & = & (40, 31) & \overset{q=1}{=} & (31, 9) & \overset{q=3}{=} & (9, 4) & \overset{q=2}{=} & (4, 1) & \overset{q=4}{=} & (1, 0)\\ (s_0, s_1) & = & (1, 0) & = & (0, 1) & = & (1, -3) & = & (-3, 7) & = & (7, \dots)\\ (t_0, t_1) & = & (0, 1) & = & (1, -1) & = & (-1, 4) & = & (4, -9) & = & (-9, \dots)\end{array}$$

El algoritmo[13] nos proporciona la igualdad $40 \cdot 7 + 31 \cdot (-9) = 1$. Por tanto, $40 \cdot 14 - 31 \cdot 18 = 2$ así que $(14, 18)$ es una solución de (1). Por consiguiente, el conjunto de todas las soluciones de la ecuación es

$$S = \Big\{(14 - 31k, 18 - 40k) \text{ t. q. } k \in \mathbb{Z}\Big\} \quad \square$$

Ejercicio: Calcular todas las soluciones de la ecuación $72x + 123y = 18$.

(Solución intencionalmente en blanco)

2.5 Ecuaciones en congruencias de grado uno

Sean $a, b, m \in \mathbb{Z}$. Escribiremos $a \equiv b \pmod m$, leído "a es congruente con b módulo m", si $m \mid (a - b)$ [14]
Ejemplo: $5 \equiv 1 \pmod 2$ y $7 \not\equiv 2 \pmod 3$.
Una ecuación en congruencias de grado uno es una expresión de la forma $ax \equiv b \pmod m$, donde $a, b, m \in \mathbb{Z}$ y x es una incógnita. Una solución de dicha ecuación es un número $c \in \mathbb{Z}$ t. q. $a \cdot c \equiv b \pmod m$.

[13] Una vez que se ha llegado a la condición de $a_1 = 0$, no es necesario calcular s_1 ni t_1. Por eso en el paso final se pone "..."
[14] Esto es equivalente a decir que $a \equiv b \pmod m$ si $a \bmod m = b \bmod m$.

Ejemplo:

- Los números $4, 9, 14, -1, -6$ y -11 son todos soluciones a la ecuación $3x \equiv 2 \pmod 5$.
- La ecuación $2x \equiv 1 \pmod 4$ no tiene solución, porque $2x$ es par para todo entero x, por tanto $2x - 1$ es impar y ningún impar es múltiplo de 4.

Teorema 5 (Procedimientos para resolver congruencias)**.**

1. La ecuación $ax \equiv b \pmod m$ tiene solución si y solo si $\text{m. c. d}\{a, m\} \mid b$.
2. Si $d = \text{m. c. d}\{a, m\}$ y $d \mid b$, entonces la ecuación $ax \equiv b \pmod m$ tiene las mismas soluciones que la ecuación $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.
3. Si $\text{m. c. d}\{a, m\} = 1$ y u es una solución de la ecuación $ax \equiv b \pmod m$, entonces el conjunto formado por todas sus soluciones es $\Big\{u + m \cdot k \text{ t. q. } k \in \mathbb{Z}\Big\}$.
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 $(a \bmod m)x \equiv (b \bmod m) \pmod m$.
6. Si $u, v \in \mathbb{Z}$ y $au + mv = 1$, entonces $(b \cdot u) \bmod m$ es una solución de la ecuación $ax \equiv b \pmod m$.

Ejercicio: Calcular todas las soluciones de la ecuación $327x \equiv 191 \pmod 5$.

Nótese que $327 \bmod 5 = 2$ y $191 \bmod 5 = 1$. entonces por el punto 5 del teorema anterior, la ecuación del enunciado tiene las mismas soluciones que

$$2x \equiv 1 \pmod 5 \tag{1}$$

$\text{m. c. d}\{2, 5\} = 1 \mid 1$. Por tanto, la ecuación tiene solución. Sabemos que una de las soluciones es un entero entre 0 y 4 por el punto 6[15] , y tras probar se obtiene que $x = 3$ es una solución de (1). Tras aplicar el punto 3, se puede afirmar que el conjunto formado por todas las soluciones de la ecuación es

$$S = \Big\{3 + 5k \text{ t. q. } k \in \mathbb{Z}\Big\} \quad \square$$

Ejercicio: Calcular todas las soluciones de la ecuación $30x \equiv 20 \pmod{50}$.

$\text{m. c. d}\{30, 50\} = 10 \mid 20$. Por tanto, esta ecuación tiene solución (punto 1) y tiene las mismas soluciones (punto 2) que $3x \equiv 2 \pmod 5$. Tras probar enteros entre 0 y 4, obtenemos $x = 4$ como una solución, así que el conjunto de todas las soluciones es

$$S = \Big\{4 + 5k \text{ t. q. } k \in \mathbb{Z}\Big\} \quad \square$$

[15] Esto es debido a que si $x, m \in \mathbb{Z}$, $0 \leq (x \bmod m) < m$ por definición.

Ejercicio: Calcular todas las soluciones de la ecuación $242x \equiv 4 \pmod{392}$.

$\text{m.c.d}\{242, 392\} = 2 \mid 4$. Por tanto, la ecuación tiene solución y además tiene las mismas soluciones que

$$121x \equiv 2 \pmod{196} \tag{1}$$

Sabemos que hay una solución en el conjunto $\{0, 1, 2, \ldots, 195\}$, y para calcular esa solución hacemos uso del punto 6 del teorema: si
$\exists u, v \in \mathbb{Z}$ t. q. $121u + 196v = 1$, entonces $2u \bmod 196$ es una solución de (1).
Para calcular dichos valores de u y v utilizamos el algoritmo extendido de Euclides con 196 y 121.

$$\begin{array}{lcccccccccccc}
(a_0, a_1) & = & (196, 121) & \overset{q=1}{=} & (121, 75) & \overset{q=1}{=} & (75, 46) & \overset{q=1}{=} & (46, 29) & \overset{q=1}{=} & (29, 17) & \overset{q=1}{=} & (17, 12) \quad \ldots \\
(s_0, s_1) & = & (1, 0) & = & (0, 1) & = & (1, -1) & = & (-1, 2) & = & (2, -3) & = & (-3, 5) \quad \ldots \\
(t_0, t_1) & = & (0, 1) & = & (1, -1) & = & (-1, 2) & = & (2, -3) & = & (-3, 5) & = & (5, -8) \quad \ldots
\end{array}$$

$$\begin{array}{lcccccccccc}
\ldots & = & (17, 12) & \overset{q=1}{=} & (12, 5) & \overset{q=2}{=} & (5, 2) & \overset{q=2}{=} & (2, 1) & \overset{q=2}{=} & (1, 0) \\
\ldots & = & (-3, 5) & = & (5, -8) & = & (-8, 21) & = & (21, -50) & = & (-50, \ldots) \\
\ldots & = & (5, -8) & = & (-8, 13) & = & (13, -34) & = & (-34, 81) & = & (81, \ldots)
\end{array}$$

El algoritmo nos proporciona la igualdad $196 \cdot (-50) + 121 \cdot 81 = 1$. Por tanto $(2 \cdot 81) \bmod 196$ es una solución de (1). $(2 \cdot 81) \bmod 196 = 162 \bmod 196 = 162$.
Por tanto el conjunto de todas las soluciones es

$$S = \Big\{162 + 196k \text{ t. q. } k \in \mathbb{Z}\Big\} \quad \square$$

Ejercicio: ¿Cuántas soluciones tiene la ecuación $72x \equiv 4 \pmod{242}$ en el intervalo $[1000, 2000]$?

(Solución intencionalmente en blanco)

2.6 Sistemas de ecuaciones en congruencias

1. [16] Resolver el sistema $\begin{cases} 4x \equiv 6 \pmod{10} & (1) \\ 3x \equiv 1 \pmod{4} & (2) \end{cases}$

   En primer lugar comprobamos que todas las ecuaciones tienen solución. Si alguna no tiene solución, entonces se concluye que el sistema no tiene solución.

   $$\begin{cases} \text{m.c.d}\{10, 4\} = 2 \mid 6 & \Longrightarrow \quad 2x \equiv 3 \pmod{5} \quad (1') \\ \text{m.c.d}\{3, 4\} = 1 & \Longrightarrow \quad 3x \equiv 1 \pmod{4} \quad (2) \end{cases}$$

   Resolvemos la ecuación $(1')$ que tiene las mismas soluciones que (1): El conjunto de soluciones es $S_1 = \{4 + 5k \text{ t. q. } k \in \mathbb{Z}\}$. Ahora, **le hemos de imponer a $4 + 5k$ que sea solución de (2):**

[16] Este apartado no contiene explicaciones ni contenido teórico, solo ejercicios a modo de ejemplo.

$$
\begin{aligned}
& 3(4+5k) \equiv 1 \pmod 4 \\
\Longrightarrow \quad & 15k + 12 \equiv 1 \pmod 4 \\
\Longrightarrow \quad & 15k \equiv -11 \pmod 4 \\
\Longrightarrow \quad & 3k \equiv 1 \pmod 4 \\
\Longrightarrow \quad & k = 3 + 4m \text{ t. q. } m \in \mathbb{Z}
\end{aligned}
$$

Por tanto, como $x = 4 + 5k$ y $k = 3 + 4m$[17],
$x = 4 + 5(3 + 4m) = 19 + 20m$. $\square$

2. Resolver el sistema $\begin{cases} 2x \equiv 2 \pmod 4 & (1) \\ 6x \equiv 3 \pmod 9 & (2) \\ 2x \equiv 3 \pmod 5 & (3) \end{cases}$

Pasamos al sistema $\begin{cases} x \equiv 1 \pmod 2 & (1') \\ 2x \equiv 1 \pmod 3 & (2') \\ 2x \equiv 3 \pmod 5 & (3) \end{cases}$.[18]
Las soluciones de $(1')$ son de la forma $2k + 1$ t. q. $k \in \mathbb{Z}$. Sustituimos esta expresión en $2'$:

$$
\begin{aligned}
& 2(2k+1) \equiv 1 \pmod 3 \\
\Longrightarrow \quad & 4k + 2 \equiv 1 \pmod 3 \\
\Longrightarrow \quad & 4k \equiv -1 \pmod 3 \\
\Longrightarrow \quad & k \equiv 2 \pmod 3 \\
\Longrightarrow \quad & k = 2 + 3m \text{ t. q. } m \in \mathbb{Z}
\end{aligned}
$$

Por tanto, $x = 2k+1 = 2(2+3m)+1 = 5+6m$. Sustituimos $5+6m$ en (3):

$$
\begin{aligned}
& 2(5+6m) \equiv 3 \pmod 5 \\
\Longrightarrow \quad & 12m + 10 \equiv 3 \pmod 5 \\
\Longrightarrow \quad & 12m \equiv -7 \pmod 5 \\
\Longrightarrow \quad & 2m \equiv 3 \pmod 5 \\
\Longrightarrow \quad & m = 4 + 5n \text{ t. q. } n \in \mathbb{Z}
\end{aligned}
$$

$$x = 5 + 6m = 5 + 6(4 + 5n) = 29 + 30n \quad \square$$

3. Resolver el sistema $\begin{cases} 2x \equiv 2 \pmod 4 & (1) \\ 3x \equiv 6 \pmod{12} & (2) \end{cases}$

Pasamos al sistema $\begin{cases} x \equiv 1 \pmod 2 & (1') \\ x \equiv 2 \pmod 4 & (2') \end{cases}$.
Las soluciones de $(1')$ son de la forma $2k + 1$ t. q. $k \in \mathbb{Z}$. Al sustituir en $(2')$, nos sale la ecuación $2k + 1 \equiv 2 \pmod 4 \implies 2k \equiv 1 \pmod 4$. Pero $\text{m. c. d}\{2, 4\} = 2 \nmid 1$. Por tanto, $(2')$ no tiene solución y el sistema no tiene solución. $\square$

[17] Escogemos otro entero arbitrario, esta vez m (Otras personas usan $\bar{k}$, es lo mismo)

[18] Es decir, dividimos por el m.c.d de "a" y "m" en cada ecuación. La ecuación (3) no cambia porque $\text{m. c. d}\{2, 5\} = 1$

4. ¿Cuántos números enteros del intervalo $[1000, 2000]$ son pares, al dividirlos entre 7 dan de resto 1 y al multiplicarlos por 3 y dividirlos entre 5 dan de resto 2?

   Planteamos el sistema[19]:

$$\begin{cases} \text{Son pares} & \Longrightarrow & x \equiv 0 \pmod 2 & (1) \\ \text{Al dividirlos entre 7 dan resto 1} & \Longrightarrow & x \equiv 1 \pmod 7 & (2) \\ \text{Al multiplicar por 3 y dividir entre 5 dan resto 2} & \Longrightarrow & 3x \equiv 2 \pmod 5 & (3) \end{cases}$$

   Y ahora resolvemos normalmente: las soluciones de (1) son $x = 0 + 2k$ t. q. $k \in \mathbb{Z}$. Sustituimos el valor de x en (2):

$$\begin{aligned} & 2k \equiv 1 \pmod 7 \\ \Longrightarrow \quad & k = 4 + 7m \text{ t. q. } m \in \mathbb{Z} \end{aligned}$$

   $x = 2k \implies x = 2(4 + 7m) = 8 + 14m$. Ahora sustituimos en (3):

$$\begin{aligned} & 3(8 + 14m) \equiv 2 \pmod 5 \\ \Longrightarrow \quad & 42m + 24 \equiv 2 \pmod 5 \\ \Longrightarrow \quad & 42m \equiv -22 \pmod 5 \\ \Longrightarrow \quad & 2m \equiv 3 \pmod 5 \\ \Longrightarrow \quad & m = 4 + 5n \text{ t. q. } n \in \mathbb{Z} \end{aligned}$$

   $x = 8 + 14n = 8 + 14(4 + 5n) = 64 + 70n$. Por tanto el conjunto de soluciones del sistema es

$$S_0 = \Big\{ 64 + 70n \text{ t. q. } n \in \mathbb{Z} \Big\}$$

   Ahora buscamos el número de elementos de S_0 que están entre 1000 y 2000:

$$\begin{aligned} & 1000 \leq 64 + 70n \leq 2000 \\ \Longrightarrow \quad & 936 \leq 70n \leq 1936 && \text{(Restamos 64 en los tres miembros)} \\ \Longrightarrow \quad & \frac{936}{70} \leq n \leq \frac{1936}{70} && \text{(Dividimos entre 70)} \\ \Longrightarrow \quad & 13.37\cdots \leq n \leq 27.65\ldots \\ \Longrightarrow \quad & 14 \leq n \leq 27 && \text{(Redondeamos porque } n \in \mathbb{Z}) \end{aligned}$$

   Por tanto $\#(S_0 \cap [1000, 2000])$
   $= \#\Big\{ 64 + 70n \text{ t. q. } n \in \{14, 15, 16, \ldots, 27\} \Big\}$
   $= 27 - 14 + 1$ [20] $= \boxed{\mathbf{14}}$ $\square$

[19] Para plantear sistemas en congruencias es recomendable tener en cuenta que $a \equiv b \pmod m$ si $a \bmod m = b \bmod m$.

[20] Si $n, m \in \mathbb{Z}$ y $m < n$, el número de elementos del conjunto $\{m, m + 1, \ldots, n\}$ es $n - m + 1$

2.7 El anillo de los enteros módulo un entero positivo

[Nota: La definición de anillo viene en el tema 3]
Dado un entero positivo m, denotaremos por $\mathbb{Z}_m$ al conjunto $\{0, 1, \ldots, m-1\}$. En $\mathbb{Z}_m$ definimos una operación suma ($\oplus$) y una operación producto ($\odot$)[21] de la siguiente manera:

$$a \oplus b = (a + b) \bmod m \quad \text{y} \quad a \odot b = (a \cdot b) \bmod m$$

Ejemplo: En $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ se cumple que $4 \oplus 5 = 9 \bmod 7 = 2$ y que
$4 \odot 5 = 20 \bmod 7 = 6$
Propiedades de la operación $\oplus$:

- Conmutativa: $a \oplus b = b \oplus a$
- Asociativa: $(a \oplus b) \oplus c = a \oplus (b \oplus c) = a \oplus b \oplus c$
- Elemento neutro: $a \oplus 0 = a$
- Elemento inverso: $a \oplus (m - a) = 0$

Nota: Al inverso para la operación $\oplus$ de $a \in \mathbb{Z}_m$ lo denotamos $-a$
Propiedades de la operación $\odot$:

- Conmutativa: $a \odot b = b \odot a$
- Asociativa: $(a \odot b) \odot c = a \odot (b \odot c) = a \odot b \odot c$
- Elemento neutro: $a \odot 1 = a$
- Distributiva: $a \odot (b \oplus c) = (a \odot b) + (a \odot c)$

Nota: En $\mathbb{Z}_m$ puede haber elementos que tienen inverso para el producto[22] y elementos que no tienen inverso para el producto. Si $a \in \mathbb{Z}_m$ tiene inverso para el producto, se denota a dicho inverso como a^{-1}.
Ejemplo:

- En $\mathbb{Z}_5$ se tiene que $-2 = 5 - 2 = 3$.
- En $\mathbb{Z}_9$, ya que $2 \odot 5 = 10 \bmod 9 = 1$, entonces $2^{-1} = 5$, pero como el 3 no tiene inverso para el producto, entonces $\nexists 3^{-1}$.

A los elementos de $\mathbb{Z}_m$ que tienen inverso para el producto se les llama unidades de $\mathbb{Z}_m$.
Ejemplo: El conjunto de las unidades de $\mathbb{Z}_9$ es $\mathrm{U}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$[23]

Teorema 6. Un elemento $a \in \mathbb{Z}_m$ tiene inverso para el producto si y solo si $\mathrm{m.c.d}\{a, m\} = 1$. Además, si $\exists u, v \in \mathbb{Z}$ t. q. $au + mv = 1$, entonces $u \bmod m$ es el inverso para el producto de a.

Ejercicio: Calcular las unidades de $\mathbb{Z}_1 5$.

$$\mathrm{U}(\mathbb{Z}_{15}) = \left\{ a \in \mathbb{Z}_{15} \text{ t. q. } \mathrm{m.c.d}\{a, 15\} = 1 \right\} = \{1, 2, 4, 7, 8, 11, 13, 14\} \quad \square$$

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

Como $\mathrm{m.c.d}\{35, 97\} = 1$, entonces $\exists 35^{-1}$ en $\mathbb{Z}_{97}$. Para calcularlo hallamos $u, v \in \mathbb{Z}$ t. q. $35u + 97v = 1$ usando el algoritmo extendido de Euclides:

[21] Conforme avancemos en el tema, se usarán los signos + y · normales
[22] Si $a \in \mathbb{Z}_m$ tiene inverso para el producto, significa que $\exists b \in \mathbb{Z}_m$ t. q. $a \odot b = 1$
[23] Obviamente, $\mathrm{U}(\mathbb{Z}_m)$ denota el conjunto de las unidades de $\mathbb{Z}_m$

$$\begin{array}{lcccccccccccccc}
(a_0,a_1) & = & (97,35) & \overset{q=2}{=} & (35,27) & \overset{q=1}{=} & (27,8) & \overset{q=3}{=} & (8,3) & \overset{q=2}{=} & (3,2) & \overset{q=1}{=} & (2,1) & \dots \\
(s_0,s_1) & = & (1,0) & = & (0,1) & = & (1,-1) & = & (-1,4) & = & (4,-9) & = & (-9,13) & \dots \\
(t_0,t_1) & = & (0,1) & = & (1,-2) & = & (-2,3) & = & (3,-11) & = & (-11,25) & = & (25,-36) & \dots
\end{array}$$

$$\begin{array}{lcccc}
\dots & = & (2,1) & \overset{q=1}{=} & (1,0) \\
\dots & = & (-9,13) & = & (13,\dots) \\
\dots & = & (25,-36) & = & (-36,\dots)
\end{array}$$

El algoritmo nos proporciona la igualdad $97 \cdot 13 + 13 \cdot (-36) = 1$. Por tanto, basándonos en el teorema anterior, $35^{-1} = (-36) \mod 97 = \boxed{\mathbf{61}}$ $\square$

Ejercicio: Resolver en $\mathbb{Z}_9$ la ecuación $x + 7 = 5x + 2$ [24]

$$\begin{array}{ll}
 & x + 7 = 5x + 2 \\
\Longrightarrow & 5x - x = 7 - 2 \\
\Longrightarrow & 4x = 5 \\
\Longrightarrow & x = 5 \cdot 4^{-1} = 5 \cdot 7 = 35 \bmod 9 \\
\Longrightarrow & x = 8 \quad \square
\end{array}$$

Ejercicio: Resolver en $\mathbb{Z}_{10}$ la ecuación $8x + 5 = 2x + 7$

$8x + 5 = 2x + 7 \implies 6x = 2$.
Sin embargo, $\text{m. c. d}\{6, 10\} \neq 1$ así que $\nexists 6^{-1}$. No podemos proceder como en el ejercicio anterior, así que convertimos la ecuación en una congruencia[25]

$$\begin{array}{ll}
 & 6x = 2 \\
\Longrightarrow & 6x \equiv 2 \pmod{10} \\
\Longrightarrow & 3x \equiv 1 \pmod{5} \qquad (\text{m. c. d}\{6, 10\} = 2 \mid 2) \\
\Longrightarrow & x = 2 + 5k \text{ t. q. } k \in \mathbb{Z}
\end{array}$$

Como la solución a la ecuación en congruencias es $S_0 = \{2 + 5k \text{ t. q. } k \in \mathbb{Z}\}$, entonces la solución a la ecuación original es $S_0 \cap \mathbb{Z}_{10} = \{2, 7\}$. Por tanto, las dos soluciones son $x = 2, \quad x = 7$ $\square$

Ejercicio: Resolver en $\mathbb{Z}_{15}$ la ecuación $9x + 14 = 1 + 3x$

$9x + 14 = 1 + 3x \implies 6x = -13 = 2$ Sin embargo, $\text{m. c. d}\{6, 15\} \neq 1$ así que $\nexists 6^{-1}$. Pasamos a resolver la siguiente congruencia

$$6x \equiv 2 \pmod{15}$$

$\text{m. c. d}\{6, 15\} = 3 \nmid 2$. Por tanto la congruencia no tiene solución, así que la ecuación original tampoco tiene solución. $\square$

[24] A partir de aquí, la suma y la multiplicación en $\mathbb{Z}_m$ se denotan igual que en $\mathbb{Z}$

[25] Ya que todas las operaciones en $\mathbb{Z}_m$ son módulo m, pasar la ecuación $ax = b$ de $\mathbb{Z}_m$ a la ecuación en congruencias $ax \equiv b \pmod{m}$ conserva las soluciones

Ejercicio: Calcular el valor de 3^{127} en $\mathbb{Z}_{10}$ [26]

$3^1 = 3, 3^2 = 9, 3^3 = 27 \bmod 10 = 7, \mathbf{3^4 = 7 \cdot 3 = 1}$

Nótese que, en $\mathbb{Z}$, $127 = 4 \cdot 31 + 3$. Por tanto, en $\mathbb{Z}_{10}$:

$$3^{127} = 3^{4 \cdot 31 + 3} = 3^{4 \cdot 31} \cdot 3^3 = (3^4)^{31} \cdot 7 = 1^{31} \cdot 7 = \boxed{\mathbf{7}} \quad \square$$

Ejercicio: Calcular el valor de 3^{127} en $\mathbb{Z}_{15}$

$3^1 = 3 \quad , \quad 3^5 = 3$
$3^2 = 9 \quad , \quad 3^6 = 9$
$3^3 = 12 \quad , \quad \ldots$
$3^4 = 6$

Como hemos calculado en el ejercicio anterior, $127 \bmod 4 = 3$. Por tanto[27],

$$3^{127} = 3^3 = \boxed{\mathbf{12}}$$

[26] Nótese que, en cuanto a números enteros, a^b no es más que una forma abreviada de expresar a mutiplicado por sí mismo b veces. Por tanto, en $\mathbb{Z}_m$, los exponentes pueden sobrepasar m sin problemas.

[27] Tras haber llegado a un bucle en las potencias de 3, se tiene en $\mathbb{Z}_{15}$ que $3^n = 3^{n+4k}$ para cualquier $n, k \in \mathbb{N}$

3 El anillo de los polinomios con coeficientes en un cuerpo

Este tema es una introducción al álgebra abstracta y a las propiedades y características de los polinomios. Se pueden ver muchas similaridades entre este tema y el anterior, donde por ejemplo los polinomios irreducibles tienen el mismo papel en este tema que el que los números primos tienen en el tema dos.
A pesar de no parecer tener relación con los temas posteriores, es necesario conocer bien a los polinomios para resolver algunos de los ejercicios que se presentarán más adelante (por ejemplo, en el tema ocho).

Un anillo es una terna $(R, +, \cdot)$ donde R es un conjunto, y $+$ y $\cdot$ son dos operaciones sobre R que cumplen las siguientes propiedades[1]:

1. La operación $+$ es conmutativa, asociativa, tiene elemento neutro (denotado 0) y todo elemento de R tiene inverso (al inverso de $x \in R$ lo se le denota $-x$).
2. La operación $\cdot$ es asociativa, tiene elemento neutro (denotado 1) y es distributiva. Si además de todo eso la operación $\cdot$ es conmutativa, se dice que el anillo es conmutativo.

Un cuerpo es un anillo conmutativo en el que todo elemento distinto de 0 tiene un inverso para la operación $\cdot$ (al inverso de un elemento x perteneciente al cuerpo se le denotará x^{-1}).
Ejemplo:

- $(\mathbb{N}, +, \cdot)$ no es un anillo porque los números naturales no tienen inverso para la suma.
- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo. No es cuerpo porque los números enteros no tienen inverso para el producto.
- $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son cuerpos.

Proposición 1. Si m es un entero mayor o igual que 2, entonces $(\mathbb{Z}_m, +, \cdot)$ es un anillo conmutativo. Además, es un cuerpo si y solo si m es un número primo.

Sea K un cuerpo. El conjunto de los polinomios en la indeterminada x con coeficientes en el cuerpo K es

$$K[x] = \left\{ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \ \text{ t. q. } \ n \in \mathbb{N} \text{ y } a_0, a_1, \ldots, a_n \in K \right\}$$

Ejercicio: Sean $a(x) = 3 + 4x + 3x^2$ y $b(x) = 4 + 2x + x^2 + 2x^3$ dos polinomios de $\mathbb{Z}_5[x]$. Calcular $a(x) + b(x)$ y $a(x) \cdot b(x)$.

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

$$a(x) \cdot b(x) = (3x^2 + 4x + 3)(2x^3 + x^2 + 2x + 4)$$
$$= (x^5 + 3x^4 + x^3 + 2x^2) + (3x^4 + 4x^3 + 3x^2 + x) + (x^3 + 3x^2 + x + 2)$$
$$= x^5 + x^4 + x^3 + 3x^2 + 2x + 2 \quad \square$$

Proposición 2. Si K es un cuerpo, entonces $(K[x], +, \cdot)$ es un anillo conmutativo y no un cuerpo.

Si $a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ y $a_n \neq 0$, entonces diremos que $a(x)$ es un polinomio de grado n, denotado $\text{gr}\left(a(x)\right) = n$. Por definición, tomamos el grado del polinomio 0 como $\text{gr}(0) = -\infty$.[2]

[1] Los conceptos de anillo y cuerpo son la generalización de los sistemas numéricos con los que se trabaja normalmente. Así, se pueden formar anillos y/o cuerpos con conjuntos de elementos no numéricos.
[2] Definimos $\text{gr}(0)$ como $-\infty$ para que la siguiente proposición se cumpla para todo polinomio.

Proposición 3. Si K es un cuerpo y $a(x), b(x) \in K[x]$, entonces $\text{gr}\big(a(x)\cdot b(x)\big)$ $= \text{gr}\big(a(x)\big) + \text{gr}\big(b(x)\big)$

Un elemento de un anillo R es una unidad si tiene inverso para el producto. Denotaremos por $\text{U}(R)$ al conjunto formado por todas las unidades de R.

Ejemplo:

- $\text{U}(\mathbb{Z}) = \{-1, 1\}$
- Si K es un cuerpo, entonces $\text{U}(K) = K \setminus \{0\}$.
- $\text{U}(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

Proposición 4. Si K es un cuerpo, entonces $\text{U}(K[x]) = \Big\{a(x) \in K[x] \ \text{ t. q. } \ \text{gr}\big(a(x)\big) = 0\Big\}$

Ejemplo: $\text{U}(\mathbb{Z}_7[x]) = \{1, 2, 3, 4, 5, 6\}$

Sea K un cuerpo. Un elemento $a(x) \in K[x]$ es irreducible si verifica que:

1. $gr\big(a(x)\big) \geq 1$
2. Si $a(x) = b(x)\cdot c(x)$ entonces $gr\big(b(x)\big) = 0$ ó $gr\big(c(x)\big) = 0$[3]

Proposición 5. Si K es un cuerpo entonces:

1. Todo polinomio de $K[x]$ de grado 1 es irreducible.
2. Si $a(x) \in K[x]$ es irreducible y $u \in K \setminus \{0\}$ entonces $u \cdot a(x)$ es también irreducible.

Un polinomio $a(x) \in K[x]$ es mónico si el coeficiente del término[4] de mayor grado (llamado coeficiente líder) vale 1.

Ejemplo: El polinomio $x^2 + 2x + 3 \in \mathbb{Z}_5[x]$ es mónico, pero el polinomio $3x^2 + 4x + 1 \in \mathbb{Z}_7[x]$ no es mónico.

Teorema 1. Sea K un cuerpo. Todo polinomio $a(x) \in K[x] \ \text{ t. q. } \ \text{gr}\big(a(x)\big) \geq 1$ se puede expresar de forma única (salvo reordenaciones) como:

$$a(x) = u \cdot p_1(x)^{\alpha_1} \cdot p_2(x)^{\alpha_2} \cdot \cdots \cdot p_r(x)^{\alpha_r}$$

donde $u \in K \setminus \{0\}$; $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N} \setminus 0$; y $p_1(x), p_2(x), \ldots, p_r(x)$ son polinomios mónicos e irreducibles.[5]

A la expresión $u \cdot p_1(x)^{\alpha_1} \cdot p_2(x)^{\alpha_2} \cdot \cdots \cdot p_r(x)^{\alpha_r}$ se le llama la descomposición en irreducibles de $a(x)$ [6]

Ejercicio: Calcular la descomposición en irreducibles de $a(x) = (4x+3)(3x+2) \in \mathbb{Z}_7[x]$.

> $4x + 3$ y $3x + 2$ son polinomios irreducibles (ya que son de grado 1). Por tanto $(4x + 3)(3x + 2)$ es una descomposición en irreducibles de $a(x)$. Para hallar *la* descomposición en irreducibles de $a(x)$, hacemos lo siguiente:
>
> $$(4x+3)(3x+2) = \big(4\cdot 2(4x+3)\big)\big(3\cdot 5(3x+2)\big) = \big(4(x+6)\big)\big(3(x+3)\big) = 5(x+6)(x+3)$$
>
> $x + 6$ y $x + 3$ son polinomios mónicos e irreducibles, y $5 \in \mathbb{Z}_7$. Por tanto, $5(x + 6)(x + 3)$ es la descomposición en irreducibles de $a(x)$ $\square$

Sea K un cuerpo y $a(x), b(x) \in K[x]$. Se dice que $a(x)$ divide a $b(x)$ (ó que $a(x)$ es un divisor de $b(x)$, ó que $b(x)$ es un múltiplo de $a(x)$), denotado $a(x) \mid b(x)$ si $\exists c(x) \in K[x] \ \text{ t. q. } \ b(x) = a(x)c(x)$.

[3] Esto es, si $a(x)$ es producto de dos polinomios, uno de ellos debe de ser una constante.

[4] Los términos de un polinomio son cada uno de los sumandos. Por tanto, el término de mayor grado de un polinomio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o$ es $a_n x^n$.

[5] Este es el Teorema Fundamental de la Aritmética (Tema 2) con polinomios.

[6] Sin embargo, a una expresión del tipo $a(x) = p_1(x)^{\alpha_1}\cdot p_2(x)^{\alpha_2}\cdot\cdots\cdot p_r(x)^{\alpha_r}$ donde $p_1(x), p_2(x), \ldots, p_r(x)$ son polinomios irreducibles pero no mónicos se le llama *una* descomposición en irreducibles de $a(x)$, no *la* descomposición en irreducibles de $a(x)$.

Si $a(x), b(x) \in K[x]$ y $a(x) \neq 0$ ó $b(x) \neq 0$, entonces un elemento $d(x) \in K[x]$ se dice que es un máximo común divisor de $a(x)$ y $b(x)$ si verifica que:

1. $d(x) \mid a(x)$ y $d(x) \mid b(x)$
2. Si $\exists c(x)$ t. q. $c(x) \mid a(x)$ y $c(x) \mid b(x)$, entonces $c(x) \mid d(x)$.[7]

Nota: Si $d(x)$ es un m.c.d de $a(x)$ y $b(x)$, entonces también lo es $u \cdot d(x)$ para todo $u \in K \setminus \{0\}$.
La expresión $\text{m. c. d}\{a(x), b(x)\}$ denota al m.c.d de $a(x)$ y $b(x)$ que es mónico.
Por ejemplo, si $a(x), b(x) \in \mathbb{Z}_5[x]$ y $3x^2 + x + 1$ es un m.c.d de $a(x)$ y $b(x)$, entonces $2(3x^2 + x + 1) = x^2 + 2x + 2$, $3(3x^2 + x + 1) = 4x^2 + 3x + 3$ y $4(3x^2 + x + 1) = 2x^2 + 4x + 4$ también son máximos comunes divisores de $a(x)$ y $b(x)$, y $\text{m. c. d}\{a(x), b(x)\} = x^2 + 2x + 2$.

Si $a(x), b(x) \in K[x]$, entonces un elemento $m(x) \in K[x]$ se dice que es un mínimo común múltiplo de $a(x)$ y $b(x)$ si verifica que:

1. $a(x) \mid m(x)$ y $b(x) \mid m(x)$
2. Si $\exists c(x)$ t. q. $a(x) \mid a(x)$ y $b(x) \mid c(x)$, entonces $m(x) \mid c(x)$.

Nota: Si $m(x)$ es un m.c.m de $a(x)$ y $b(x)$, entonces también lo es $u \cdot m(x)$ para todo $u \in K \setminus \{0\}$.
La expresión $\text{m. c. m}\{a(x), b(x)\}$ denota al m.c.m de $a(x)$ y $b(x)$ que es mónico.

Teorema 2. Sea K un cuerpo,

$$a(x) = u \cdot p_1(x)^{\alpha_1} \cdot p_2(x)^{\alpha_2} \cdot \cdots \cdot p_r(x)^{\alpha_r} \text{ y } b(x) = v \cdot p_1(x)^{\beta_1} \cdot p_2(x)^{\beta_2} \cdot \cdots \cdot p_r(x)^{\beta_r}$$

con $u, v \in K \setminus \{0\}$; $\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_r, \beta_r \in \mathbb{N}$; y $p_1(x), p_2(x), \ldots, p_r(x)$ polinomios mónicos e irreducibles de $K[x]$. Entonces:

$$\text{m. c. d}\{a(x), b(x)\} = p_1(x)^{\min\{\alpha_1, \beta_1\}} p_2(x)^{\min\{\alpha_2, \beta_2\}} \ldots p_r(x)^{\min\{\alpha_r, \beta_r\}}$$

$$\text{m. c. m}\{a(x), b(x)\} = p_1(x)^{\max\{\alpha_1, \beta_1\}} p_2(x)^{\max\{\alpha_2, \beta_2\}} \ldots p_r(x)^{\max\{\alpha_r, \beta_r\}}$$ [8]

Ejercicio: Dados los polinomios $a(x) = (x+1)(2x+3)$ y $b(x) = (x+2)(4x+1)$ de $\mathbb{Z}_5[x]$, calcular $\text{m. c. d}\{a(x), b(x)\}$ y $\text{m. c. m}\{a(x), b(x)\}$.

$a(x) = (x+1)(2x+3) = (x+1)\big(2 \cdot 3(2x+3)\big) = 2(x+1)(x+4)$, y
$b(x) = (x+2)(4x+1) = (x+2)\big(4 \cdot 4(4x+1)\big) = 4(x+2)(x+4)$.
Esto implica que $a(x) = (x+1)^1(x+2)^0(x+4)^1$ y $b(x) = (x+1)^0(x+2)^1(x+4)^1$.
Por tanto, aplicando el teorema anterior:

- $\text{m. c. d}\{a(x), b(x)\} = (x+1)^0(x+2)^0(x+4)^1 = x+4$
- $\text{m. c. m}\{a(x), b(x)\} = (x+1)^1(x+2)^1(x+4)^1 = (x+1)(x+2)(x+4)$ □

Propiedad de la división
Sea K un cuerpo y $a(x), b(x) \in K[x]$ t. q. $b(x) \neq 0$. Entonces existen dos únicos polinomios $q(x), r(x) \in K[x]$ tales que $a(x) = q(x)b(x) + r(x)$ y $\text{gr}\big(r(x)\big) < \text{gr}\big(b(x)\big)$.
A $q(x)$ y $r(x)$ se les llama, respectivamente, el cociente y el resto de dividir $a(x)$ entre $b(x)$ respectivamente, y los denotaremos como $q(x) = a(x)$ div $b(x)$ y $r(x) = a(x)$ mod $b(x)$.
Ejercicio: Calcular el resto de dividir $3x^3 + 4x^2 + 2x + 3$ entre $2x^2 + 2x + 1$ en $\mathbb{Z}_5[x]$.

[7] Igual a las explicaciones de m.c.m y m.c.d de números enteros.
[8] Este es el teorema 3 (regla de "solo comunes al menor exponente" y "comunes y no comunes al mayor exponente") del tema 2 con polinomios

$$\begin{array}{ll} 3x^3+4x^2+2x+3 & \underline{|2x^2+2x+1} \\ 2x^3+2x^2+x & \quad 4x+3 \\ \hline x^2+3x+3 & \\ 4x^2+4x+2 & \\ \hline 2x & \end{array}$$

Por tanto [9], $(3x^3+4x^2+2x+3) \text{ div } (2x^2+2x+1) = 4x+3$
y $(3x^3+4x^2+2x+3) \bmod (2x^2+2x+1) = 2x$ $\square$

3.1 Algoritmo de Euclides

Entrada: Dos polinomios $a(x)$ y $b(x)$ distintos de cero.
Salida: Un m.c.d de $a(x)$ y $b(x)$
Al principio, $\big(a_0(x), a_1(x)\big) = \big(a(x), b(x)\big)$. Mientras $a_1(x) \neq 0$, se sustituye $\big(a_0(x), a_1(x)\big)$ por $\big(a_1(x), a_0(x) \bmod a_1(x)\big)$. Si $a_1(x) = 0$, entonces devuelve $a_0(x)$ como salida.
Nota: El algoritmo anterior también sirve para calcular un m.c.m de dos polinomios, ya que si $a(x)$ y $b(x)$ son polinomios del mismo anillo y $d(x)$ es un m.c.d de $a(x)$ y $b(x)$, entonces $\big(a(x) \cdot b(x)\big) \text{ div } d(x)$ es un m.c.m de $a(x)$ y $b(x)$.
Ejercicio: Calcular un m.c.d y un m.c.m de los polinomios x^3+x^2+4x+4 y $2x^2+x+4$ de $\mathbb{Z}_5[x]$.

Usamos el algoritmo de Euclides para calcular un m.c.d de ambos polinomios:

$$\big(a_0(x), a_1(x)\big) = (x^3+x^2+4x+4, 2x^2+x+4) = (2x^2+x+4, 3x+3) = (3x+3, 0)$$

Por tanto, $3x+3$ es un m.c.d de los polinomios del enunciado. Ahora, tendremos en cuenta que
$\big((x^3+x^2+4x+4)(2x^2+x+4)\big) \text{ div } (3x+3) = (2x^5+3x^4+3x^3+x^2+1) \text{ div } (3x+3)$
es un m.c.m.

(El ejercicio continúa en la siguiente página)

[9] El procedimiento para la división de polinomios en cuerpos tipo $\mathbb{Z}_p$ es similar a la división de polinomios usual, excepto que las operaciones son módulo p. Tomando como ejemplo la división del ejercicio, $3x^3$ entre $2x^2$ es $4x$, porque $2x^2 \cdot 4x = (2 \cdot 4)x^3 = 3x^3$. Tras multiplicar $4x$ por el divisor y "restar" (sumar el inverso), luego dividimos $4x^2$ entre $2x^2$, lo cual da 3. Se repite el proceso hasta llegar a un polinomio de grado menor que el divisor ($2x$ en nuestro caso).

$$
\begin{array}{l|l}
2x^5+3x^4+3x^3+x^2 \quad +1 & |3x+3 \\
3x^5+3x^4 & \overline{4x^4+2x^3+4x^2+3x+2} \\
\hline
\quad x^4+3x^2+x^2 \quad +1 & \\
\quad 4x^4+4x^3+ & \\
\hline
\quad\quad 2x^3+x^2 \quad +1 & \\
\quad\quad 3x^3+3x^2 & \\
\hline
\quad\quad\quad 4x^2 \quad +1 & \\
\quad\quad\quad x^2+x & \\
\hline
\quad\quad\quad\quad x+1 & \\
\quad\quad\quad\quad 4x+4 & \\
\hline
\quad\quad\quad\quad\quad 0 &
\end{array}
$$

Por tanto $4x^4+2x^3+4x^2+3x+2$ es un m.c.m de x^3+x^2+4x+4 y $2x^2+x+4$ $\square$

Sea $a(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in K[x]$. Un elemento $\alpha\in K$ diremos que es una raíz de $a(x)$ si

$$a(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0$$

Ejercicio: Calcular las raíces del polinomio $a(x)=x^3+2x^2+x+2\in\mathbb{Z}_5[x]$

- $a(0)=0+0+0+2=2$
- $a(1)=1+2\cdot 1+1+2=2$
- $a(2)=2^3+2\cdot 2^2+2+2=3+3+2+2=0$
- $a(3)=3^3+2\cdot 3^2+3+2=2+3+3+2=0$
- $a(4)=4^3+2\cdot 4^2+4+2=4+2+4+2=2$

Por tanto, las raíces de $a(x)$ son 2 y 3. $\square$

Teorema 3 (Teorema del factor)**.** Sea $a(x)\in K[x]$ y $\alpha\in K$. Entonces α es una raíz de $a(x)$ si y solo si $(x-\alpha)\mid a(x)$.

Corolario 1. Un polinomio $a(x)\in K[x]\setminus\{0\}$ es un múltiplo de otro polinomio de grado uno si y solo si $a(x)$ tiene al menos una raíz.

Corolario 2. Sea $a(x)\in K[x]$ t. q. $\operatorname{gr}\big(a(x)\big)\in\{2,3\}$. Entonces $a(x)$ es irreducible si y solo si no tiene raíces.

Ejercicio: Estudiar la reducibilidad o irreducibilidad de los siguientes polinomios de $\mathbb{Z}_3[x]$:
$2x+1$; x^3+x+1; x^2+1

- $2x+1$ es irreducible porque es de grado 1.
- x^3+x+1 es reducible porque el 1 es una raíz.
- x^2+1 es irreducible porque es de grado 2 y no tiene raíces.

$\square$

Teorema 4. Sea $a(x) \in K[x]$. Entonces: [10]

- Si $\operatorname{gr}\big(a(x)\big) = 1$ entonces $a(x)$ es irreducible.
- Si $\operatorname{gr}\big(a(x)\big) \geq 2$ y $a(x)$ tiene una raíz o más entonces $a(x)$ es reducible.
- Si $\operatorname{gr}\big(a(x)\big) \in \{2, 3\}$ entonces $a(x)$ es irreducible si y solo si no tiene raíces.
- Si $\operatorname{gr}\big(a(x)\big) \in \{4, 5\}$ entonces $a(x)$ es irreducible si y solo si no tiene raíces y no es divisible por ningún polinomio mónico e irreducible de grado 2 de $K[x]$.
- Si $\operatorname{gr}\big(a(x)\big) \in \{6, 7\}$ entonces $a(x)$ es irreducible si y solo si no tiene raíces y no es divisible por ningún polinomio mónico e irreducible de grado 2 ni 3 de $K[x]$. [11]

Ejercicio: ¿Es irreducible el polinomio $x^4 + x^2 + 2 \in \mathbb{Z}_3[x]$?

Obsérvese que el polinomio no tiene raíces. Como es de grado 4, será irreducible si no lo divide ningún polinomio mónico e irreducible de grado 2 de $\mathbb{Z}_3[x]$.
Vamos a construir todos los polinomios mónicos e irreducibles de grado 2 de $\mathbb{Z}_3[x]$.
Para ello construimos todos los polinomios mónicos de grado 2 [12] y tachamos los que son reducibles (es decir, los que tienen raíces).

$$\begin{array}{ccc} \cancel{x^2} & x^2+1 & \cancel{x^2+2} \\ \cancel{x^2+x} & \cancel{x^2+x+2} & x^2+x+2 \\ \cancel{x^2+2x} & \cancel{x^2+2x+1} & x^2+2x+2 \end{array}$$

Por tanto, los polinomios mónicos e irreducibles de grado 2 de $\mathbb{Z}_3[x]$ son $x^2 + 1$, $x^2 + x + 2$ y $x^2 + 2x + 2$. Dividimos $x^4 + x + 2$ entre cada uno de estos polinomios, y si alguna división da de resto 0, el polinomio del enunciado es reducible.

- $(x^4 + x^2 + 2) \bmod (x^2 + 1) = 2 \neq 0$ [13]
- $(x^4 + x^2 + 2) \bmod (x^2 + x + 2) = 2x + 2 \neq 0$
- $(x^4 + x^2 + 2) \bmod (x^2 + 2x + 2) = x + 2 \neq 0$

Por tanto, como ninguno de los restos es 0, el polinomio $x^4 + x^2 + 2$ es irreducible.
□

Teorema 5 (Teorema del resto)**.** Sea $a(x) \in K[x]$ y $\alpha \in K$. Entonces $a(x) \bmod (x - \alpha) = a(\alpha)$.

Ejercicio: Sea $a(x) = 3x^4 + x^3 + 2x^2 + x + 4 \in \mathbb{Z}_5[x]$. Calcular el resto de dividir $a(x)$ entre $x + 4$.

$a(x) \bmod (x + 4) = a(x) \bmod (x - 1) = a(1) = 3 \cdot 1 + 1 + 2 \cdot 1 + 1 + 4 = 1$ □

Ejercicio: Calcular en $\mathbb{Z}_5[x]$ el resto de dividir $x^{1002} + x^{77} + 1$ entre $x + 3$

$(x^{1002} + x^{77} + 1) \bmod (x + 3) = (x^{1002} + x^{77} + 1) \bmod (x - 2) = 2^{1002} + 2^{77} + 1$.
Veamos el valor de 2^{1002} y 2^{77} en $\mathbb{Z}_5$.

$$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$$

- $1002 = 4 \cdot 250 + 2 \implies 2^{1002} = 2^{4 \cdot 250} \cdot 2^2 = 1^{250} \cdot 4 = 4$
- $77 = 4 \cdot 19 + 1 \implies 2^{77} = 2^{4 \cdot 19} \cdot 2^1 = 1^{19} \cdot 2 = 2$

Por tanto, $(x^{1002} + x^{77} + 1) \bmod (x + 3) = 2^{1002} + 2^{77} + 1 = 4 + 2 + 1 = \boxed{\mathbf{2}}$ □

[10] Esta es la generalización del corolario anterior.
[11] El patrón continúa de la siguiente manera: Si $\operatorname{gr}\big(a(x)\big) \in \{2n, 2n + 1\}$ entonces $a(x)$ es irreducible si y solo si no tiene raíces y no es divisible por ningún polinomio mónico e irreducible de grado $2, 3, \ldots, n - 1$ ni n de $K[x]$, para cualquier $n \in \mathbb{N} \setminus \{0\}$.
[12] Para esto hemos de tener en cuenta que un polinomio mónico de grado 2 tiene la forma $x^2 + ax + b$, donde $a, b \in \mathbb{Z}_3$. Por tanto, tenemos 3 posibilidades para a y para b, dando 9 en total.
[13] El procedimiento de las divisiones de polinomios a partir de ahora se deja como ejercicio para el lector.

Sea $a(x) \in K[x] \setminus \{0\}$. Si α es una raíz de $a(x)$, entonces $a(x) = (x-\alpha)^m \cdot b(x)$ [14] con $m \in \mathbb{N} \setminus \{0\}$ y $b(\alpha) \neq 0$. A m lo llamaremos la multiplicidad de la raíz α. Si $m = 1$ se dice que α es una raíz simple, y si $m \geq 2$ se dice que α es una raíz múltiple.

Proposición 6. Si $a(x) \in K[x] \setminus \{0\}$, la suma de las multiplicidades de todas las raíces de $a(x)$ es menor o igual que $\operatorname{gr}\big(a(x)\big)$. [15]

Ejercicio: Calcular las raíces y sus multiplicidades del polinomio $x^3 + 2x + 3 \in \mathbb{Z}_5[x]$.

Las raíces de $x^3 + 2x + 3$ son 2 y 4. Ahora vemos sus multiplicidades:

- Como 4 es una raíz, entonces $x - 4 = (x + 1) \mid (x^3 + 2x + 3)$. Tras dividir, obtenemos que $x^3 + 2x + 3 = (x - 4)(x^2 + 4x + 3)$. Como $x^2 + 4x + 3$ también se anula en 4, entonces la raíz 4 tiene multiplicidad mayor a 1. Volvemos a dividir entre $x - 4 = x + 1$ y obtenemos que $x^2 + 4x + 3 = (x - 4)(x + 3)$ $\implies x^3 + 2x + 3 = (x - 4)^2(x + 3)$. Como $x + 3$ no se anula en 4, concluimos que la raíz 4 tiene multiplicidad 2.
- Como 2 es una raíz, tiene multiplicidad de 1 o más. Basándonos en la proposición anterior, la suma de la multiplicidad de la raíz 4 (que es 2) y la de la raíz 2 no debe exceder $\operatorname{gr}(x^3 + 2x + 3) = 3$. Por tanto, la multiplicidad de la raíz 2 debe de ser 1. [16]

□

Teorema 6. Sea α una raíz de $a(x) \in K[x]$. Entonces α es una raíz múltiple si y solo si es también raíz de $a'(x)$, donde $a'(x)$ es la derivada de $a(x)$.

Nota: Si $a(x) = 4x^3 + 3x^2 + 2x + 1 \in \mathbb{Z}_5[x]$, entonces $a'(x) = 2x^2 + x + 2$. [17]

Ejercicio: Calcular las raíces múltiples del polinomio $a(x) = x^3 + 4x^2 + 5x + 2 \in \mathbb{R}[x]$.

Como es un polinomio de grado 3 en $\mathbb{R}[x]$, no tenemos forma de calcular sus raíces directamente [18]. Sin embargo, su derivada será de grado 2 y para calcular sus raíces podremos usar la fórmula cuadrática. Las raíces múltiples de $a(x)$ serán las raíces de $a'(x)$ que también anulan a $a(x)$. Como $a'(x) = 3x^2 + 8x + 5$:

$$3x^2 + 8x + 5 = 0 \implies x = \frac{-8 \pm \sqrt{8^2 - 4 \cdot 3 \cdot 5}}{2 \cdot 3} = \frac{-8 \pm \sqrt{4}}{6} = \begin{cases} -1 \\ \\ -\dfrac{5}{3} \end{cases}$$

Como $a(1) = 0$ y $a\left(-\dfrac{5}{3}\right) \neq 0$, podemos concluir que -1 es la única raíz múltiple de $a(x)$. □

Corolario 3. Ses $a(x) \in K[x]$ y $\alpha \in K$. Si $a(\alpha) = 0$, $a'(\alpha) = 0$, $a''(\alpha) = 0$, *dots*, $a^{m-1)}(\alpha) = 0$, y $a^{m)}(\alpha) \neq 0$,[19] entonces α es una raíz de multiplicidad m.

[14] Esto es debido al Teorema del factor.

[15] Como consecuencia de esto, si un polinomio de grado n tiene n raíces distintas entonces cada una de las raíces tiene multiplicidad 1.

[16] Si no se cae en la cuenta de esto, se puede hacer el mismo procedimiento que con la raíz 4.

[17] En general, si $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es un polinomio de $K[x]$, entonces su derivada es $a'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 + 0$. Si el cuerpo es de la forma $\mathbb{Z}_p$, entonces todos los coeficientes son obviamente módulo p.

[18] Al menos, no tenemos forma fácil de calcularlas.

[19] Donde $a''(x)$ denota la segunda derivada (derivada de la derivada) de $a(x)$, y $a^{n)}(x)$ denota la n-ésima derivada de $a(x)$.

Ejercicio: Calcular las raíces y sus multiplicidades del polinomio $x^3 + 2x + 3 \in \mathbb{Z}_5[x]$.

Las raíces de $x^3 + 2x + 3$ son 2 y 4.
$a'(x) = 3x^2 + 2$. Como $a'(2) = 4 \neq 0$, entonces 2 es una raíz de multiplicidad 1. Sin embargo, $a'(4) = 0$, así que la multiplicidad de la raíz 4 es mayor a 1.
$a''(x) = x$. Como $a'(4) \neq 0$, entonces concluimos que la multiplicidad de la raíz 4 es 2. □

Corolario 4. Sea $a(x) \in K[x] \setminus \{0\}$. Entonces las raíces múltiples de $a(x)$ son las raíces de $\mathrm{m.\,c.\,d}\{a(x), a'(x)\}$.

Ejercicio: Calcular las raíces múltiples del polinomio $x^5 + x^4 - 5x^3 - 5x^2 + 6x + 6 \in \mathbb{R}[x]$.

(Solución intencionalmente en blanco)

3.2 Cuerpos finitos

Sea $m(x) \in K[x] \setminus \{0\}$. Denotamos por $K[x]_{m(x)}$ al conjunto

$$K[x]_{m(x)} = \left\{ a(x) \in K[x] \ \text{ t. q. } \ \mathrm{gr}\big(a(x)\big) < \mathrm{gr}\big(m(x)\big) \right\}$$

En el conjunto anterior definimos una operación $\oplus$ y una operación $\odot$ de la siguiente manera: [20]

- $a(x) \oplus b(x) = \big(a(x) + b(x)\big) \bmod m(x)$[21]
- $a(x) \odot b(x) = \big(a(x) \cdot b(x)\big) \bmod m(x)$

Proposición 7. $\Big(K[x]_{m(x)}, \oplus, \odot\Big)$ es un anillo conmutativo.

Ejercicio: Calcular $(x+3) \oplus (x+4)$ y $(x+3) \odot (x+4)$ en el anillo $\mathbb{Z}_5[x]_{x^2+x+1}$.

- $(x+3) \oplus (x+4) = (x+3+x+4) \bmod (x^2+x+1) = (2x+2) \bmod (x^2+x+1) = 2x+2$
- $(x+3) \odot (x+4) = \big((x+3)(x+4)\big) \bmod (x^2+x+1) =$
  $(x^2 + 2x + 2) \bmod (x^2 + x + 1) = x + 1.$

□

Proposición 8. Sea $a(x) \in K[x]_{m(x)}$. Entonces $a(x)$ es una unidad del anillo $K[x]_{m(x)}$ si y solo si $\mathrm{m.\,c.\,d}\{a(x), m(x)\} = 1$.

Ejercicio: ¿Es $x + 3$ una unidad de $\mathbb{Z}_5[x]_{x^2+x+1}$?

Calculamos $\mathrm{m.\,c.\,d}\{x^2 + x + 1, x + 3\}$ usando el algoritmo de Euclides:

$$\big(a_0(x), a_1(x)\big) = (x^2 + x + 1, x + 3) = (x + 3, 2) = (2, 0)$$

Por tanto, 2 es un m.c.d de $x^2 + x + 1$ y $x + 3$, así que $3 \cdot 2 = 1$ también es un m.c.d de ambos polinomios. Por consiguiente, $\mathrm{m.\,c.\,d}\{x^2 + x + 1, x + 3\} = 1 \implies x + 3$ es una unidad del anillo $\mathbb{Z}_5[x]_{x^2+x+1}$ □

Corolario 5. $K[x]_{m(x)}$ es un cuerpo si y solo si $m(x)$ es un polinomio irreducible.

[20] Al igual que en el tema 2, conforme avancemos iremos usando los operadores + y · normales.

[21] Nótese que si $\mathrm{gr}\big(a(x)\big) < \mathrm{gr}\big(m(x)\big)$ y $\mathrm{gr}\big(b(x)\big) < \mathrm{gr}\big(m(x)\big)$, entonces $\mathrm{gr}\big(a(x) + b(x)\big) = \max\Big\{ \mathrm{gr}\big(a(x)\big), \mathrm{gr}\big(b(x)\big) \Big\} < \mathrm{gr}\big(m(x)\big) \implies \big(a(x)+b(x)\big) \bmod m(x) = a(x)+b(x)$. Por tanto, la definición de $a(x) \oplus b(x)$ en $K[x]_{m(x)}$ puede directamente ser $a(x) \oplus b(x) = a(x) + b(x)$. Sin embargo, no es el caso con el operador $\odot$.

Ejercicio: ¿Es $\mathbb{Z}_5[x]_{x^2+x+1}$ un cuerpo?

Sí, ya que $x^2+x+1 \in \mathbb{Z}_5[x]$ es un polinomio de grado 2 sin raíces y por tanto es irreducible. $\square$

Proposición 9. El cardinal de un cuerpo finito[22] siempre es la potencia de un número primo. Además, si p es un número primo positivo y $m(x) \in \mathbb{Z}_p[x] \setminus \{0\}$, entonces $\mathbb{Z}_p[x]_{m(x)}$ tiene cardinal igual a $p^{\text{gr}\left(m(x)\right)}$.

Ejercicio: ¿Existen cuerpos de cardinal 10?

No, porque $10 = 2 \cdot 5$ no es la potencia de un número primo. $\square$

Ejercicio: Dar un cuerpo de cardinal 9.

Sabemos que $\mathbb{Z}_3[x]_{x^2+1}$ es un anillo conmutativo de cardinal $3^2 = 9$. Además, como $x^2+1 \in \mathbb{Z}_3[x]$ es de grado 2 y no tiene raíces, entonces es irreducible y por tanto $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo de cardinal 9. $\square$

Ejercicio: Dar un cuerpo de cardinal 16.

Sabemos que $\mathbb{Z}_3[x]_{x^4+x+1}$ es un anillo conmutativo de cardinal $2^4 = 16$. Además, como $x^4+x+1 \in \mathbb{Z}_2[x]$ es irreducible (demostrado más adelante), tenemos que $\mathbb{Z}_2[x]_{x^4+x+1}$ es un cuerpo de cardinal 16.

Nótese que $x^4+x+1 \in \mathbb{Z}_2[x]$ no tiene raíces. Será irreducible si no lo divide ningun polinomio mónico e irreducible de grado 2.
Los polinomios mónicos de grado 2 de $\mathbb{Z}_2[x]$ son x^2, x^2+1, x^2+x y x^2+x+1. El único irreducible es x^2+x+1 ya que no tiene raíces. Como $(x^4+x+1) \bmod (x^2+x+1) = 1 \neq 0$, entonces podemos afirmar que x^4+x+1 es irreducible. $\square$

Proposición 10. Sea $m(x) \in K[x] \setminus \{0\}$ y $a(x) \in K[x]_{m(x)}$. Si existen $u(x), v(x) \in K[x]$ tales que $a(x)u(x) + m(x)v(x) = 1$, entonces $a(x)^{-1} = u(x) \bmod m(x)$ en $K[x]_{m(x)}$.

3.3 Algoritmo extendido de Euclides

Entrada: $a(x), b(x) \in K[x] \setminus \{0\}$
Salida: $d(x), s(x), t(x) \in \mathbb{K}[x]$ t. q. $d(x)$ es un m.c.d de $a(x)$ y $b(x)$, y $a(x)s(x) + b(x)t(x) = d(x)$
Al principio,

$$\begin{aligned} \big(a_0(x), a_1(x)\big) &= \big(a(x), b(x)\big) \\ \big(s_0(x), s_1(x)\big) &= (1, 0) \\ \big(t_0(x), t_1(x)\big) &= (0, 1) \end{aligned}$$

Mientras, $a_1(x) \neq 0$, se toma $q(x) = a_0(x)$ div $a_1(x)$ y se sustituyen

$$\begin{gathered} \big(a_0(x), a_1(x)\big) \text{ por } \big(a_1(x), a_0(x) - q(x)a_1(x)\big) \\ \big(s_0(x), s_1(x)\big) \text{ por } \big(s_1(x), s_0(x) - q(x)s_1(x)\big) \\ \big(t_0(x), t_1(x)\big) \text{ por } \big(t_1(x), t_0(x) - q(x)t_1(x)\big) \end{gathered}$$

Cuando $a_1(x) = 0$, entonces se devuelve como salida $d(x) = a_0(x), s(x) = s_0(x), t(x) = t_0(x)$.[23]

[22] Con "cuerpo finito" nos referimos a un cuerpo con una cantidad finita de elementos. Por tanto, $\mathbb{Z}_3$ y $\mathbb{Z}_5[x]_{x^2+x+1}$ son cuerpos finitos, pero $\mathbb{Q}$ y $\mathbb{R}$ no lo son.

[23] Al igual que con el algoritmo de Euclides, este es el mismo algoritmo que en el tema 2, solo que con polinomios.

Ejercicio: Calcular el inverso para el producto de $2x+1$ en al anillo $\mathbb{Z}_5[x]_{x^2+2x+1}$

Sabemos que $2x+1 = 2(x+3)$ y $x^2+2x+1 = (x+1)^2$, y que $x+1$ y $x+3$ son mónicos e irreducibles. Por tanto, $\text{m. c. d}\{x^2+2x+1, 2x+1\}$ $= \text{m. c. d}\left\{2(x+3), (x+1)^2\right\} = (x+3)^0(x+1)^0 = 1$, así que $\exists(2x+1)^{-1}$. Para calcularlo aplicamos el algoritmo extendido de Euclides a x^2+2x+1 y $2x+1$:

$$\begin{array}{lcccccc} \big(a_0(x), a_1(x)\big) & = & (x^2+2x+1, 2x+1) & \overset{q=3x+2}{=} & (2x+1, 4) & = & (4, 0) \\ \big(s_0(x), s_1(x)\big) & = & (1, 0) & = & (0, 1) & = & (1, \dots) \\ \big(t_0(x), t_1(x)\big) & = & (0, 1) & = & (1, 2x+3) & = & (2x+3, \dots) \end{array}$$

El algoritmo nos proporciona la igualdad $1(x^2+2x+1) + (2x+3)(2x+1) = 4$. Tras multiplicar ambos lados por 4 tenemos que $4(x^2+2x+1) + (3x+2)(2x+1) = 1$. Por tanto, $(3x+2) \mod (x^2+2x+1) = 3x+2$ es el inverso de $2x+1$ $\square$

Ejercicio: Resolver en el anillo $\mathbb{Z}_7[x]_{x^2+x+1}$ la ecuación $(3x+4)A + 3x + 1 = (2x+5)A + x + 5$.[24] [25]

$$\begin{array}{ll} & (3x+4)A \ + \ 3x+1 = (2x+5)A \ + \ x+5 \\ \Longrightarrow & (3x+4 \ - \ 2x-5)A = x+5 \ - \ 3x-1 \\ \Longrightarrow & (x+6)A = 5x+4 \\ \Longrightarrow & A = (x+6)^{-1}(5x+4) \end{array}$$

Como $\text{m. c. d}\{x+6, x^2+x+1\} = 1$, sabemos que $\exists(x+6)^{-1}$ en $\mathbb{Z}_7[x]_{x^2+x+1}$. Para calcularlo usamos el algoritmo extendido de Euclides con x^2+x+1 y $x+6$ como entrada.

$$\begin{array}{lcccccc} \big(a_0(x), a_1(x)\big) & = & (x^2+x+1, x+6) & \overset{q(x)=x+2}{=} & (x+6, 3) & = & (3, 0) \\ \big(s_0(x), s_1(x)\big) & = & (1, 0) & = & (0, 1) & = & (1, \dots) \\ \big(t_0(x), t_1(x)\big) & = & (0, 1) & = & (1, 6x+5) & = & (6x+5, \dots) \end{array}$$

El algoritmo nos proporciona la igualdad $1(x^2+x+1) + (6x+5)(x+6) = 3$ $\Longrightarrow 5(x^2+x+1) + (2x+4)(x+6) = 5 \cdot 3 = 1$. Por tanto, en $\mathbb{Z}_7[x]_{x^2+x+1}$, $(x+6)^{-1} = (2x+4) \mod (x^2+x+1) = 2x+4$. Así que

$$A = (2x+4)(5x+4) = (3x^2+2) \mod (x^2+x+1) = \boxed{\mathbf{4x+6}} \quad \square$$

[24] Aquí ya se usan de nuevo los operadores $+$ y $\cdot$ en lugar de $\oplus$ y $\odot$

[25] Cabe señalar que la incógnita de esta ecuación es A, ya que x es la indeterminada de los polinomios.

4 Matrices con coeficientes en un cuerpo

A diferencia de los tres anteriores, este tema y sus contenidos deberían de ser en su mayoría familiares a aquellos que hayan cursado bachillerato de ciencias. Las matrices son la base del álgebra lineal, por lo que casi no hace falta decir que estarán presentes casi a lo largo del resto del temario.
No obstante, este tema no consiste en *todo* lo que tiene que ver con matrices. Se irán introduciendo más conceptos relacionados a las matrices cuando sean necesarios a lo largo de temas posteriores.

Sean los conjuntos $I = \{1, 2, \dots, m\}$ y $J = \{1, 2, \dots, n\}$. Una matriz de orden $m \times n$ sobre un cuerpo K es una aplicación [1]

$$\begin{array}{rccc} A: & I \times J & \longrightarrow & K \\ & (i,j) & \longrightarrow & a_{ij} \end{array}$$

Normalmente a la matriz A la representaremos de la forma

$$A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \dots & a_{m\,n} \end{pmatrix}$$

Y diremos que A es una matriz de m filas y n columnas.
Denotaremos por $\mathcal{M}_{m\times n}(K)$ al conjunto de todas las matrices de orden $m \times n$ sobre el cuerpo K.

Proposición 1. $\#\mathcal{M}_{m\times n}(\mathbb{Z}_p) = p^{m\cdot n}$ [2]

Ejemplo:

$$\mathcal{M}_{2\times 3}(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right\}$$
$$\#\mathcal{M}_{2\times 3}(\mathbb{Z}_2) = 2^{2\cdot 3} = 2^6 = 64$$

4.1 Suma de matrices

Si $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \dots & a_{m\,n} \end{pmatrix}$ y $B = \begin{pmatrix} b_{1\,1} & b_{1\,2} & \dots & b_{1\,n} \\ b_{2\,1} & b_{2\,2} & \dots & b_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m\,1} & b_{m\,2} & \dots & b_{m\,n} \end{pmatrix}$ son dos matrices de $\mathcal{M}_{m\times n}(K)$, entonces la matriz

$$A + B = \begin{pmatrix} a_{1\,1} + b_{1\,1} & a_{1\,2} + b_{1\,2} & \dots & a_{1\,n} + b_{1\,n} \\ a_{2\,1} + b_{2\,1} & a_{2\,2} + b_{2\,2} & \dots & a_{2\,n} + b_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} + b_{m\,1} & a_{m\,2} + b_{m\,2} & \dots & a_{m\,n} + b_{m\,n} \end{pmatrix}$$

es también una matriz de $\mathcal{M}_{m\times n}(K)$.

Proposición 2. $\mathcal{M}_{m\times n}(K)$ con la operación suma de matrices tiene estructura de grupo abeliano. Esto es, la suma de matrices es conmutativa, asociativa, tiene elemento neutro (denotado 0) y todo elemento tiene inverso para la suma (Al inverso de $A \in \mathcal{M}_{m\times n}(K)$ lo denotaremos $-A$)

---

[1] Esto quiere decir que a cada posición (i, j) donde $i \in I$ y $j \in J$, la matriz A le asocia un elemento de K; por tanto, las matrices entran bajo la definición de aplicación.
[2] Donde p es un número primo positivo.

Nota:

$0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ es el elemento neutro; y

$$-\begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \dots & a_{m\,n} \end{pmatrix} = \begin{pmatrix} -a_{1\,1} & -a_{1\,2} & \dots & -a_{1\,n} \\ -a_{2\,1} & -a_{2\,2} & \dots & -a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m\,1} & -a_{m\,2} & \dots & -a_{m\,n} \end{pmatrix}$$

Ejercicio: Sean $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} 3 & 4 & 3 \\ 2 & 3 & 2 \end{pmatrix}$ dos elementos de $\mathcal{M}_{2\times 3}(\mathbb{Z}_5)$.

a) Calcular $A + B$.

b) ¿Cuál es el elemento neutro de la suma en $\mathcal{M}_{2\times 3}(\mathbb{Z}_5)$?

c) Calcular $-A$

- $A + B = \begin{pmatrix} 1+3 & 2+4 & 3+3 \\ 0+2 & 4+3 & 1+2 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 1 \\ 2 & 2 & 3 \end{pmatrix}$ □
- El elemento neutro es $0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ □
- $-A = \begin{pmatrix} -1 & -2 & -3 \\ -0 & -4 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 2 \\ 0 & 1 & 4 \end{pmatrix}$ □

4.2 Producto de matrices

Si $A \in \mathcal{M}_{m\times n}(K)$ y $B \in \mathcal{M}_{n\times p}(K)$, entonces $A \cdot B \in \mathcal{M}_{m\times p}(K)$. Además, si

$\begin{pmatrix} a_{i\,1}, & a_{i\,2}, & \dots, & a_{i\,n} \end{pmatrix}$ [3] 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 de posición (i, j) en la matriz $A \cdot B$ es
$(a_{i\,1} \cdot b_{1\,j}) + (a_{i\,2} \cdot b_{2\,j}) + \dots + (a_{i\,n} \cdot b_{n\,j})$ [4]

Ejercicio: Sean $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix}$ y $B = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \\ 3 & 2 & 3 & 1 \end{pmatrix}$ dos matrices con coeficientes en $\mathbb{Z}_7$.

Calcular $A \cdot B$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 2 \\ 3 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 2 + 2\cdot 1 + 3\cdot 3 & 1\cdot 3 + 2\cdot 1 + 3\cdot 2 & \dots \\ 3\cdot 2 + 4\cdot 1 + 2\cdot 3 & \dots & \dots \end{pmatrix} = \begin{pmatrix} 6 & 4 & 1 & 5 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

□

[3] A las matrices de solo una fila se las denota con comas entre cada uno de los elementos, y son prácticamente intercambiables con n-tuplas.

[4] Es decir, se multiplica, elemento por elemento, la fila i por la columna j.

Una matriz de orden $n \times n$ se dice que es cuadrada de orden n.

Proposición 3. $\left(\mathcal{M}_{n\times n}(K), +, \cdot\right)$ es un anillo no conmutativo. Además, el elemento neutro para el producto es $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$, a la cual llamaremos la matriz identidad de orden n.

Ejercicio: Sean $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$ dos elementos de $\mathcal{M}_{2\times 2}(\mathbb{Q})$. Comprobar que $A \cdot B \neq B \cdot A$

- $A \cdot B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 11 & 6 \end{pmatrix}$
- $B \cdot A = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 2 & 4 \end{pmatrix}$

$\begin{pmatrix} 5 & 2 \\ 11 & 6 \end{pmatrix} \neq \begin{pmatrix} 7 & 10 \\ 2 & 4 \end{pmatrix} \implies AB \neq BA$ □

4.3 Determinantes

Dada una matriz cuadrada A, se define el determinante de A, denotado $|A|$ ó $\det(A)$, de la siguiente manera:

- $\left| \ a \ \right| = a$
- $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$ [5]
- $\begin{vmatrix} a & b & c \\ p & q & r \\ x & y & z \end{vmatrix} = aqz + brx + cpy \ - \ ary - bpz - cqx$

Ejercicio: Calcular $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix}$ y $\begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 3 & 1 & 4 \end{vmatrix}$ en $\mathbb{Z}_5$.

- $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 4 - 1 = 3$
- $\begin{vmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 3 & 1 & 4 \end{vmatrix} = 4 + 1 \cancel{+2} \cancel{-2} - 3 - 3 = -1 = 4$ [6]

□

[5] El determinante de una matriz en su "forma expandida" también se denota sustituyendo los paréntesis que delimitan la matriz por barras verticales, como en $|A|$.

[6] Nótese que, debido a que el cálculo de determinantes se reduce a sumas y multiplicaciones, el determinante de una matriz con coeficientes en $\mathbb{Z}_p$ (con p primo) puede obtenerse haciendo las operaciones en $\mathbb{Z}$ y tomando el resto de dividir el resultado entre p.

Dada una matriz $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \dots & a_{n\,n} \end{pmatrix} \in \mathcal{M}_{n\times n}(K)$, denotaremos por $A_{i\,j}$ a la matriz que se obtiene a partir de A tras quitarle la fila i y la columna j. Llamaremos adjunto del elemento $a_{i\,j}$ a

$$\alpha_{i\,j} = (-1)^{i+j} \cdot |A_{i\,j}|$$

Ejercicio: Dada la matriz $A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ 3 & 3 & 1 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}_5)$, calcular $\alpha_{1\,2}$.

$$A_{1\,2} = \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix} \implies \alpha_{1\,2} = (-1)^{1+2} \begin{vmatrix} 1 & 1 \\ 3 & 1 \end{vmatrix} = 4(1-3) = \boxed{\mathbf{2}} \quad \square$$

4.4 Desarrollo de Laplace

Si $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \dots & a_{n\,n} \end{pmatrix} \in \mathcal{M}_{n\times n}(K)$, entonces:

1. Desarrollo de Laplace por la fila i: $|A| = a_{i\,1}\alpha_{i\,1} + a_{i\,2}\alpha_{i\,2} + \cdots + a_{i\,n}\alpha_{i\,n}$
2. Desarrollo de Laplace por la columna j: $|A| = a_{1\,j}\alpha_{1\,j} + a_{2\,j}\alpha_{2\,j} + \cdots + a_{n\,j}\alpha_{n\,j}$

Ejercicio: Calcular el determinante de $A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 2 & 0 & 1 & 3 \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5)$.

Usamos el desarrollo de Laplace por la segunda columna: [7]

$$\begin{vmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 2 & 0 & 1 & 3 \end{vmatrix} = 2\alpha_{1\,2} + 0\alpha_{2\,2} + 1\alpha_{3\,2} + 0\alpha_{4\,2} = 2\cdot(-1)^3 \begin{vmatrix} 2 & 1 & 1 \\ 3 & 0 & 1 \\ 2 & 1 & 3 \end{vmatrix} + 1\cdot(-1)^5 \begin{vmatrix} 1 & 3 & 1 \\ 2 & 1 & 1 \\ 2 & 1 & 3 \end{vmatrix}$$

$$= 2\cdot 4\cdot 4 + 1\cdot 4\cdot 0 = \boxed{\mathbf{2}} \quad \square$$

[7] Nótese que, si en el desarrollo de Laplace hay muchos ceros en la fila o columna, entonces no hace falta calcular sus adjuntos. Por tanto, cuando calculemos determinantes de órdenes mayores a 3, buscaremos maximizar los ceros en alguna fila o columna.

Si $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \dots & a_{m\,n} \end{pmatrix} \in \mathcal{M}_{m\times n}(K)$, entonces llamaremos matriz transpuesta de A, y denotaremos A^t, a la matriz

$$A^t = \begin{pmatrix} a_{1\,1} & a_{2\,1} & \dots & a_{m\,1} \\ a_{1\,2} & a_{2\,2} & \dots & a_{m\,2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1\,n} & a_{2\,n} & \dots & a_{m\,n} \end{pmatrix} \in \mathcal{M}_{n\times m}(K)$$

Propiedades de los determinantes

Sea $A \in \mathcal{M}_{n\times n}(K)$. Entonces:

1. $|A| = |A^t|$ [8]
2. Si intercambiamos dos filas o dos columnas de A obtenemos otra matriz cuyo determinante es $-A$.
3. Si multiplicamos todos los elementos de una fila o columna de A por un elemento $\alpha \in K$, obtenemos otra matriz cuyo determinante es $\alpha|A|$.
4. Si a una fila de A le sumamos otra fila distinta de A multiplicada por un elemento cualquiera de K, obtenemos otra matriz con el mismo determinante que A. Esto también cumple si esta operación la hacemos con columnas en vez de filas.
5. Sea $B \in \mathcal{M}_{n\times n}(K)$, entonces $|A \cdot B| = |A| \cdot |B|$. [9]

Ejercicio: Calcular el determinante de $A = \begin{pmatrix} 2 & 3 & 4 & 0 \\ 3 & 1 & 2 & 2 \\ 4 & 3 & 3 & 1 \\ 2 & 3 & 3 & 2 \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5)$. [10]

$$\begin{matrix}(F_1)\\(F_2)\\(F_3)\\(F_4)\end{matrix}\begin{vmatrix} 2 & 3 & 4 & 0 \\ 3 & 1 & 2 & 2 \\ 4 & 3 & 3 & 1 \\ 2 & 3 & 3 & 2 \end{vmatrix} \overset{\substack{F_2 \to F_2 + F_1 \\ F_3 \to F_3 + 3F_1 \\ F_4 \to F_4 + 4F_1}}{=\!=\!=} \begin{vmatrix} 2 & 3 & 4 & 0 \\ 0 & 4 & 1 & 2 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 4 & 2 \end{vmatrix} = 2 \cdot (-1)^2 \cdot \begin{vmatrix} 4 & 1 & 2 \\ 2 & 0 & 1 \\ 0 & 4 & 2 \end{vmatrix} + 0 + 0 + 0$$

$$= 2(0 + 0 + \not{4} - 0 - \not{4} - 4) = \boxed{\mathbf{2}} \quad \square$$

[8] Como consecuencia de esto, todas las propiedades de los determinantes que funcionan mediante operaciones con filas también funcionan con columnas de la misma manera.

[9] Por tanto, $|A \cdot B| = |B \cdot A|$ aunque $A \cdot B \neq B \cdot A$.

[10] En la resolución de este ejercicio y los siguientes, la notación $F_i \to F_i + \alpha F_j$ quiere decir "se le suma a la fila número i la fila j multiplicada por α". Como hemos visto en las propiedades de los determinantes, esto da una matriz con determinante idéntico.

Ejercicio: Calcular el determinante de $A = \begin{pmatrix} 1 & 2 & 2 & 4 & 5 \\ 2 & 4 & 3 & 1 & 3 \\ 6 & 1 & 4 & 2 & 3 \\ 3 & 3 & 1 & 4 & 2 \\ 3 & 0 & 2 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{5\times 5}(\mathbb{Z}_7)$.

$$|A| = \begin{vmatrix} 1 & 2 & 2 & 4 & 5 \\ 2 & 4 & 3 & 1 & 3 \\ 6 & 1 & 4 & 2 & 3 \\ 3 & 3 & 1 & 4 & 2 \\ 3 & 0 & 2 & 1 & 0 \end{vmatrix} \overset{F_2 \to F_2 + 5F_1}{=\!=} \begin{vmatrix} 1 & 2 & 2 & 4 & 5 \\ 0 & 0 & 6 & 0 & 0 \\ 6 & 1 & 4 & 2 & 3 \\ 3 & 3 & 1 & 4 & 2 \\ 3 & 0 & 2 & 1 & 0 \end{vmatrix} = 6 \cdot (-1)^5 \begin{vmatrix} 1 & 2 & 4 & 5 \\ 6 & 1 & 2 & 3 \\ 3 & 3 & 4 & 2 \\ 3 & 0 & 1 & 0 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 2 & 4 & 5 \\ 6 & 1 & 2 & 3 \\ 3 & 3 & 4 & 2 \\ 3 & 0 & 1 & 0 \end{vmatrix} \overset{\substack{F_2 \to F_2 + F_1 \\ F_3 \to F_3 + 4F_1 \\ F_4 \to F_4 + 4F_1}}{=\!=} \begin{vmatrix} 1 & 2 & 4 & 5 \\ 0 & 3 & 6 & 1 \\ 0 & 4 & 6 & 1 \\ 0 & 1 & 3 & 6 \end{vmatrix} = 1(-1)^2 \begin{vmatrix} 3 & 6 & 1 \\ 4 & 6 & 1 \\ 1 & 3 & 6 \end{vmatrix}$$

$$= 3 + \cancel{6} + 5 - \cancel{6} - 4 - 2 = \boxed{\mathbf{2}} \quad \square$$

Una matriz $A \in \mathcal{M}_{n\times n}(K)$ es regular si tiene inversa para el producto, es decir, si existe $B \in \mathcal{M}_{n\times n}(K)$ t. q. $AB = BA = I_n$. En dicho caso, diremos que B es la inversa de A, denotada A^{-1}.

La matriz adjunta de $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \dots & a_{n\,n} \end{pmatrix} \in \mathcal{M}_{n\times n}(K)$ se define como la matriz

$\overline{A} = \begin{pmatrix} \alpha_{1\,1} & \alpha_{1\,2} & \dots & \alpha_{1\,n} \\ \alpha_{2\,1} & \alpha_{2\,2} & \dots & \alpha_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n\,1} & \alpha_{n\,2} & \dots & \alpha_{n\,n} \end{pmatrix}$, donde $\alpha_{i\,j}$ es el adjunto del elemento $a_{i\,j}$.

Teorema 1. Sea $A \in \mathcal{M}_{n\times n}(K)$. Entonces A es regular si y solo si $|A| \neq 0$. Además, en dicho caso, $A^{-1} = |A|^{-1} \cdot (\overline{A})^t$. [11]

Ejercicio: Calcular la inversa de $A = \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_7)$.

$|A| = 4 - 2 = 2 \implies |A|^{-1} = 4$

$\overline{A} = \begin{pmatrix} 4 & -1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 5 & 1 \end{pmatrix} \implies (\overline{A})^t = \begin{pmatrix} 4 & 5 \\ 6 & 1 \end{pmatrix}$

Por tanto,

$$A^{-1} = |A|^{-1} \cdot (\overline{A})^t = 4 \begin{pmatrix} 4 & 5 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 3 & 4 \end{pmatrix} \quad \square$$

[11] No se ha definido el producto de una matriz por un elemento de su cuerpo, pero es obvio que el producto de $k \in K$ por la matriz $A \in \mathcal{M}_{m\times n}(K)$ da como resultado la matriz A con todos sus elementos multiplicados por k.

Ejercicio: Calcular la inversa de $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}_5)$.

$|A| = \cancel{2} + 2 + 4 - \cancel{2} - 3 - 1 = 2 \implies |A|^{-1} = 3$

$$\overline{A} = \begin{pmatrix} \begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 4 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 4 & 2 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ \begin{vmatrix} 2 & 3 \\ 2 & 3 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ 4 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 4 & 2 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 0 & 2 \\ 0 & 4 & 4 \end{pmatrix} \implies (\overline{A})^t = \begin{pmatrix} 1 & 4 & 0 \\ 2 & 0 & 4 \\ 4 & 2 & 4 \end{pmatrix}$$

Por tanto,

$$A^{-1} = |A|^{-1} \cdot (\overline{A})^t = 3 \begin{pmatrix} 1 & 4 & 0 \\ 2 & 0 & 4 \\ 4 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 0 \\ 1 & 0 & 2 \\ 2 & 1 & 2 \end{pmatrix} \quad \square$$

4.5 Otra forma de calcular inversas: operaciones por filas

Si A es una matriz con coeficientes en un cuerpo K, entonces las operaciones elementales por filas[12] que se pueden hacer en A son:

- Intercambiar dos filas [13]
- Multiplicar todos los elementos de una fila por $\alpha \in K \setminus \{0\}$ [14]
- Sumar a una fila otra distinta multiplicada por un elemento $\alpha \in K$ [15]

Usaremos operaciones por filas para calcular inversas de matrices [16] , como en el siguiente ejemplo en el que calculamos la inversa de la matriz del ejercicio anterior (Obviamente, en $\mathbb{Z}_5$):

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 2 & 3 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{pmatrix} \overbrace{\substack{F_2 \to F_2 + F_1 \\ F_3 \to F_3 + 3F_1}} \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 4 & 1 & 1 & 1 & 0 \\ 0 & 3 & 0 & 3 & 0 & 1 \end{pmatrix} \overbrace{\substack{F_3 \to 2F_3 \\ F_2 \to F_2 + F_3 \\ F_1 \to F_1 + 3F_3}} \begin{pmatrix} 1 & 0 & 3 & 4 & 0 & 1 \\ 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 \end{pmatrix} \dots$$

$$\dots \overbrace{\substack{F_2 \leftrightarrow F_3 \\ F_1 \to F_1 + 2F_3}} \begin{pmatrix} 1 & 0 & 0 & 3 & 2 & 0 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 & 1 & 2 \end{pmatrix} \implies \begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 2 & 0 \\ 1 & 0 & 2 \\ 2 & 1 & 2 \end{pmatrix}$$

[12] Estas operaciones por filas sirven para obtener una matriz similar a A, es decir, con algunas características (que se verán más tarde) idénticas. Las operaciones por filas son esenciales para triangularizar matrices, por ejemplo.

[13] Esto será denotado por $F_i \leftrightarrow F_j$.

[14] Esto será denotado por $F_i \to \alpha F_i$.

[15] Esto será denotado por $F_i \to F_i + \alpha F_j$.

[16] Este procedimiento consiste en generar una matriz la cual consista de la matriz cuya inversa queremos calcular, unida a la identidad del mismo orden por la derecha, y hacer operaciones por filas hasta que nos quede la identidad por la izquierda y otra nueva matriz por la derecha. La matriz nueva será la inversa que queremos calcular

Ejercicio: Resolver en el anillo $\mathcal{M}_{2\times 2}(\mathbb{Z}_7)$ la ecuación

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

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

$$\implies \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} X = \begin{pmatrix} 0 & 6 \\ 6 & 6 \end{pmatrix}$$

$$\implies \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} X = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 6 \\ 6 & 6 \end{pmatrix}$$ [17]

$$\implies X = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 6 \\ 6 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}^{-1} \cdot \left[\overline{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}} \right]^t = (1)^{-1} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^t = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}$$

Por tanto, $X = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 0 & 6 \\ 6 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 6 \\ 6 & 0 \end{pmatrix}$ $\square$

Ejercicio: Resolver el siguiente sistema de ecuaciones en el anillo $\mathcal{M}_{2\times 2}(\mathbb{Z}_7)$:

$$\begin{cases} A + 2B = \begin{pmatrix} 3 & 2 \\ 0 & 0 \end{pmatrix} & (1) \\ 2A + B = \begin{pmatrix} 3 & 0 \\ 4 & 4 \end{pmatrix} & (2) \end{cases}$$

Tras multiplicar la ecuación (1) por 3, tenemos que:

$$\left.\begin{cases} 3A + B = \begin{pmatrix} 4 & 1 \\ 0 & 0 \end{pmatrix} & (1') \\ 2A + B = \begin{pmatrix} 3 & 0 \\ 4 & 4 \end{pmatrix} & (2) \end{cases}\right\} \text{Sumamos } (1') \text{ y } (2) \implies 2B = \begin{pmatrix} 2 & 1 \\ 4 & 4 \end{pmatrix}$$

Por tanto, $B = 3\begin{pmatrix} 2 & 1 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$, y entonces:

$$A = \begin{pmatrix} 3 & 2 \\ 0 & 0 \end{pmatrix} - 2B = \begin{pmatrix} 3 & 2 \\ 0 & 0 \end{pmatrix} + 3\begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} \implies A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

La solución del sistema es $(A, B) = \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} \right)$ $\square$

[17] Nótese que como el producto de matrices no es conmutativo, hemos de diferenciar entre multiplicar por la izquierda en ambos lados (como se ha hecho en este ejercicio) y multiplicar por la derecha en ambos lados.

5 Espacios vectoriales

Los espacios vectoriales son el segundo gran concepto que el álgebra lineal estudia, al igual que las matrices son el primero. Aunque en el bachillerato de ciencias se suele dar una breve introducción a los espacios vectoriales, ésta es más bien orientada a la geometría euclídea en el plano ($\mathbb{R}^2$) y en el espacio ($\mathbb{R}^3$); sin embargo, este tema es más generalizado y apenas tiene relación con la geometría.

Sea K un cuerpo. Diremos que un conjunto V tiene estructura de espacio vectorial sobre K si verifica lo siguiente:

1. En V hay una operación $+$ tal que $(V,+)$ es un grupo abeliano[1]. Se denotará por $\vec{0}$ al elemento neutro de $+$ y al inverso de $\vec{v} \in V$ se le denotará como $-\vec{v}$.
2. Existe una aplicación $K \times V \longrightarrow V;\ (a,\vec{v}) \longrightarrow a \cdot \vec{v}$ que cumple las siguientes propiedades:
   - $a \cdot (\vec{u}+\vec{v}) = a\vec{u} + a\vec{v} \quad \forall a \in K;\ \vec{u},\vec{v} \in V$
   - $(a+b)\vec{v} = a\vec{v} + b\vec{v} \quad \forall a,b \in K;\ \vec{v} \in V$
   - $a \cdot (b\vec{v}) = (ab)\vec{v} \quad \forall a,b \in K;\ \vec{v} \in V$
   - $1\vec{v} = \vec{v} \quad \forall \vec{v} \in V$

A los elementos de V los llamaremos vectores, a los elementos de K escalares[2], y a la aplicación del apartado 2. se le llamará producto por un escalar.

5.1 Ejemplos de espacios vectoriales

1. Si K es un cuerpo y $n \in \mathbb{N} \setminus \{0\}$, entonces K^n es un espacio vectorial sobre K, definiendo la operación $+$ como

   $$(a_1,a_2,\dots,a_n) + (b_1,b_2,\dots,b_n) = (a_1+b_1, a_2+b_2, \dots, a_n+b_n)$$

   y el producto por escalar como

   $$k \cdot (a_1,a_2,\dots,a_n) = (k\cdot a_1, k\cdot a_2, \dots, k\cdot a_n)$$

2. Si K es un cuerpo y $n \in \mathbb{N} \setminus \{0\}$, entonces $K[x]_n \coloneqq \left\{ a(x) \in K[x] \ \text{ t. q. } \ \text{gr}\left(a(x)\right) \leq n \right\}$ es un espacio vectorial sobre K, definiendo la operación $+$ como la suma de polinomios y el producto por escalar como

   $$k \cdot (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = (ka_n)x^n + (ka_{n-1})x^{n-1} + \cdots + (ka_1)x + ka_0$$

3. Si K es un cuerpo y $m,n \in \mathbb{N} \setminus 0$, entonces $\mathcal{M}_{m\times n}(K)$ es un espacio vectorial sobre K, definiendo la operación $+$ como la suma de matrices y el producto por escalar como producto de una matriz por un elemento de K. [3]

Ejemplo: ${\mathbb{Z}_3}^4, \mathcal{M}_{2\times 2}(\mathbb{Z}_3)$ y $\mathbb{Z}_3[x]_3$ son espacios vectoriales sobre $\mathbb{Z}_3$. Además, los tres tienen cardinal 81. [4]

---

[1] Véase la definición de grupo abeliano en el tema 4

[2] Además, a los vectores se les diferencia de los escalares mediante una flecha encima del elemento (como se ha visto en las propiedades anteriores), de modo que $\vec{a} \neq a$ ya que $\vec{a} \in V$ y $a \in K$.

[3] Véase la nota al pie 11 del tema 4.

[4] Nótese que si K es un cuerpo finito con cardinal k, entonces $\#K[x]_n = k^{n+1}$.

Proposición 1. Sea V un espacio vectorial sobre un cuerpo K, $a, b \in K$ y $\vec{u}, \vec{v} \in V$. Entonces:

1. $0\vec{v} = \vec{0}$
2. $a\vec{0} = \vec{0}$
3. Si $a\vec{v} = \vec{0}$ entonces $a = 0$ ó $\vec{v} = \vec{0}$.
4. $-(a\vec{v}) = (-a)\vec{v} = a \cdot (-\vec{v})$
5. $a \cdot (\vec{u} - \vec{v}) = a\vec{u} - a\vec{v}$
6. $(a - b)\vec{v} = a\vec{v} - b\vec{v}$
7. Si $a\vec{u} = a\vec{v}$ y $a \neq 0$ entonces $\vec{u} = \vec{v}$.
8. Si $a\vec{v} = b\vec{v}$ y $\vec{v} \neq \vec{0}$ entonces $a = b$.

Nota: Para evitar la repetitividad, a partir de aquí V denotará un espacio vectorial sobre un cuerpo K.

Un subconjunto no vacío $U \subseteq V$ es un subespacio vectorial de V si verifica que:

1. Si $\vec{u}, \vec{v} \in U$ entonces $\vec{u} - \vec{v} \in U$. [5]
2. Si $a \in K$ y $\vec{u} \in U$ entonces $a\vec{u} \in U$.

Proposición 2. Si U es un subespacio vectorial de V entonces U también es un espacio vectorial sobre K.

Ejercicio: Sabiendo que $\mathbb{Q}^3$ es un espacio vectorial sobre $\mathbb{Q}$, demostrar que $U = \left\{(x, y, z) \in \mathbb{Q}^3 \text{ t. q. } x + y + z = 0\right\}$ es un subespacio vectorial de $\mathbb{Q}^3$.

- Si $(x_1, y_1, z_1) \in U$ y $(x_2, y_2, z_2) \in U$, entonces $x_1 + y_1 + z_1 = x_2 + y_2 + z_2 = 0$. Además, $(x_1, y_1, z_1) - (x_2, y_2, z_2) = (x_1 - x_2,\ y_1 - y_2,\ z_1 - z_2)$ y claramente $(x_1 - x_2) + (y_1 - y_2) + (z_1 - z_2) = (x_1 + y_1 + z_1) - (x_2 + y_2 + z_2) = 0 - 0 = 0$. Por tanto $(x_1, y_1, z_1) - (x_2, y_2, z_2) \in U$.
- Si $(x, y, z) \in U$ entonces $x + y + z = 0$. Sea $r \in \mathbb{Q}$. Tenemos que $r(x, y, z) = (rx, ry, rz)$. Como $rx + ry + rz = r(x + y + z) = r \cdot 0 = 0$, entonces $r(x, y, z) \in U$.

Por tanto, U es un subespacio vectorial de $\mathbb{Q}^3$. $\square$

Ejercicio: ¿Qué cardinal tiene $U = \left\{(x, y) \in {\mathbb{Z}_3}^2 \text{ t. q. } x + y = 0\right\}$?

Obviamente $U = \{(0, 0), (1, 2), (2, 1)\}$. Por tanto, $\#U = 3$ $\square$

Proposición 3. La intersección de varios subespacios vectoriales de V es también un subespacio vectorial de V.

[5] Esto junto con la segunda condición es equivalente a decir que si $\vec{u}, \vec{v} \in U$ entonces $\vec{u} + \vec{v} \in U$.

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 todos los elementos de S. A dicho subespacio lo denotaremos como $\langle S \rangle$.[6] Nótese que $\langle S \rangle$ es el menor subespacio vectorial de V que contiene a S.

Proposición 4. Si $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\} \subseteq V$, entonces

$$\langle S \rangle = \Big\{ a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n \ \text{ t. q. } \ a_1, a_2, \ldots, a_n \in K \Big\}$$

Ejercicio: Calcular todos los elementos del subespacio vectorial de ${\mathbb{Z}_2}^3$ generado por $\big\{(1,1,0),(0,1,1)\big\}$.

$\Big\langle \big\{(1,1,0),(0,1,1)\big\} \Big\rangle = \Big\{ a(1,1,0) + b(0,1,1) \ \text{ t. q. } \ a, b \in \mathbb{Z}_2 \Big\}$
$= \Big\{ (0,0,0) + b(0,1,1),\ (1,1,0) + b(0,1,1) \ \text{ t. q. } \ b \in \mathbb{Z}_2 \Big\}$ [7]
$= \Big\{ (0,0,0), (0,1,1), (1,1,0), (1,0,1) \Big\}$ $\square$

Si $U_1, U_2, \ldots, U_n$ son subespacios vectoriales de V, entonces el subespacio vectorial suma de todos ellos es

$$U_1 + U_2 + \cdots + U_n = \Big\{ \vec{u}_1 + \vec{u}_2 + \cdots + \vec{u}_n \ \text{ t. q. } \ \vec{u}_1 \in U_1, \vec{u}_2 \in U_2, \ldots, \vec{u}_n \in U_n \Big\}$$

Proposición 5. Si $U_1, U_2, \ldots, U_n$ son subespacios vectoriales de V:

1. $U_1 + U_2 + \cdots + U_n = \big\langle U_1 \cup U_2 \cup \cdots \cup U_n \big\rangle$
2. Si $U_1 = \langle S_1 \rangle, U_2 = \langle S_2 \rangle, \ldots, U_n = \langle S_n \rangle$, entonces $U_1 + U_2 + \cdots + U_n = \big\langle S_1 \cup S_2 \cup \cdots \cup S_n \big\rangle$

Ejercicio: Sean U_1 y U_2 los subespacios vectoriales de ${\mathbb{Z}_3}^3$ generados por $\big\{(1,2,0)\big\}$ y $\big\{(0,1,2)\big\}$ respectivamente. Calcular todos los elementos de $U_1 + U_2$.

Como $U_1 = \Big\langle \big\{(1,2,0)\big\} \Big\rangle$ y $U_2 = \Big\langle \big\{(0,1,2)\big\} \Big\rangle$, entonces
$U_1 + U_2 = \Big\langle \big\{(1,2,0),(0,1,2)\big\} \Big\rangle = \Big\{ a(1,2,0) + b(0,1,2) \ \text{ t. q. } \ a, b \in \mathbb{Z}_3 \Big\}$
$= \Big\{ (0,0,0), (0,1,2), (0,2,1),\ (1,2,0), (1,0,2), (1,1,1),\ (2,1,0), (2,2,2), (2,0,1) \Big\}$ $\square$

Sean U y W subespacios vectoriales de V. Se dice que V es la suma directa de U y W, lo cual se denota como $V = U \oplus W$, si todo vector $\vec{v} \in V$ se puede poner de forma única como $\vec{v} = \vec{u} + \vec{w}$ t. q. $\vec{u} \in U, \vec{w} \in W$. En dicho caso diremos que los subespacios U y W son complementarios [8].

Proposición 6. Si U y W son subespacios vectoriales de V, entonces $V = U \oplus W$ si y solo si se cumple que:

- $V = U + W$
- $U \cap W = \{\vec{0}\}$

[6] Y diremos que S es un sistema de generadores de $\langle S \rangle$

[7] Le damos a a los valores 0 y 1 por separado, igual que en el siguiente paso se le dan los mismos valores a b.

[8] O que W es un complementario de U, o viceversa.

Ejercicio: Sean $U = \left\{(x,y) \in \mathbb{R}^2 \text{ t. q. } x+y=0\right\}$ y $W = \left\{(x,y) \in \mathbb{R}^2 \text{ t. q. } x-y=0\right\}$ dos subespacios vectoriales de $\mathbb{R}^2$. Demostrar que $\mathbb{R}^2 = U \oplus W$.

Para demostrar lo que pide el enunciado, haremos uso de la proposición anterior. Pasamos a demostrar que $\mathbb{R}^2 = U + W$ y que $U \cap W = \{\vec{0}\}$:

- La primera condición se cumple si para todo $(x,y) \in \mathbb{R}^2$ $\exists\ \vec{u} \in U$, $\vec{w} \in W$ t. q. $(x,y) = \vec{u} + \vec{w}$. Nótese que los vectores de U son de la forma $(a,-a)$ t. q. $a \in \mathbb{R}$ y los vectores de W son de la forma (b,b) t. q. $b \in \mathbb{R}$ [9]. Entonces:

$$(x,y) = (a,-a) + (b,b) \implies \left\{ \begin{array}{r} a+b=x \\ -a+b=y \end{array} \right\} \implies 2b = x+y$$

  Por tanto, $b = \dfrac{x+y}{2} \implies a = \dfrac{x-y}{2}$. Entonces todo vector $(x,y) \in \mathbb{R}^2$ se puede expresar como suma de $(a,-a) \in U$ y $(b,b) \in W$, así que $\mathbb{R}^2 = U + W$.

- Si $(x,y) \in U \cap W$, entonces cumple que $x+y=0$ y $x-y=0$. Pero la única solución del sistema $\left\{ \begin{array}{l} x+y=0 \\ x-y=0 \end{array} \right.$ es $x=y=0 \implies (x,y) = \vec{0}$. Por tanto, $U \cap W = \{\vec{0}\}$.

Como se verifican ambos apartados, podemos concluir que $\mathbb{R}^2 = U \oplus W$ $\square$

Un conjunto de vectores $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\} \subseteq V$ es linealmente dependiente (L.D) si existe $(a_1, a_2, \ldots, a_n) \in K^n \setminus \{(0,0,\ldots,0)\}$ t. q. $a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n = \vec{0}$. En caso contrario se dice que $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es linealmente independiente (L.I).

Ejercicio: ¿Son los vectores $(1,1,0), (1,0,1), (0,1,1) \in \mathbb{R}^3$ L.I?

$$a(1,1,0)+b(1,0,1)+c(0,1,1) = (0,0,0) \implies (a+b, a+c, b+c) = (0,0,0) \implies \left\{ \begin{array}{rl} a+b & =0 \\ a & +c=0 \\ & b+c=0 \end{array} \right.$$

Sin embargo, la única solución del sistema resultante es $(a,b,c) = (0,0,0)$. Por tanto, los vectores son L.I. $\square$

Ejercicio: ¿Son los vectores $(2,3,4)$ y $(4,1,3)$ de ${\mathbb{Z}_5}^3$ L.I?

$$a(2,3,4) + b(4,1,3) = (0,0,0) \implies \left\{ \begin{array}{l} 2a+4b=0 \\ 3a+\ \ b=0 \\ 4a+3b=0 \end{array} \right. \xrightarrow[E_3 \to E_3+3E_1]{E_2 \to E_2+E_1} \left\{ \begin{array}{r} 2a+4b=0 \\ 0=0 \\ 0=0 \end{array} \right.$$

La ecuación $2a+4b=0$ en $\mathbb{Z}_5$ tiene 5 soluciones [10]:
$(a,b) \in \left\{(0,0),(1,2),(2,4),(3,1),(4,3)\right\}$.

[9] Debido a que $U = \left\{(x,y) \in \mathbb{R}^2 \text{ t. q. } x+y=0 \implies x=-y\right\}$ y $W = \left\{(x,y) \in \mathbb{R}^2 \text{ t. q. } x-y=0 \implies x=y\right\}$.

[10] Ya que es un sistema compatible indeterminado (como se estudiará en el tema 7), tiene más de una solución; en concreto, el número de soluciones es igual al cardinal del cuerpo de los coeficientes

Por tanto, los vectores son L.D ya que existen valores no nulos de a y b. $\square$

Proposición 7. Sea $S \subseteq V$.

1. S es L.D si y solo si $\exists \vec{v} \in S$ t. q. $\vec{v} \in \langle S \setminus \{\vec{v}\}\rangle$.
2. Si $\vec{0} \in S$ entonces S es L.D.
3. Si S es L.D y $\vec{v} \in V$ entonces $S \cup \{\vec{v}\}$ es L.D.
4. Si S es L.I y $\vec{v} \in S$ entonces $S \setminus \{\vec{v}\}$ es L.I.

Una base de V es un subconjunto $B \subseteq V$ que verifica las siguientes propiedades:

1. B es L.I.
2. $V = \langle B\rangle$

Ejercicio: Demostrar que $B = \{(1,2),(1,3)\}$ es una base de ${\mathbb{Z}_5}^2$.[11]

Veamos que B es L.I:

$$a(1,2)+b(1,3) = (0,0) \implies \left\{ \begin{array}{rl} a+ & b = 0 \\ 2a+3b = 0 & \end{array} \right. \xrightarrow{E_2 \to E_2+3E_1} \left\{ \begin{array}{rl} a+ & b = 0 \\ & b = 0 \end{array} \right. \implies a = b = 0$$

Como B es L.I, pasamos a demostrar que ${\mathbb{Z}_5}^2 = \langle B\rangle$. Claramente, $\langle B\rangle \subseteq {\mathbb{Z}_5}^2$, así que basta con probar que ${\mathbb{Z}_5}^2 \subseteq \langle B\rangle = \left\{a(1,2)+b(1,3) \text{ t. q. } a,b \in \mathbb{Z}_5\right\}$, lo cual se cumple si para todo $(x,y) \in {\mathbb{Z}_5}^2$ $\exists a,b \in \mathbb{Z}_5$ t. q. $(x,y) = a(1,2)+b(1,3)$.

$$(x,y) = a(1,2)+b(1,3) \implies \left\{ \begin{array}{rl} a+ & b = x \\ 2a+3b = y & \end{array} \right. \xrightarrow{E_2 \to E_2+3E_1} \left\{ \begin{array}{rl} a+ & b = x \\ & b = y+3x \end{array} \right.$$

Como $b = y+3x$, entonces $a = x-b = x+4y+2x = 3x+4y$. Por tanto, si $(x,y) \in {\mathbb{Z}_5}^2$ entonces $(x,y) = (3x+4y)\cdot(1,2)+(3x+y)\cdot(1,3)$, así que $(x,y) \in \langle B\rangle$.
Por tanto ${\mathbb{Z}_5}^2 \subseteq \langle B\rangle \implies {\mathbb{Z}_5}^2 = \langle B\rangle$.
Como B es L.I y ${\mathbb{Z}_5}^2 = \langle B\rangle$, entonces B es una base de ${\mathbb{Z}_5}^2$. $\square$

Proposición 8. Si $B = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es una base de V y $\vec{v} \in V$, entonces existe una única n-tupla $(a_1, a_2, \ldots, a_n) \in K^n$ t. q. $\vec{v} = a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n$.

A la n-tupla de la proposición anterior, $(a_1, a_2, \ldots, a_n)$, se le llaman las coordenadas de $\vec{v}$ respecto de la base B. Si $(a_1, a_2, \ldots, a_n)$ son las coordenadas de un vector $\vec{v}$ respecto de una base B, se denotará como $\vec{v} \underset{B}{\equiv} (a_1, a_2, \ldots, a_n)$.

Ejercicio: Dada la base $B = \{(1,2),(1,3)\}$ de ${\mathbb{Z}_5}^2$, calcular las coordenadas del vector $(2,4)$ respecto de B.

$$(a(1,2)+b(1,3) = (2,4) \implies \left\{ \begin{array}{rl} a+ & b = 2 \\ 2a+3b = 4 & \end{array} \right. \implies \left\{ \begin{array}{rl} a+ & b = 2 \\ & b = 0 \end{array} \right. \implies (a,b) = (2,0)$$

Por tanto $(2,4) \underset{B}{\equiv} (2,0)$ $\square$

[11] Es importante señalar que el orden de los vectores en las bases es importante, aunque se escriban entre llaves. Es decir, la base $\{(1,2),(1,3)\}$ de ${\mathbb{Z}_5}^2$ no es la misma base que $\{(1,3),(1,2)\}$.

Teorema 1 (Teorema de la Base)**.** Todo espacio vectorial V distinto de $\{\vec{0}\}$ tiene al menos una base. Además, todas las bases de V tienen el mismo cardinal.

Al cardinal de una base cualquiera de V lo llamaremos la dimensión de V, denotado $\dim(V)$. La dimensión del espacio vectorial cero la tomamos como $\dim\big(\{\vec{0}\}\big) = 0$.
Ejemplo: En un ejercicio anterior se ha demostrado que $B = \big\{(1,2),(1,3)\big\}$ es una base de ${\mathbb{Z}_5}^2$. Por tanto, $\dim({\mathbb{Z}_5}^2) = \#B = 2$.

Proposición 9.

1. $\dim(K^n) = n$, y además $B_{can} = \big\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\big\}$ es una base de K^n a la que llamaremos la base canónica.
2. $\dim\big(\mathcal{M}_{m\times n}(K)\big) = m\cdot n$, y además
$$B_{can} = \left\{ \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \right\}$$ es una base de $\mathcal{M}_{m\times n}(K)$ a la que llamaremos la base canónica.
3. $\dim\big(K[x]_n\big) = n+1$, y además $B_{can} = \{1, x, x^2, \ldots, x^n\}$ es una base de $K[x]_n$ a la que llamaremos la base canónica.

Ejemplo:

1. $\dim({\mathbb{Z}_5}^4) = 4$, y $B_{can} = \big\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\big\}$ es la base canónica de ${\mathbb{Z}_5}^4$.
2. $\dim\big(\mathcal{M}_{2\times 2}(\mathbb{Z}_5)\big) = 4$, y $B_{can} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ es la base canónica de $\mathcal{M}_{2\times 2}(\mathbb{Z}_5)$.
3. $\dim\big(\mathbb{Z}_5[x]_3\big) = 4$, y $B_{can} = \{1, x, x^2, x^3\}$ es la base canónica de $\mathbb{Z}_5[x]_3$.

Teorema 2 (Teorema de Ampliación de la Base)**.** Si $\dim(V) = n$ y B es un conjunto de vectores L.I de V entonces $\#B \leq n$. Además, $\exists A \subseteq V$ t. q. $A \cup B$ es una base de V.

Corolario 1. Si $\dim(V) = n$, entonces n vectores L.I de V son una base de V.

Ejercicio: ¿Es $\big\{(1,2,1),(1,1,1),(1,0,0)\big\}$ una base de ${\mathbb{Z}_5}^3$?

Como $\dim({\mathbb{Z}_5}^3) = 3 = \#\big\{(1,2,1),(1,1,1),(1,0,0)\big\}$, entonces los vectores del enunciado formarán una base si son L.I.

$$a(1,2,1) + b(1,1,1) + c(1,0,0) = (0,0,0) \implies \begin{cases} a+b+c = 0 \\ 2a+b \quad = 0 \\ a+b \quad = 0 \end{cases}$$

Como la única solución del sistema resultante es $a = b = c = 0$ [12], entonces los vectores son L.I y por tanto $\big\{(1,2,1),(1,1,1),(1,0,0)\big\}$ es una base de ${\mathbb{Z}_5}^3$. $\square$

[12] La resolución del sistema se deja como un ejercicio para el lector.

Ejercicio: Ampliar $\{(1,1,1)\}$ a una base de $\mathbb{R}^3$.

Como el conjunto tiene un vector, hay que añadir dos vectores más de forma que los tres sean L.I para que forme una base. Sabemos que los vectores de la base canónica funcionarán[13]. Tomamos los vectores $(1,0,0)$ y $(0,1,0)$ y comprobamos que $\{(1,1,1),(1,0,0),(0,1,0)\}$ es un conjunto L.I:

$$a(1,1,1)+b(1,0,0)+c(0,1,0)=(0,0,0) \implies \left\{\begin{array}{rr} a+b & =0 \\ a & +c=0 \\ a & =0 \end{array}\right\} \implies a=b=c=0$$

Por tanto, $\{(1,1,1),(1,0,0),(0,1,0)\}$ es una base de $\mathbb{R}^3$. $\square$

Ejercicio: Demostrar que $B=\{x^2+x, x^2+1, x+1\}$ es una base de $\mathbb{R}[x]_2$, y calcular las coordenadas del vector $3x^2+2x+3$ respecto de la base B.

$\dim\left(\mathbb{R}[x]_2\right)=3=\#B$, así que para demostrar que es una base, comprobamos que B es L.I:

$$a(x^2+x)+b(x^2+1)+c(x+1)=0 \implies (a+b)x^2+(a+c)x+(b+c)=0x^2+0x+0 \implies \left\{\begin{array}{rr} a+b & =0 \\ a & +c=0 \\ & b+c=0 \end{array}\right.$$

La única solución del sistema es $a=b=c=0$, así que B es una base. Ahora pasamos a calcular las coordenadas de $3x^2+2x+3$ respecto de B:

$$a(x^2+x)+b(x^2+1)+c(x+1)=3x^2+3x+3 \implies (a+b)x^2+(a+c)x+(b+c)=3x^2+2x+3$$

El sistema resultante es $\left\{\begin{array}{rr} a+b & =3 \\ a & +c=2 \\ & b+c=3 \end{array}\right. \implies (a,b,c)=(1,2,1).$

Por tanto, $3x^2+2x+3 \underset{B}{\equiv} (1,2,1)$ $\square$

5.2 Métodos para calcular una base de un subespacio vectorial a partir de su sistema de generadores

([14])

- Primer método: Quitar los vectores del conjunto que sean combinación lineal de otros anteriores. El conjunto resultante es una base del subespacio.
- Segúndo método Triangularizar la matriz cuyas filas son los vectores del subespacio[15]. Las filas no nulas de la matriz triangularizada forman un conjunto de vectores que es base del subespacio.

[13] Ya que es asegurado que son L.I, hay dos vectores de la base canónica que junto con $\{(1,1,1)\}$ forman una base

[14] Como es de esperar, una base de un subespacio vectorial es un conjunto linealmente independiente que además genera a dicho subespacio.

[15] Técnicamente, se usan las coordenadas de los vectores respecto de la base canónica.

Ejercicio: Usando el primer método, Calcular una base del subespacio vectorial de $\mathbb{R}^3$ $U = \Big\langle \big\{(1,2,1),(2,4,2),(1,3,2),(2,5,3)\big\} \Big\rangle$.

Es fácil ver que $(2,4,2) = 2 \cdot (1,2,1)$. Por tanto, $(2,4,2)$ no forma parte de la base. Similarmente, $\nexists a \in \mathbb{R}$ t. q. $a(1,2,1) = (1,3,2)$, así que $(1,2,1)$ y $(1,3,2)$ son L.I. Ahora vemos si $(2,5,3)$ es combinación lineal de los dos vectores:

$$a(1,2,1) + b(1,3,2) = (2,5,3) \implies \begin{cases} a + \ b = 2 \\ 2a + 3b = 5 \\ a + 2b = 3 \end{cases} \implies a = b = 1$$

Entonces $(2,5,3) = (1,2,1) + (1,3,2)$ y por tanto $B = \big\{(1,2,1),(1,3,2)\big\}$ es una base de U. $\square$

Ejercicio: Usando el segundo método, Calcular una base del subespacio vectorial de $\mathbb{R}^3$ $U = \Big\langle \big\{(1,2,1),(2,4,2),(1,3,2),(2,5,3)\big\} \Big\rangle$.

La matriz cuyas filas son los vectores de $\big\{(1,2,1),(2,4,2),(1,3,2),(2,5,3)\big\}$ es la siguiente:

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 3 & 2 \\ 2 & 5 & 3 \end{pmatrix} \overbrace{\substack{F_2 \to F_2 - 2F_1 \\ F_3 \to F_3 - F_1 \\ F_4 \to F_4 - 2F_1}}^{F_2 \to F_2 - 2F_1} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \overbrace{\qquad}^{F_4 \leftrightarrow F_2} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \overbrace{\qquad}^{F_3 \to F_3 - F_2} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto[16], $B = \big\{(1,2,1),(0,1,1)\big\}$ es una base de U [17]. $\square$

Ejercicio: Sea U el subespacio vectorial de ${\mathbb{Z}_5}^4$ generado por $\big\{(1,2,3,4),(2,1,3,2),(1,2,1,1),(4,0,2,2)\big\}$. Calcular una base de U.

Pasamos a triangularizar la siguiente matriz[18]:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 2 \\ 1 & 2 & 1 & 1 \\ 4 & 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 2 & 4 \\ 0 & 0 & 3 & 2 \\ 0 & 2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 2 & 4 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 3 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 2 & 2 & 4 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Entonces, $B = \big\{(1,2,3,4),(0,2,2,4),(0,0,3,2)\big\}$ es una base de U. $\square$

Proposición 10. Sea U un subespacio vectorial de V. Entonces $U = V$ si y solo si $\dim(U) = \dim(V)$.

[16] Como se puede ver, el proceso de triangularizar una matriz consiste en hacer operaciones elementales hasta que todos los elementos de la matriz por debajo de las posiciones $(1,1),(2,2),...$ sean 0. La matriz no tiene por qué ser cuadrada.

[17] Aunque nos haya salido una base distinta a la del ejercicio anterior, el conjunto sigue siendo una base de U, al igual que tanto $\big\{(1,0),(0,1)\big\}$ como $\big\{(1,2),(1,3)\big\}$ son bases de ${\mathbb{Z}_5}^2$

[18] Por su simplicidad, se suele usar el método de triangularización a la hora de calcular bases de subespacios vectoriales.

Ejercicio: Sean $U = \left\langle \{(1,1,1),(1,2,1)\} \right\rangle$ y $W = \left\langle \{(1,2,3),(0,0,2)\} \right\rangle$ dos subespacios vectoriales de ${\mathbb{Z}_5}^3$. ¿${\mathbb{Z}_5}^3 = U + W$?

$U + W = \left\langle \{(1,1,1),(1,2,1)\} \cup \{(1,2,3),(0,0,2)\} \right\rangle =$
$\left\langle \{(1,1,1),(1,2,1),(1,2,3),(0,0,2)\} \right\rangle$. Pasamos a calcular una base del subespacio $U + W$:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Como $B = \{(1,1,1),(0,1,0),(0,0,2)\}$ es una base de $U + W$ y $\#B = 3$, entonces $\dim(U + W) = 3 = \dim({\mathbb{Z}_5}^3)$. Por tanto $U + W = {\mathbb{Z}_5}^3$ $\square$

5.3 Método para calcular el complementario de un subespacio vectorial

Sea U un subespacio vectorial de V. Un método para calcular un complementario[19] de U es el siguiente:

1. Hallar una base B_U de U.
2. Ampliar la base B_U a una base B del espacio vectorial V.[20]
3. El subespacio vectorial $W = \langle B \setminus B_U \rangle$ 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.

Calculamos una base de U:

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

Tenemos que $B_U = \{(1,1,1),(0,-1,1)\}$ es una base de U. Le añadimos el vector $(0,0,1)$ y el conjunto resultante $B = \{(1,1,1),(0,-1,1),(0,0,1)\}$ es L.I[21] y por tanto una base de $\mathbb{Q}^3$. Entonces $W = \langle B \setminus B_U \rangle = \left\langle \{(0,0,1)\} \right\rangle$ es un complementario de U.
$\square$

Ejercicio: Sean $B = \{(1,1,0),(1,2,1),(1,1,2)\}$ y $B' = \{(1,1,0),(1,0,1),(1,1,1)\}$ dos bases de ${\mathbb{Z}_5}^3$. Si las coordenadas de un vector $\vec{v}$ respecto de la base B son $(1,2,3)$, calcular las coordenadas de $\vec{v}$ respecto de B'.

$\vec{v} \underset{B}{\equiv} (1,2,3) \implies \vec{v} = 1 \cdot (1,1,0) + 2 \cdot (1,2,1) + 3 \cdot (1,1,2) = (1,3,3)$
Ahora pasamos el vector $(1,3,3)$ a la base B':

[19] Nótese que un subespacio vectorial puede tener varios complementarios; entonces este método calcula *un complementario* de U, no *el complementario* de U.
[20] O lo que es lo mismo, hallar un subconjunto $S \subseteq V$ t. q. $B_U \cup S$ es base de V.
[21] La prueba de esto se deja como ejercicio para el lector

$$a(1,1,0)+b(1,0,1)+c(0,1,1)=(1,3,3) \implies \begin{cases} a+b \quad\quad = 1 \\ a \quad\quad + c = 3 \\ \quad\quad b+c=3 \end{cases} \implies (a,b,c)=(3,3,0)$$

Por tanto, $\vec{v} \underset{B'}{\equiv} (3,3,0)$ $\square$

5.4 Ecuaciones del cambio de base

Sean $B=\{\vec{v}_1,\vec{v}_2,\ldots,\vec{v}_n\}$ y $B'=\{\vec{v}'_1,\vec{v}'_2,\ldots,\vec{v}'_n\}$ dos bases de V. Supongamos que
$\vec{v}_1 \underset{B'}{\equiv} (a_{1\,1},a_{1\,2},\ldots,a_{1\,n})$, $\vec{v}_2 \underset{B'}{\equiv} (a_{2\,1},a_{2\,2},\ldots,a_{2\,n})$, ……., $\vec{v}_n \underset{B'}{\equiv} (a_{n\,1},a_{n\,2},\ldots,a_{n\,n})$.
Sea $\vec{x}\in V$ t. q. $\vec{x} \underset{B}{\equiv} (x_1,x_2,\ldots,x_n)$ y $\vec{x} \underset{B'}{\equiv} (x'_1,x'_2,\ldots,x'_n)$. Entonces se cumple que

$$(x'_1,x'_2,\ldots,x'_n)=(x_1,x_2,\ldots,x_n)\cdot\begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \ldots & a_{n\,n} \end{pmatrix}$$

A esta expresión se le llama la expresión matricial del cambio de base de B a B' [22]. A la matriz $A=\begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \ldots & a_{n\,n} \end{pmatrix}$ se le llama la matriz del cambio de base de B a B'. A es siempre regular, y A^{-1} es justamente la matriz del cambio de base de B' a B.
De la expresión matricial anterior obtenemos que:

$$\begin{cases} x'_1 &= a_{1\,1}x_1+a_{2\,1}x_2+\cdots+a_{n\,1}x_n \\ x'_2 &= a_{1\,2}x_1+a_{2\,2}x_2+\cdots+a_{n\,2}x_n \\ \vdots & \quad \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ x'_n &= a_{1\,n}x_1+a_{2\,n}x_2+\cdots+a_{n\,n}x_n \end{cases}$$

A esta expresión se le llama las ecuaciones del cambio de base de B a B'.
Ejercicio: Sean 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 ${\mathbb{Z}_5}^3$.

a) Calcular las ecuaciones del cambio de base de B a B'.

b) Si las coordenadas de un vector $\vec{v}$ respecto de la base B son $(1,2,3)$, calcular las coordenadas de $\vec{v}$ respecto de B'.

- Calculamos las coordenadas de cada uno de los vectores de B respecto de la base B':

[22] Esto se interpreta de la siguiente manera: Si en $(x_1,x_2,\ldots,x_n)$ se introducen las coordenadas de un vector respecto de la base B y se multiplica por la matriz (como si las coordenadas fuesen una matriz de una sola fila), la n-tupla resultante son las coordenadas del mismo vector respecto de la base B'.

$$\left.\begin{array}{l}(1,1,0) \underset{B'}{\equiv} (1,0,0)\\ (1,2,1) \underset{B'}{\equiv} (1,0,1)\\ (1,1,2) \underset{B'}{\equiv} (0,1,1)\end{array}\right\} \Longrightarrow \text{La matriz de cambio de base es } \begin{pmatrix}1&0&0\\1&0&1\\0&1&1\end{pmatrix}$$

Por tanto, si $\vec{v} \in {\mathbb{Z}_5}^3$, $\vec{v} \underset{B}{\equiv} (x,y,z)$ y $\vec{v} \underset{B'}{\equiv} (x',y',z')$, entonces:

$$(x',y',z') = (x,y,z)\begin{pmatrix}1&0&0\\1&0&1\\0&1&1\end{pmatrix} \Longrightarrow \left\{\begin{array}{l}x' = x+y\\ y' = z\\ z' = y+z\end{array}\right.$$

- Usamos la expresión matricial del cambio de base:
  $(1,2,3)\begin{pmatrix}1&0&0\\1&0&1\\0&1&1\end{pmatrix} = (3,3,0)$. Por tanto, $\vec{v} \underset{B'}{\equiv} (3,3,0)$

□

5.5 Ecuaciones paramétricas de un subespacio vectorial

Sea U un subespacio vectorial de V, $B = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ una base de V y $B_U = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_r\}$ una base de U [23]. Supongamos que
$\vec{u}_1 \underset{B}{\equiv} (a_{1\,1}, a_{1\,2}, \ldots, a_{1\,n})$; $\vec{u}_2 \underset{B}{\equiv} (a_{2\,1}, a_{2\,2}, \ldots, a_{2\,n})$; . . . . . ; $\vec{u}_r \underset{B}{\equiv} (a_{r\,1}, a_{r\,2}, \ldots, a_{r\,n})$.
Sea $\vec{x} \in V$ t. q. $x \underset{B}{\equiv} (x_1, x_2, \ldots, x_n)$. Entonces $\vec{x} \in U$ si y solo si existen
$\lambda_1, \lambda_2, \ldots, \lambda_r \in K$ tales que

$$(x_1, x_2, \ldots, x_n) = \lambda_1(a_{1\,1}, a_{1\,2}, \ldots, a_{1\,n}) + \lambda_2(a_{2\,1}, a_{2\,2}, \ldots, a_{2\,n}) + \cdots + \lambda_r(a_{r\,1}, a_{r\,2}, \ldots, a_{r\,n})$$

Por tanto, $\vec{x} \in U$ si y solo si:

$$\left.\begin{array}{rcl}x_1 &=& a_{1\,1}\lambda_1 + a_{2\,1}\lambda_2 + \cdots + a_{r\,1}\lambda_r\\ x_2 &=& a_{1\,2}\lambda_1 + a_{2\,2}\lambda_2 + \cdots + a_{r\,2}\lambda_r\\ \vdots && \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\\ x_n &=& a_{1\,n}\lambda_1 + a_{2\,n}\lambda_2 + \cdots + a_{r\,n}\lambda_r\end{array}\right\} \text{ para algún } \lambda_1, \lambda_2, \ldots, \lambda_r \in K$$

A esta expresión se le llaman las ecuaciones paramétricas de U respecto de la base B [24].
Nota: Si se dan o se piden las ecuaciones paramétricas de un subespacio vectorial sin especificar la base respecto de la que son, se asume que son respecto de la base canónica.
Ejercicio: Sea $B = \{(1,1,0),(1,0,1),(0,1,1)\}$ una base de $\mathbb{Q}^3$ y U el subespacio vectorial de $\mathbb{Q}^3$ generado por $\{(1,2,1),(1,3,2),(2,5,3)\}$. Calcular las ecuaciones paramétricas de U respecto de B.

Primero calculamos una base de U triangularizando la siguiente matriz:

[23] Nótese que r no tiene por qué ser igual a n, y suele no serlo.
[24] Esto se interpreta de la siguiente manera: Si se le dan valores cualquiera de K a los parámetros $\lambda_1, \lambda_2, \ldots, \lambda_r$, entonces la n-tupla resultante $(x_1, x_2, \ldots, x_n)$ son las coordenadas de un vector de U respecto de la base B (cuidado, no es un vector de U, son sus coordenadas).

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto, $B_U = \big\{(1,2,1),(0,1,1)\big\}$ es una base de U. Ahora calculamos las coordenadas de cada vector de B_U respecto de la base B:

$(1,2,1) \underset{B}{\equiv} (1,0,1)$

$(0,1,1) \underset{B}{\equiv} (0,0,1)$

Por tanto, las ecuaciones paramétricas de U respecto de la base B son

$$(x,y,z) = \lambda(1,0,1) + \mu(0,0,1) \implies \begin{cases} x = \lambda \\ y = 0 \\ z = \lambda + \mu \end{cases} \qquad \square$$

Ejercicio: Calcular las ecuaciones paramétricas del subespacio vectorial U de ${\mathbb{Z}_7}^3$ generado por $\big\{(2,3,5),(3,1,4),(2,3,1)\big\}$.

Como no se especifica la base respecto de la que calcular las ecuaciones paramétricas, entonces las calcularemos respecto de la base canónica de ${\mathbb{Z}_7}^3$:

$B_{can} = \big\{(1,0,0),(0,1,0),(0,0,1)\big\}$

Pasamos a la realización del ejercicio. Primero calculamos una base de U:

$$\begin{pmatrix} 2 & 3 & 5 \\ 3 & 1 & 4 \\ 2 & 3 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 5 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

Luego $B_U = \big\{(2,3,5),(0,0,3)\big\}$.

$$\left.\begin{array}{l} (2,3,5) \underset{B_{can}}{\equiv} (2,3,5) \\ (0,0,3) \underset{B_{can}}{\equiv} (0,0,3) \end{array}\right\} \implies (x,y,z) = \lambda(2,3,5) + \mu(0,0,3)$$

Entonces las ecuaciones paramétricas de U son

$$\begin{cases} x = 2\lambda \\ y = 3\lambda \\ z = 5\lambda + 3\mu \end{cases} \qquad \square$$

6 Aplicaciones lineales

Este tema es en su mayor parte una continuación del anterior: las aplicaciones lineales entre dos espacios vectoriales tienen propiedades que nos permiten ahondar más en el estudio de éstos; por tanto, el álgebra lineal también estudia estas estructuras.

En todo este tema, V y V' denotarán dos espacios vectoriales sobre el mismo cuerpo K.

Una aplicación $f : V \longrightarrow V'$ es lineal (o un homomorfismo de espacios vectoriales) si verifica que:

1. $f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v}) \quad \forall \vec{u}, \vec{v} \in V$
2. $f(a\vec{v}) = a \cdot f(\vec{v}) \quad \forall \vec{v} \in V, a \in K$

Ejercicio: Demostrar que la aplicación $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ definida por $f(x, y, z) = (x + y, x + z)$ es lineal.

- Sean $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{R}^3$. Entonces

$$\begin{aligned} & f\big((x_1, y_1, z_1) + (x_2, y_2, z_2)\big) = f(x_1 + x_2,\ y_1 + y_2, z_1 + z_2) \\ = \ & \big((x_1 + x_2) + (y_1 + y_2),\ (x_1 + x_2) + (z_1 + z_2)\big) \\ = \ & \big((x_1 + y_1) + (x_2 + y_2),\ (x_1 + z_1) + (x_2 + z_2)\big) \\ = \ & (x_1 + y_1, x_1 + z_1) + (x_2 + y_2, x_2 + z_2) \\ = \ & f(x_1, y_1, z_1) + f(x_2, y_2, z_2) \end{aligned}$$

- Sea $a \in \mathbb{R}$ y $(x, y, z) \in \mathbb{R}^3$. Entonces

$$\begin{aligned} & f\big(a(x, y, z)\big) = f(ax, ay, az) \\ = \ & (ax + ay, ax + az) \\ = \ & \big(a(x + y), a(x + z)\big) \\ = \ & a(x + y, x + z) \\ = \ & a \cdot f(x, y, z) \end{aligned}$$

Como se cumplen ambas condiciones, entonces f es una aplicación lineal. $\square$

Ejercicio: ¿Es lineal la aplicación $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ definida por $f(x, y, z) = (x + y + 1, x + z)$?

$f\big((1, 0, 0) + (0, 1, 0)\big) = f(1, 1, 0) = (1 + 1 + 1, 1 + 0) = (3, 1)$. Pero
$f(1, 0, 0) + f(0, 1, 0) = (1 + 0 + 1, 1 + 0) + (0 + 1 + 1, 0 + 0) = (2, 1) + (2, 0) = (4, 1)$.
Como $f\big((1, 0, 0) + (0, 1, 0)\big) \neq f(1, 0, 0) + f(0, 1, 0)$, entonces f no es lineal. $\square$

Proposición 1. Si $f : V \longrightarrow V'$ es una aplicación lineal, entonces:

1. $f(\vec{0}) = \vec{0}$
2. $f(-\vec{v}) = -f(\vec{v})$
3. $N(f) \coloneqq \left\{ \vec{v} \in V \ \text{ t. q. } \ f(\vec{v}) = \vec{0} \right\}$ es un subespacio vectorial de V al que llamaremos el núcleo de f.
4. La imagen $\mathrm{Im}(f)$ de f es un subespacio vectorial de V'.

Ejercicio: Dada la aplicación lineal $f : {\mathbb{Z}_5}^3 \longrightarrow {\mathbb{Z}_5}^2$ definida por $f(x, y, z) = (2x + y + z, x + y + z)$, calcular todos los elementos del núcleo de f.

$$\begin{aligned} & N(f) = \left\{(x, y, z) \in {\mathbb{Z}_5}^3 \text{ t. q. } f(x, y, z) = \vec{0}\right\} \\ = & \left\{(x, y, z) \in {\mathbb{Z}_5}^3 \text{ t. q. } (2x + y + z, x + y + z) = (0, 0)\right\} \\ = & \left\{(x, y, z) \in {\mathbb{Z}_5}^3 \text{ t. q. } \begin{array}{r} 2x + y + z = 0 \\ x + y + z = 0 \end{array}\right\} \end{aligned}$$

Por tanto $N(f)$ contiene las soluciones al siguiente sistema de ecuaciones:

$$\left\{\begin{array}{r} x + y + z = 0 \\ 2x + y + z = 0 \end{array}\right. \Longrightarrow \left\{\begin{array}{r} x + y + z = 0 \\ x = 0 \end{array}\right. \Longrightarrow \left\{\begin{array}{r} x = 0 \\ y + z = 0 \end{array}\right.$$

Entonces las soluciones del sistema, es decir, los elementos de $N(f)$ son $(x, y, z) \in \{(0, 0, 0), (0, 1, 4), (0, 2, 3), (0, 3, 2), (0, 4, 1)\}$ $\square$

6.1 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 2. Sea $f : V \longrightarrow V'$ una aplicación lineal. Entonces:

1. Si f es un isomorfismo entonces f^{-1} también es un isomorfismo.
2. f es un monomorfismo si y solo si $N(f) = \{\vec{0}\}$.
3. Si $V = \langle\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}\rangle$, entonces $\text{Im}(f) = \left\langle\left\{f(\vec{v}_1), f(\vec{v}_2), \ldots, f(\vec{v}_n)\right\}\right\rangle$
4. Si f es un monomorfismo y $\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ es un conjunto L.I de vectores de V entonces $\left\{f(\vec{v}_1), f(\vec{v}_2), \ldots, f(\vec{v}_n)\right\}$ es un conjunto de vectores L.I de V'. [1]

Ejercicio: Dada la aplicación lineal $f : {\mathbb{Z}_5}^3 \longrightarrow {\mathbb{Z}_5}^4$ definida por $f(x, y, z) = (x + y, x + z, 2x + y + z, y + 4z)$:

a) Calcular una base de $\text{Im}(f)$.

b) ¿Es f un epimorfismo?

c) ¿Es f un monomorfismo?

- Sabemos que ${\mathbb{Z}_5}^3 = \left\langle\left\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\right\}\right\rangle$. Por tanto, según el punto 3 de la proposición anterior, $\text{Im}(f) = \left\langle\left\{f(1, 0, 0), f(0, 1, 0), f(0, 0, 1)\right\}\right\rangle = \left\langle\left\{(1, 1, 2, 0), (1, 0, 1, 1), (0, 1, 1, 4)\right\}\right\rangle$. Para calcular una base de $\text{Im}(f)$ triangularizamos la siguiente matriz:

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 4 & 4 & 1 \\ 0 & 1 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 4 & 4 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

[1] Esto junto con el punto anterior implica que si se le aplica un monomorfismo a cada vector de una base de V entonces se obtendrá una base de $\text{Im}(f)$.

Entonces $B = \{(1,1,2,0),(0,4,4,1)\}$ es una base de $\mathrm{Im}(f)$.

- $\dim\big(\mathrm{Im}(f)\big) = 2 \neq 4 = \dim({\mathbb{Z}_5}^4)$. Por tanto, $\mathrm{Im}(f) \neq {\mathbb{Z}_5}^4$ y f no es un epimorfismo.
- Nótese que $f(4,1,1) = (4+1, 4+1, 3+1+1, 1+4) = (0,0,0,0)$. Por tanto, $(4,1,1) \in N(f)$ así que $N(f) \neq \{(0,0,0,0)\}$. Por tanto, f no es un monomorfismo.

□

Teorema 1. Sea $B = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ una base de V y $\{\vec{v}'_1, \vec{v}'_2, \ldots, \vec{v}'_n\} \subseteq V'$. Entonces existe una única aplicación lineal $f : V \longrightarrow V'$ que verifica que
$f(\vec{v}_1) = \vec{v}'_1,\ f(\vec{v}_2) = \vec{v}'_2, \ldots,\ f(\vec{v}_n) = \vec{v}'_n$. Además, f es un isomorfismo si y solo si el conjunto $\{\vec{v}'_1, \vec{v}'_2, \ldots, \vec{v}'_n\}$ es una base de V'.

Nota: El teorema anterior nos dice que una aplicación lineal queda únicamente determinada conociendo las imágenes de cada vector de una base de V, y que la aplicación lineal en cuestión es un isomorfismo si esas imágenes forman una base de V'.

Dos espacios vectoriales V y V' son isomorfos si existe un isomorfismo $f : V \longrightarrow V'$.

Corolario 1. Dos espacios vectoriales V y V' sobre el mismo cuerpo K son isomorfos si y solo si $\dim(V) = \dim(V')$.

Ejemplo:

- ${\mathbb{Z}_5}^2$ y ${\mathbb{Z}_7}^2$ no son espacios vectoriales isomorfos porque no están sobre el mismo cuerpo.
- Los espacios vectoriales $\mathcal{M}_{2\times 2}(\mathbb{Z}_5)$ y ${\mathbb{Z}_5}^4$ son isomorfos ya que son ambos espacios sobre el cuerpo $\mathbb{Z}_5$ de dimensión 4.

Ejercicio: Sea U el subespacio vectorial de ${\mathbb{Z}_5}^3$ generado por $\{(1,2,3),(0,1,2),(1,3,0)\}$. Calcular el cardinal de U.

Vamos a calcular una base de U mediante triangularización:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 1 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto, $B = \{(1,2,3),(0,1,2)\}$ es una base de U. Como $\#B = 2$ entonces podemos afirmar que $\dim(U) = 2$. U es un espacio vectorial sobre el cuerpo $\mathbb{Z}_5$ de dimensión 2, así que U es isomorfo a ${\mathbb{Z}_5}^2$, es decir, existe un isomorfismo $f : U \longrightarrow {\mathbb{Z}_5}^2$. Como f es biyectiva entonces deducimos que [2]
$\#U = \#{Z_5}^2 = 5^2 = 25$ □

[2] Es fácil de ver que si A y B son conjuntos con cardinal finito y $f : A \longrightarrow B$ es una aplicación biyectiva entonces $\#A = \#B$

6.2 Ecuaciones de una aplicación lineal

Sea $f : V \longrightarrow V'$ una aplicación lineal, $B = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ una base de V y $B' = \{\vec{v}'_1, \vec{v}'_2, \ldots, \vec{v}'_m\}$ una base de V' [3]. Supongamos que $f(\vec{v}_1) \underset{B'}{\equiv} (a_{1\,1}, a_{1\,2}, \ldots, a_{1\,m})$; $f(\vec{v}_2) \underset{B'}{\equiv} (a_{2\,1}, a_{2\,2}, \ldots, a_{2\,m}); \ldots$; $f(\vec{v}_n) \underset{B'}{\equiv} (a_{n\,1}, a_{n\,2}, \ldots, a_{n\,m})$. Sea $\vec{x} \in V$ t. q. $\vec{x} \underset{B}{\equiv} (x_1, x_2, \ldots, x_n)$ y $f(\vec{x}) \underset{B'}{\equiv} (x'_1, x'_2, \ldots, x'_m)$. Entonces

$$(x'_1, x'_2, \ldots, x'_m) = (x_1, x_2, \ldots, x_n) \cdot \begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,m} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \ldots & a_{n\,m} \end{pmatrix}$$

A esta expresión se le llama la expresión matricial de f respecto de las bases B de V y B' de V' [4].

A la matriz $\begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,m} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} & a_{n\,2} & \ldots & a_{n\,m} \end{pmatrix}$ la llamaremos la matriz asociada a f respecto de las bases B de V y B' de V'. De la expresión matricial obtenemos que

$$\begin{cases} x'_1 &= a_{1\,1}x_1 + a_{2\,1}x_2 + \cdots + a_{n\,1}x_n \\ x'_2 &= a_{1\,2}x_1 + a_{2\,2}x_2 + \cdots + a_{n\,2}x_n \\ \vdots &= \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ x'_m &= a_{1\,m}x_1 + a_{2\,m}x_2 + \cdots + a_{n\,m}x_n \end{cases}$$

Estas son las ecuaciones de f respecto de las bases B de V y B' de V'.

Nota:

- f es un isomorfismo si y solo si su matriz asociada es regular.
- Cuando se pida o se dé la expresión matricial o las ecuaciones de una aplicación lineal y no se especifique respecto de qué bases, se asume que son respecto de la base canónica de V y la base canónica de V'.

Ejercicio: Sea $f : \mathbb{Q}^2 \longrightarrow \mathbb{Q}^3$ la aplicación lineal definida por $f(x, y) = (x, x + y, x - y)$. Calcular la expresión matricial de f respecto de las bases $B = \{(1, 1), (1, 2)\}$ de $\mathbb{Q}^2$ y $B' = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ de $\mathbb{Q}^3$.

$f(1, 1) = (1, 2, 0) \underset{B}{\equiv} \left(\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}\right)$

$f(1, 2) = (1, 3, -1) \underset{B}{\equiv} \left(\frac{5}{2}, -\frac{3}{2}, \frac{1}{2}\right)$

Por tanto, la matriz asociada a f respecto de B y B' es $\begin{pmatrix} \frac{3}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{5}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$.

Entonces la expresión matricial de f respecto de las bases B y B' es

$$(x', y', z') = (x, y) \begin{pmatrix} \frac{3}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{5}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix} \quad \square$$

[3] Claramente, $\dim(V) = n$ no tiene por qué ser igual a $\dim(V') = m$

[4] Esto se interpreta de la siguiente manera: Si en $(x_1, x_2, \ldots, x_n)$ se introducen las coordenadas de un vector de V respecto de la base B, entonces la m-tupla resultante $(x'_1, x'_2, \ldots, x'_m)$ son las coordenadas de la imagen de ese mismo vector respecto de la base B'.

Ejercicio: Sea $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}$ la matriz asociada a una aplicación lineal $f : {\mathbb{Z}_5}^2 \longrightarrow {\mathbb{Z}_5}^3$ respecto de las bases $B = \{(2,1),(3,1)\}$ de ${\mathbb{Z}_5}^2$ y $B' = \{(1,1,0),(1,0,1),(0,1,1)\}$ de ${\mathbb{Z}_5}^3$. Calcular $f(2,3)$.

Sabemos que la expresión matricial de f es la siguiente:

$$(x', y', z') = (x, y) \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix}$$

Esto significa que si $\vec{v} \in {\mathbb{Z}_5}^2$ y $\vec{v} \underset{B}{\equiv\!\equiv\!\equiv} (x, y)$, entonces $f(\vec{v}) \underset{B'}{\equiv\!\equiv\!\equiv} (x', y', z')$. Por tanto, si calculamos las coordenadas de $(2,3)$ respecto de la base B y las multiplicamos por la matriz asociada, obtendremos las coordenadas de $f(2,3)$ respecto de la base B'.

$$a(2,1) + b(3,1) = (2,3) \implies \begin{cases} 2a + 3b = 2 \\ a + \ b = 3 \end{cases} \implies (a, b) = (2, 1)$$

Tenemos que $(2,3) \underset{B}{\equiv\!\equiv\!\equiv} (2,1)$. Como $(2,1) \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \end{pmatrix} = (4,0,0)$, entonces sabemos que $f(2,3) \underset{B'}{\equiv\!\equiv\!\equiv} (4,0,0)$. Por tanto, $f(2,3) = 4(1,1,0) + 0 + 0 = (4,4,0)$ $\square$

Ejercicio: Calcular una aplicación $f : {\mathbb{Z}_7}^2 \longrightarrow {\mathbb{Z}_7}^3$ verificando que $f(1,2) = (2,3,1)$ y $f(2,5) = (3,4,2)$.

Como los vectores $(1,2)$ y $(2,5)$ forman una base de ${\mathbb{Z}_7}^2$, podemos afirmar que la aplicación lineal que verifica lo propuesto por el enunciado es única.
Supongamos que la expresión matricial de f [5] es $(x', y', z') = (x, y) \cdot A$, donde A es una matriz. Entonces A debe verificar que:

$$\begin{cases} (1,2)A = (2,3,1) \\ (2,5)A = (3,4,2) \end{cases} \implies \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} A = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \end{pmatrix}$$ [6]

Como $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 5 \\ 5 & 1 \end{pmatrix}$ [7], tenemos que

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

Entonces, $f(x, y) = (x, y) \begin{pmatrix} 4 & 0 & 1 \\ 6 & 5 & 0 \end{pmatrix} \implies f(x, y) = (4x + 6y, 5y, x)$ $\square$

[5] Al no especificar, es respecto de las bases canónicas de ${\mathbb{Z}_7}^2$ y ${\mathbb{Z}_7}^3$

[6] Para este tipo de ejercicios es conveniente saber esta propiedad.

[7] En estos ejercicios la matriz que hemos de invertir será regular, ya que sus filas serán una base del espacio vectorial dominio, y por tanto su determinante será distinto de cero (ya que sus filas son L.I)

Ejercicio: Calcular una aplicación lineal $f:\mathbb{R}^3 \longrightarrow \mathbb{R}^2$ verificando que $(1,0,0) \in N(f)$ y que $\mathrm{Im}(f) = \Big\langle \big\{(2,3)\big\} \Big\rangle$.

Sabemos que $f(1,0,0)$ debe ser $(0,0)$, y que el resto de vectores de $\mathbb{R}^3$ deben de tener una imagen de la forma $a \cdot (2,3)$ t. q. $a \in \mathbb{R}$ ya que $\mathrm{Im}(f)$ viene generada por el conjunto $\big\{(2,3)\big\}$.
Supongamos que $f(0,1,0) = 1 \cdot (2,3) = (2,3)$ y $f(0,0,1) = 2 \cdot (2,3) = (4,6)$ [8]. Ahora pasamos a calcular la única aplicación lineal que verifica que $\begin{cases} f(1,0,0) = (0,0) \\ f(0,1,0) = (2,3) \\ f(0,0,1) = (4,6) \end{cases}$.
Entonces la expresión matricial de f será de la forma $(x',y') = (x,y,z) \cdot A$, donde A es una matriz que verifica que:

$$\begin{cases} (1,0,0)A = (0,0) \\ (0,1,0)A = (2,3) \\ (0,0,1)A = (4,6) \end{cases} \implies \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A = \begin{pmatrix} 0 & 0 \\ 2 & 3 \\ 4 & 6 \end{pmatrix} \implies A = \begin{pmatrix} 0 & 0 \\ 2 & 3 \\ 4 & 6 \end{pmatrix}$$

Entonces, $f(x,y,z) = (x,y,z) \begin{pmatrix} 0 & 0 \\ 2 & 3 \\ 4 & 6 \end{pmatrix} \implies f(x,y,z) = (2y+4z, 3y+6z)$ $\square$

Teorema 2. Si $f: V \longrightarrow V'$ es una aplicación lineal entonces
$\dim(V) = \dim\big(N(f)\big) + \dim\big(\mathrm{Im}(f)\big)$.

Ejercicio: Dada la aplicación lineal $f:\mathbb{R}^3 \longrightarrow \mathbb{R}^2$ definida por $f(x,y,z) = (2x+y, 3x+z)$, calcular una base de $\mathrm{Im}(f)$ y una base de $N(f)$.

- Sabemos que $\mathbb{R}^3 = \Big\langle \big\{(1,0,0),(0,1,0),(0,0,1)\big\} \Big\rangle$, así que $\mathrm{Im}(f) = \Big\langle \big\{f(1,0,0), f(0,1,0), f(0,0,1)\big\} \Big\rangle = = \Big\langle \big\{(2,3),(1,0),(0,1)\big\} \Big\rangle$.
  Pasamos a triangularizar para calcular una base de $\mathrm{Im}(f)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

  Entonces una base de $\mathrm{Im}(f)$ es la base canónica de $\mathbb{R}^2$: $B_{can_{\mathbb{R}^2}} = \big\{(1,0),(0,1)\big\}$

- Por el teorema anterior sabemos que $\dim(\mathbb{R}^3) = \dim\big(N(f)\big) + \dim\big(\mathrm{Im}(f)\big)$.
  Como $\dim(\mathbb{R}^3) = 3$ y $\dim\big(\mathrm{Im}(f)\big) = 2$, entonces $\dim\big(N(f)\big) = 1$. Por tanto, una base de $N(f)$ será un elemento no nulo del núcleo.

$$N(f) = \left\{ (x,y,z) \in \mathbb{R}^3 \text{ t. q. } \begin{array}{rl} 2x+y & = 0 \\ 3x \quad +z & = 0 \end{array} \right\} \implies (1,-2,-3) \in N(f)$$

  Así que una base de $N(f)$ es $B_N = \big\{(1,-2,-3)\big\}$

$\square$

[8] Estamos cogiendo los vectores de la base canónica de $\mathbb{R}^3$, ya que, además de ser una base, la matriz resultante de la cual tenemos que calcular la inversa como en el ejercicio anterior será la matriz identidad, y obviamente la inversa de la identidad es ella misma. Nótese que hay infinitas aplicaciones lineales que verifican las condiciones del enunciado, pero nosotros hemos añadido más condiciones para calcular una de ellas.

Teorema 3. Si U y W son subespacios vectoriales de V, entonces se cumple que

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W)$$

Ejercicio: Sean U y W los subespacios vectoriales de ${\mathbb{Z}_5}^3$ generados por $\{(1,1,1),(1,2,3)\}$ y $\{(1,0,0),(2,1,3)\}$, respectivamente. Calcular la dimensión de $U \cap W$.

Para ello, vamos a calcular una base de U, de W y de $U + W = \left\langle \{(1,1,1),(1,2,3),(1,0,0),(2,1,3)\} \right\rangle$ mediante triangularización:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix} \implies \dim(U) = 2$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \end{pmatrix} \implies \dim(W) = 2$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 0 & 0 \\ 2 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 4 & 4 \\ 0 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \implies \dim(U + W) = 3$$

Como $\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W)$, entonces obtenemos que $\dim(U \cap W) = \dim(U) + \dim(W) - \dim(U + W) = 2 + 2 - 3 = \boxed{\mathbf{1}}$ $\square$

Ejercicio: Sean U y W los subespacios vectoriales de ${\mathbb{Z}_5}^4$ generados por $\{(1,2,3,4),(1,0,1,4),(2,2,2,0)\}$ y $\{(1,2,1,1),(1,2,3,3),(2,4,2,2)\}$, respectivamente. ¿${\mathbb{Z}_5}^4 = U \oplus W$?

Recuérdese que ${\mathbb{Z}_5}^4 = U \oplus W$ si y solo si ${\mathbb{Z}_5}^4 = U + W$ y $U \cap W = \{\vec{0}\}$. Pasamos a calcular bases: [9]

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 4 \\ 2 & 2 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 2 \\ 0 & 3 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto $B_U = \{(1,2,3,4),(0,3,1,2)\}$ es una base de U y $\dim(U) = 2$.

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 1 & 2 & 3 & 3 \\ 2 & 4 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto $B_W = \{(1,2,1,1),(0,0,2,2)\}$ es una base de W y $\dim(W) = 2$.
Para calcular una base de $U + W$, tenemos en cuenta que $U + W = \langle B_U \cup B_W \rangle$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 2 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 2 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix} \implies \dim(U + W) = 4$$

[9] Se calcula una base de U y de W por separado para hallar su dimensión, pues lo necesitaremos para comprobar que $U \cap W = \{\vec{0}\}$; además de que es más cómodo trabajar con un conjunto de menos vectores a la hora de calcular una base de $U + W$

Ahora pasamos a comprobar si ${\mathbb{Z}_5}^4 = U \oplus W$:

- Como $\dim(U+W) = 4 = \dim({\mathbb{Z}_5}^4)$, entonces ${\mathbb{Z}_5}^4 = U + W$.
- Sabemos que $\dim(U \cap W) = \dim(U) + \dim(W) - \dim(U+W) = 2 + 2 - 4 = 0$. El único subespacio vectorial con dimensión 0 es el subespacio vectorial $\{\vec{0}\}$, y como $\dim(U \cap W) = 0$, entonces podemos concluir que $U \cap W = \{\vec{0}\}$.

Por tanto, ${\mathbb{Z}_5}^4 = U \oplus W$. $\square$

Ejercicio: ¿Existe una aplicación lineal $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$ tal que $(1,0) \in N(f)$ y $\big\{(1,2,3),(2,1,2)\big\} \subseteq \mathrm{Im}(f)$?

- Como $(1,0) \in N(f)$, entonces $\dim\big(N(f)\big) \geq 1$.
- Además, como $\big\{(1,2,3),(2,1,2)\big\} \subseteq \mathrm{Im}(f)$ y $\big\{(1,2,3),(2,1,2)\big\}$ es un conjunto L.I de vectores, entonces $\dim\big(\mathrm{Im}(f)\big) \geq 2$.

Como f debe de ser una aplicación lineal, entonces debe de cumplirse que $\dim(\mathbb{R}^2) = \dim\big(\mathrm{Im}(f)\big) + \dim\big(N(f)\big)$. Sin embargo, $\dim(\mathbb{R}^2) = 2$; y además, $\dim\big(N(f)\big) \geq 1$ y $\dim\big(\mathrm{Im}(f)\big) \geq 2$, así que $\dim\big(\mathrm{Im}(f)\big) + \dim\big(N(f)\big) \geq 3 > 2$. Por tanto, no puede cumplirse que $\dim(\mathbb{R}^2) = \dim\big(\mathrm{Im}(f)\big) + \dim\big(N(f)\big)$, por lo que no existe ninguna aplicación lineal que verifique las condiciones del enunciado. $\square$

Ejercicio: Dada la aplicación lineal $f : \mathcal{M}_{2\times 2}(\mathbb{Z}_5) \longrightarrow \mathbb{Z}_5[x]_2$ definida por $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a+b)x^2 + (c+d)x + d$:

a) Calcular una base de $\mathrm{Im}(f)$.

b) Calcular una base de $N(f)$.

- Sabemos que $\mathcal{M}_{2\times 2}(\mathbb{Z}_5) = \left\langle \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \right\rangle$.

  Entonces,

  $$\mathrm{Im}(f) = \left\langle \left\{ f\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, f\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, f\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\} \right\rangle = \langle \{x^2, x^2, x, x+1\} \rangle$$

  Calculamos una base de $\mathrm{Im}(f)$ triangularizando la siguiente matriz: [10]

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

  Por tanto una base de $\mathrm{Im}(f)$ es $B_{\mathrm{Im}} = \{x^2, x, 1\}$.

[10] Cuando se trabaja con espacios vectoriales cuyos elementos no son n-tuplas (como matrices o polinomios en nuestro caso), a la hora de triangularizar matrices se usan las coordenadas de cada vector respecto de una base (normalmente la canónica) como filas de la matriz a triangularizar. En este ejercicio usamos la base $B = \{x^2, x, 1\}$ para los polinomios, que es la base canónica con los vectores intercambiados, de modo que $x + 1 \underset{B}{\equiv} (0,1,1)$.

- Sabemos que $\dim\big(\mathcal{M}_{2\times 2}(\mathbb{Z}_5)\big) = \dim\big(\operatorname{Im}(f)\big) + \dim\big(N(f)\big)$. Como $\dim\big(\mathcal{M}_{2\times 2}(\mathbb{Z}_5)\big) = 4$ y $\dim\big(\operatorname{Im}(f)\big) = 3$, entonces $\dim\big(N(f)\big) = 1$. Nótese que $N(f) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_5) \text{ t. q. } \begin{array}{rr} a+b & =0 \\ c+d & =0 \\ d & =0 \end{array} \right\}$, así que una base del núcleo de f será una solución no nula del sistema resultante. Por tanto, $B_N = \left\{ \begin{pmatrix} 1 & 4 \\ 0 & 0 \end{pmatrix} \right\}$ es una base de $N(f)$.

□

Ejercicio: Sea U el subespacio vectorial de $\mathbb{Z}_5[x]_3$ generado por $\{2x^3+3x^2+2x+1,\ 3x^3+2x^2+3x+4,\ x^2+x+1,\ 2x^3+x^2+4\}$. Calcular el cardinal de U.

Primero calculamos una base de U:

$$\begin{pmatrix} 2 & 3 & 2 & 1 \\ 3 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 \\ 2 & 1 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 3 & 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 3 & 3 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 2 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto, $B_U = \{2x^3+3x^2+2x+1,\ x^2+x+1\}$ es una base de U, así que $\dim(U) = 2$. Como U es un espacio vectorial sobre $\mathbb{Z}_5$ de dimensión 2, tenemos que U es isomorfo a ${\mathbb{Z}_5}^2$. En consecuencia, $\#U = \#{\mathbb{Z}_5}^2 = 5^2 = 25$ □

Ejercicio: Sea $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$ la matriz asociada a una aplicación $f : \mathcal{M}_{2\times 2}(\mathbb{Z}_5) \longrightarrow \mathbb{Z}_5[x]_2$ respecto de las bases $B = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ de $\mathcal{M}_{2\times 2}(\mathbb{Z}_5)$ y $B' = \{x^2+x+1, 2x+3, 4\}$ de $\mathbb{Z}_5[x]_2$. Calcular $f\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

El enunciado nos dice que la expresión matricial de f respecto de las bases B y B' es:

$$(x', y', z') = (x, y, z, t) \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Es decir, si $\vec{v} \in \mathcal{M}_{2\times 2}(\mathbb{Z}_5)$ y $\vec{v} \underset{B}{\equiv} (x, y, z, t)$, entonces $f(\vec{v}) \underset{B'}{\equiv} (x', y', z')$.

Nótese que $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \underset{B}{\equiv} (4,4,4,4)$. Además, $(4,4,4,4)\begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = (1,1,4) \implies$

$f\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \underset{B'}{\equiv} (1,1,4) \implies f\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 1(x^2+x+1) + 1(2x+3) + 4(4)$

Por tanto, $f\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = x^2 + 3x$ □

7 Sistemas de ecuaciones lineales

Los sistemas de ecuaciones lineales son el tercer gran concepto que el álgebra lineal se ocupa en estudiar, y justamente el que da nombre y origen a esta rama de las matemáticas. Sin embargo, para poder estudiar bien este tipo de sistemas, es necesario conocer el concepto de rango de una matriz, por lo que este tema empieza con una breve introducción a dicho concepto.
A su vez, en este tema también estudiamos las aplicaciones que tienen los sistemas lineales a otras ramas del álgebra lineal, mayormente en el estudio de espacios vectoriales.

Sea K un cuerpo y $A = \begin{pmatrix} a_{1\,1} & a_{1\,2} & \dots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \dots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \dots & a_{m\,n} \end{pmatrix} \in \mathcal{M}_{m\times n}(K)$.
El rango por filas de la matriz A, denotado $\mathrm{RF}(A)$, es la dimensión del subespacio vectorial de K^n generado por cada una de las filas de A [1]. El rango por columnas de la matriz A, denotado $\mathrm{RC}(A)$, es la dimensión del subespacio vectorial de K^m generado por cada una de las columnas de A.
Ejercicio: Calcular el rango por filas y el rango por columnas de la matriz

$$A = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathbb{Z}_5)$$

- Sea U el subespacio vectorial de ${\mathbb{Z}_5}^4$ generado por las filas de A. Obviamente, $U = \Big\langle \big\{(2,3,4,1),(3,3,2,4),(0,1,1,0)\big) \Big\rangle$.

$$\begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

  Por tanto, $\dim(U) = 2 \implies \mathrm{RF}(A) = 2$ [2]

- Sea W el subespacio vectorial de ${\mathbb{Z}_5}^3$ generado por las columnas de A. Obviamente, $W = \Big\langle \big\{(2,3,0),(3,3,1),(4,2,1),(1,4,0)\big\} \Big\rangle$

$$\begin{pmatrix} 2 & 3 & 0 \\ 3 & 3 & 1 \\ 4 & 2 & 1 \\ 1 & 4 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

  Por tanto, $\dim(W) = 2 \implies \mathrm{RC}(A) = 2$

□

Teorema 1. Si $A \in \mathcal{M}_{m\times n}(K)$, entonces $\mathrm{RF}(A) = \mathrm{RC}(A)$.

Al número $\mathrm{RF}(A) = \mathrm{RC}(A)$ lo llamaremos el rango de A, y lo denotaremos $\mathrm{rang}(A)$.
Sea A una matriz. Entonces se dice que B es una submatriz de A si B se obtiene a partir de A tras quitarle algunas filas y columnas [3].

[1] Esto es equivalente a decir que el rango por filas de A es el número de filas de A que no son combinación lineal de las otras, y el rango por columnas tiene una explicación análoga.
[2] No pasamos por el cálculo de una base de U ya que solo necesitamos la dimensión.
[3] Incluyendo el hecho de no quitar filas y/o no quitar columnas, por lo que toda matriz es submatriz de sí misma.

Ejemplo: Si $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 0 & 3 \\ 3 & 1 & 2 & 0 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathbb{R})$, entonces $B = \begin{pmatrix} 1 & 4 \\ 3 & 0 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$ es una submatriz de A ya que se ha obtenido tras quitarle a A las columnas 2 y 3 y la fila 2.

Teorema 2. El rango de una matriz es el máximo de los órdenes de sus submatrices cuadradas regulares. [4]

Ejercicio: Calcular el rango de la matriz $A = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 3 & 2 & 4 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathbb{Z}_5)$

La matriz $\begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}$ es una submatriz de A con determinante $3 \cdot 1 - 3 \cdot 0 = 3 \neq 0$, por lo que $\text{rang}(A) \geq 2$. Veamos si $\text{rang}(A) = 2$ ó $\text{rang}(A) = 3$ [5].

Como $\begin{vmatrix} 2 & 3 & 4 \\ 3 & 3 & 2 \\ 0 & 1 & 1 \end{vmatrix} = 0$, tenemos que la columna $\begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}$ es combinación lineal de las columnas $\begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$ y $\begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix}$ [6].

Como $\begin{vmatrix} 2 & 3 & 1 \\ 3 & 3 & 4 \\ 0 & 1 & 0 \end{vmatrix} = 0$, tenemos que la columna $\begin{pmatrix} 1 \\ 4 \\ 0 \end{pmatrix}$ es también combinación lineal de $\begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$ y $\begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix}$.

Por tanto, $\text{RC}(A) = 2 \implies \text{rang}(A) = 2$ $\square$

Ejercicio: ¿Es $\{(1,1,0),(1,0,1),(0,1,1)\}$ una base de ${\mathbb{Z}_5}^3$?

$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{vmatrix} = (0+0+0) - (0+1+1) = 3 \neq 0 \implies \text{rang} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} = 3$

$\implies \dim\left(\left\langle \{(1,1,0),(1,0,1),(0,1,1)\} \right\rangle\right) = 3 \implies \{(1,1,0),(1,0,1),(0,1,1)\}$ es L.I

$\implies \{(1,1,0),(1,0,1),(0,1,1)\}$ es una base de ${\mathbb{Z}_5}^3$ $\square$

Ejercicio: ¿Es el conjunto $\{(1,2,1),(1,3,1)\} \subseteq {\mathbb{Z}_5}^3$ L.I?

Sea la matriz $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 1 \end{pmatrix}$. Como $\begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} \neq 0$, entonces tenemos que $\text{RF}(A) = \text{rang}(A) = 2$. Por tanto, los vectores son L.I. $\square$

[4] Es decir, el rango de una matriz es el mayor de los órdenes de los determinantes no nulos de las submatrices de A. Por ejemplo, si A es una matriz de orden 4×5 que tiene una submatriz cuadrada de orden 3 con determinante no nulo, y todos los determinantes de las submatrices de orden 4 de A son 0, entonces $\text{rang}(A) = 3$.

[5] El rango de A no puede ser mayor que 3, ya que para toda matriz A de orden $m \times n$, el rango por filas (menor o igual a m) coincide con el rango por columnas (menor o igual a n) y por tanto $\text{rang}(A) \leq \min\{m, n\}$

[6] El teorema anterior nos dice que si una matriz cuadrada tiene determinante 0, entonces al menos una de sus filas es combinación lineal del resto (también aplica a columnas)

7.1 Expresión matricial de un sistema de ecuaciones

Un sistema de m ecuaciones lineales con n incógnitas sobre un cuerpo K es una expresión de la siguiente forma:

$$\begin{cases} a_{1\,1}x_1 + a_{1\,2}x_2 + \cdots + a_{1\,n}x_n &= b_1 \\ a_{2\,1}x_1 + a_{2\,2}x_2 + \cdots + a_{2\,n}x_n &= b_2 \\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{cases}$$

donde $a_{1\,1}, a_{1\,2}, \ldots, a_{mn} \in K$ [7], $b_1, b_2, \ldots, b_m \in K$ [8], y $x_i, x_2, \ldots, x_n$ son incógnitas. Una solución del sistema es una n-tupla $(s_1, s_2, \ldots, s_n) \in K^n$ tal que si se sustituyen los valores $x_1 = s_1, x_2 = s_2, \ldots, x_n = s_n$, se cumplen todas las m ecuaciones del sistema. Estas igualdades se pueden expresar como una sola igualdad entre matrices:

$$\begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \ldots & a_{m\,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

A la cual se le llama la expresión matricial del sistema.

A las matrices $A \coloneqq \begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\,1} & a_{m\,2} & \ldots & a_{m\,n} \end{pmatrix}$, $X \coloneqq \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ y $B \coloneqq \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$ se les llama la matriz de los coeficientes, la matriz incógnita y la matriz de los términos independientes respectivamente.

Además, se define la matriz ampliada como $A' \coloneqq \begin{pmatrix} a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} & b_1 \\ a_{2\,1} & a_{2\,2} & \ldots & a_{2\,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m\,1} & a_{m\,2} & \ldots & a_{m\,n} & b_m \end{pmatrix}$.

7.2 Tipos especiales de sistemas de ecuaciones

Si un sistema tiene solución diremos que es compatible, y de lo contrario diremos que es incompatible. Un sistema con una única solución es compatible determinado, y un sistema con más de una solución es compatible indeterminado. [9]

Dos sistemas de ecuaciones sobre el mismo cuerpo se dice que son equivalentes si tienen las mismas soluciones.

Proposición 1. En todo sistema de ecuaciones sobre un cuerpo K se cumple lo siguiente:

1. Si intercambiamos de posición dos ecuaciones distintas, obtendremos un sistema equivalente.
2. Si multiplicamos ambos miembros de una ecuación por un elemento no nulo de K, obtendremos un sistema equivalente.
3. Si a una ecuación le sumamos otra ecuación multiplicada por un elemento de K [10], obtendremos un sistema equivalente.

[7] Estos son los coeficientes del sistema

[8] Estos son los términos independientes del sistema

[9] A lo largo de este tema, abreviaremos "sistema incompatible", "sistema compatible determinado" y "sistema compatible indeterminado" como S.I, S.C.D, y S.C.I respectivamente.

[10] Por "sumar una ecuación a otra" nos referimos a sumar todos los elementos del lado izquierdo de una al lado izquierdo de la otra, e igual con el lado derecho.

7.3 Método de Gauss

1. [11] Resolver el siguiente sistema con coeficientes en $\mathbb{Z}_7$: $\begin{cases} x+2y+3z=1 \\ x+\ y+2z=0 \\ 2x+\ y+4z=3 \end{cases}$

$$\begin{cases} x+2y+3z=1 \\ x+\ y+2z=0 \\ 2x+\ y+4z=3 \end{cases} \overset{\substack{E_2\to E_2-E_1 \\ E_3\to E_3+5E_1}}{\sim} \begin{cases} x+2y+3z=1 \\ 6y+6z=6 \\ 4y+5z=1 \end{cases} \overset{\substack{E_3\to E_3+4E_2 \\ E_2\to 6E_2}}{\sim} \begin{cases} x+2y+3z=1 \\ y+\ z=1 \\ z=4 \end{cases}$$

$z=4 \implies y+4=1 \implies y=4 \implies x+2\cdot 4+3\cdot 4=1 \implies x=2$

Por tanto [12], $(x,y,z)=(2,4,4)$ $\square$

2. Resolver el siguiente sistema con coeficientes en $\mathbb{Q}$: $\begin{cases} x+\ y+\ z=1 \\ x+2y-\ z=2 \\ 2x+\ y+4z=0 \end{cases}$

$$\begin{cases} x+\ y+\ z=1 \\ x+2y-\ z=2 \\ 2x+\ y+4z=0 \end{cases} \overset{\substack{E_2\to E_2-E_1 \\ E_3\to E_3-2E_1}}{\sim} \begin{cases} x+y+\ z=1 \\ y-2z=1 \\ -y+2z=-2 \end{cases} \overset{E_3\to E_3+E_2}{\sim} \begin{cases} x+y+\ z=1 \\ y-2z=1 \\ 0=-1 \end{cases}$$

Hemos obtenido una igualdad falsa. Por tanto, el sistema es incompatible y no tiene solución. $\square$

3. Resolver el siguiente sistema con coeficientes en $\mathbb{Z}_5$: $\begin{cases} x+\ y+\ z=1 \\ 2x+\ y+3z=0 \\ x+4y+3z=2 \end{cases}$

$$\begin{cases} x+\ y+\ z=1 \\ 2x+\ y+3z=0 \\ x+4y+3z=2 \end{cases} \overset{\substack{E_2\to E_2+3E_1 \\ E_3\to E_3-E_1}}{\sim} \begin{cases} x+\ y+\ z=1 \\ 4y+\ z=3 \\ 3y+2z=1 \end{cases} \overset{E_3\to E_3+3E_2}{\sim} \begin{cases} x+\ y+z=1 \\ 4y+z=3 \\ 0=0 \end{cases}$$

La última ecuación no aporta nada al sistema. Por tanto tenemos un sistema de 2 ecuaciones y 3 incógnitas, así que es un S.C.I[13]. Convertimos una incógnita en parámetro y despejamos las otras dos:

$$z=\lambda \implies \begin{cases} 4y=3+4\lambda \implies y=2+\lambda \\ x=1+4y+4\lambda \implies x=1+4(2+\lambda)+4\lambda \implies x=4+3\lambda \end{cases}$$

Por cada valor que le demos a $\lambda \in \mathbb{Z}_5=\{0,1,2,3,4\}$, obtenemos una solución. Por tanto, el sistema tiene 5 soluciones: [14]

$$(x,y,z)=(4+3\lambda,\ 2+\lambda,\ \lambda) \text{ t. q. } \lambda \in \mathbb{Z}_5 \quad \square$$

Teorema 3 (Teorema de Rouché-Frobenius)**.** Un sistema de ecuaciones lineales es compatible si y solo si el rango de su matriz de coeficientes coincide con el rango de su matriz ampliada. Además, es compatible determinado si y solo si ambos rangos coinciden con el número de incógnitas del sistema.

[11] Al igual que el punto 6 del tema 2, este punto consiste de ejercicios a modo de ejemplo de cómo se usa el método de Gauss para resolver sistemas.

[12] Como se puede ver, el método de Gauss consiste en sumar y multiplicar ecuaciones hasta obtener una expresión en la que una incógnita aparezca por sí sola (nótese que en el proceso se triangulariza la matriz de los coeficientes). Después se usa el valor de esa incógnita para resolver el resto.

[13] Un sistema con más incógnitas que ecuaciones no puede ser compatible determinado, y si fuera incompatible el método de Gauss nos habría llevado a una igualdad falsa.

[14] Nótese que si la solución de un S.C.I con coeficientes en un cuerpo finito de cardinal k depende de n parámetros, entonces el sistema tiene k^n soluciones.

Ejercicio: Estudiar[15] el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_5$:

$$\begin{cases} 2x+4y+4z=1 \\ 3x+\ y+2z=2 \\ 2x+4y\ \ \ \ \ =3 \end{cases}$$

Vamos a calcular los rangos de las matrices $A=\begin{pmatrix}2&4&4\\3&1&2\\2&4&0\end{pmatrix}$ y $A'=\begin{pmatrix}2&4&4&1\\3&1&2&2\\2&4&0&3\end{pmatrix}$:

$$\begin{pmatrix}2&4&4\\3&1&2\\2&4&0\end{pmatrix}\sim\begin{pmatrix}2&4&4\\0&0&1\\0&0&1\end{pmatrix}\sim\begin{pmatrix}2&4&4\\0&0&1\\0&0&0\end{pmatrix}\implies \operatorname{rang}(A)=2$$

$$\begin{pmatrix}2&4&4&1\\3&1&2&2\\2&4&0&3\end{pmatrix}\sim\begin{pmatrix}2&4&4&1\\0&0&1&3\\0&0&1&2\end{pmatrix}\sim\begin{pmatrix}2&4&4&1\\0&0&1&3\\0&0&0&4\end{pmatrix}\implies \operatorname{rang}(A')=3$$

Como $\operatorname{rang}(A)\neq\operatorname{rang}(A')$, el sistema propuesto es un S.I. $\square$

Ejercicio: Estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_7$ y que depende del parámetro a: $\begin{cases} ax+\ y+\ z=1 \\ \ x+ay+\ z=0 \\ \ x+\ y+az=a \end{cases}$ [16]

Primero calculamos el rango de la matriz de coeficientes $A=\begin{pmatrix}a&1&1\\1&a&1\\1&1&a\end{pmatrix}$ en función de a. Como es cuadrada, calculamos su determinante:

$$\begin{vmatrix}a&1&1\\1&a&1\\1&1&a\end{vmatrix}=a^3+1+1-a-a-a=a^3+4a+2$$

$a^3+4a+2=0\implies a\in\{1,5\}$. Por tanto:

- Si $a\notin\{1,5\}$, entonces $\operatorname{rang}(A)=3\implies \operatorname{rang}\begin{pmatrix}a&1&1&1\\1&a&1&0\\1&1&a&a\end{pmatrix}=3$. Por tanto, el sistema es compatible determinado.
- Si $a=1$, entonces $A=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}$ y $A'=\begin{pmatrix}1&1&1&1\\1&1&1&0\\1&1&1&1\end{pmatrix}$. Claramente $\operatorname{rang}(A)=1$, y como $\begin{vmatrix}1&1\\1&0\end{vmatrix}\neq 0$ entonces $\operatorname{rang}(A')=2$. Por tanto, el sistema es incompatible.
- Si $a=5$, entonces $A=\begin{pmatrix}5&1&1\\1&5&1\\1&1&5\end{pmatrix}$ y $A'=\begin{pmatrix}5&1&1&1\\1&5&1&0\\1&1&5&5\end{pmatrix}$. Como $\operatorname{rang}(A)<3$ y $\begin{vmatrix}5&1\\1&5\end{vmatrix}\neq 0$, tenemos que $\operatorname{rang}(A)=2$. Además, $\begin{vmatrix}5&1&1\\1&5&0\\1&1&5\end{vmatrix}\neq 0$ así que $\operatorname{rang}(A')=3$. Por tanto el sistema es incompatible.

[15] Estudiar un sistema es determinar si es un S.I, S.C.D ó un S.C.I.

[16] Debido al Teorema de Rouché-Frobenius, este tipo de ejercicios consisten en determinar el rango de las matrices de coeficientes y ampliada según varían los parámetros. En la mayoría de las ocasiones, se dan varios casos particulares que se tienen que estudiar por separado.

Entonces el sistema del enunciado es: $\begin{cases} \text{S.C.D} & \text{si } a \in \{0,2,3,4,6\} \\ \text{S.I} & \text{si } a \in \{1,5\} \end{cases}$ □

Ejercicio: Estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{R}$ y que depende de los parámetros a y b: $\begin{cases} ax + y + z = 1 \\ x + y + z = b \\ ax + by + z = 1 \end{cases}$

$$|A| = \begin{vmatrix} a & 1 & 1 \\ 1 & 1 & 1 \\ a & b & 1 \end{vmatrix} = \cancel{a} + a + b - \cancel{a} - 1 - ab = a(1-b) + b - 1 = (a-1)(1-b)$$

$(a-1)(1-b) = 0 \implies \begin{cases} a-1=0 & \implies & a=1 \\ 1-b=0 & \implies & b=1 \end{cases}$ Por tanto, se dan 4 casos:

- Si $\underline{a \neq 1 \text{ y } b \neq 1}$, entonces
  $\text{rang}(A) = 3 \implies \text{rang}(A') = \text{rang}\begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & 1 & b \\ a & b & 1 & 1 \end{pmatrix} = 3$. Por tanto el sistema es compatible determinado.
- Si $\underline{a = 1 \text{ y } b \neq 1}$, entonces $\text{rang}(A) = 2$ pero $\text{rang}(A') = 3$. Por tanto el sistema es incompatible.
- Si $\underline{a \neq 1 \text{ y } b = 1}$, entonces $\text{rang}(A) = \text{rang}(A') = 2$. Como el número de incógnitas es 3, entonces el sistema es compatible indeterminado.
- Si $\underline{a = b = 1}$, entonces el rango de ambas matrices es claramente $1 < 3$. Por tanto el sistema es compatible indeterminado.

Entonces el sistema del enunciado es: $\begin{cases} \text{S.C.D} & \text{si } a \neq 1 \text{ y } b \neq 1 \\ \text{S.C.I} & \text{si } b = 1 \\ \text{S.I} & \text{si } a = 1 \text{ y } b \neq 1 \end{cases}$ □

Ejercicio: Estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_5$ y que depende del parámetro a: $\begin{cases} ax + y + z = 1 \\ x + y + z = 2 \end{cases}$

$A = \begin{pmatrix} a & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Si $a = 1$, claramente $\text{rang}(A) = 1$, de lo contrario $\text{rang}(A) = 2$. Sin embargo, $\text{rang}(A') = \text{rang}\begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix} = 2$ porque $\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \neq 0$.

Por tanto, el sistema propuesto es: $\begin{cases} \text{S.C.I} & \text{si } a = 1 \\ \text{S.I} & \text{si } a \neq 1 \end{cases}$ □

Ejercicio: Estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{R}$ y que depende del parámetro a: $\begin{cases} ax + y + z = 1 \\ x - y + z = 1 \end{cases}$

Nótese que la matriz de coeficientes, $A = \begin{pmatrix} a & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}$; y la matriz ampliada, $A' = \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix}$ tienen ambas rango 2 ya que $\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} \neq 0$. Por tanto, el sistema propuesto es compatible indeterminado independientemente del valor de a.
□

Ejercicio: Estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_7$ y que depende del parámetro a: $\begin{cases} ax + y + z = 1 \\ x + 2y + az = 2 \end{cases}$

La matriz de coeficientes del sistema es $A = \begin{pmatrix} a & 1 & 1 \\ 1 & 2 & a \end{pmatrix}$. Nótese que $\begin{vmatrix} a & 1 \\ 1 & 2 \end{vmatrix} = 2a - 1$ y $2a - 1 = 0 \implies a = 4$.

- Si $a \neq 4$, entonces $\operatorname{rang}(A) = 2$ y $\operatorname{rang}(A') = \operatorname{rang} \begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 2 & a & 2 \end{pmatrix} = 2$. Por tanto el sistema es compatible indeterminado.
- Si $a = 4$, entonces también tenemos que $\operatorname{rang}(A) = 2$ ya que $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix}$ y $\begin{vmatrix} 1 & 1 \\ 2 & 4 \end{vmatrix} \neq 0$. Por tanto, $\operatorname{rang}(A) = \operatorname{rang}(A') = 2$ y el sistema es también compatible indeterminado.

Por consiguiente, el sistema del enunciado es compatible indeterminado independientemente del valor de a. $\square$

Un sistema de ecuaciones lineales es de Cramer si su matriz de coeficientes es regular. Todo sistema de Cramer es compatible determinado.

7.4 Fórmula de Cramer

Sea $A \cdot X = B$ la expresión matricial de un sistema de Cramer con n incógnitas. Entonces su única solución es

$$(x_1, x_2, \ldots, x_n) = |A|^{-1} \cdot (|M_1|, |M_2|, \ldots, |M_n|)$$

donde, para todo $i \in \{1, 2, \ldots, n\}$, M_i es la matriz que se obtiene al sustituir la i-ésima columna de A por la matriz B.

Ejercicio: Probar que el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_7$ es de Cramer y calcular su única solución con la fórmula de Cramer: $\begin{cases} x + y + z = 1 \\ x + 6y + z = 0 \\ x + y + 6z = 2 \end{cases}$

$|A| = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 6 & 1 \\ 1 & 1 & 6 \end{vmatrix} = 1 + 1 + 1 - 6 - 1 - 6 = 4 \neq 0 \implies$ El sistema del enunciado es un sistema de Cramer. Su única solución es:

$$(x, y, z) = 4^{-1} \cdot \left(\begin{vmatrix} 1 & 1 & 1 \\ 0 & 6 & 1 \\ 2 & 1 & 6 \end{vmatrix}, \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 2 & 6 \end{vmatrix}, \begin{vmatrix} 1 & 1 & 1 \\ 1 & 6 & 0 \\ 1 & 1 & 2 \end{vmatrix} \right) = 2(4, 2, 5) = (1, 4, 3) \quad \square$$

7.5 Ecuaciones cartesianas de un subespacio vectorial

Sea V un espacio vectorial sobre un cuerpo K, U un subespacio vectorial de V,
$B = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ una base de V y $B_U = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_r\}$ una base de U [17]. Supongamos que $\vec{u}_1 \underset{B}{\equiv} (a_{1\,1}, a_{1\,2}, \ldots, a_{1\,n})$; $\vec{u}_2 \underset{B}{\equiv} (a_{2\,1}, a_{2\,2}, \ldots, a_{2\,n})$; $\ldots$; $\vec{u}_r \underset{B}{\equiv} (a_{r\,1}, a_{r\,2}, \ldots, a_{r\,n})$. Sea
$\vec{x} \in V$ t. q. $\vec{x} \underset{B}{\equiv} (x_1, x_2, \ldots, x_n)$. Entonces $\vec{x} \in U$ si y solo si se cumple que

$$\operatorname{rang} \begin{pmatrix} a_{1\,1} & a_{2\,1} & \ldots & a_{r\,1} & x_1 \\ a_{1\,2} & a_{2\,2} & \ldots & a_{r\,2} & x_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{1\,n} & a_{2\,n} & \ldots & a_{r\,n} & x_n \end{pmatrix} = r$$

Para que esto ocurra, varios determinantes deben de valer 0. El desarrollo de estos determinantes igualados a 0 nos proporcionan $n - r$ ecuaciones L.I de la forma

$$\begin{cases} b_{1\,1}x_1 + b_{1\,2}x_2 + \ldots + b_{1\,n}x_n = 0 \\ b_{2\,1}x_1 + b_{2\,2}x_2 + \ldots + b_{2\,n}x_n = 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots \\ b_{(n-r)\,1}x_1 + b_{(n-r)\,2}x_2 + \ldots + b_{(n-r)\,n}x_n = 0 \end{cases}$$

Donde $b_{1\,1}, b_{1\,2}, \ldots, b_{(n-r)\,n} \in K$.
A estas ecuaciones se les llama las ecuaciones cartesianas de U respecto de la base B [18].
Nota:

1. U viene dado por $n - r = \dim(V) - \dim(U)$ ecuaciones cartesianas L.I [19]
2. Si se dan o se piden las ecuaciones cartesianas de un subespacio vectorial sin especificar la base respecto de la que son, se asume que son respecto de la base canónica.

Ejercicio: Sea U el subespacio vectorial de ${\mathbb{Z}_5}^3$ generado por $\{(2,3,4),(1,4,2)\}$. Calcular las ecuaciones cartesianas de U respecto de la base $B = \{(1,1,0),(1,0,1),(0,1,1)\}$.

Primero calculamos una base de U:

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 & 4 \\ 0 & 0 & 0 \end{pmatrix}$$

Tenemos que $\{(2,3,4)\}$ es una base de U.
Ahora calculamos las coordenadas del vector $(2,3,4)$ respecto de la base B:

$$a(1,1,0)+b(1,0,1)+c(0,1,1) = (2,3,4) \implies \begin{cases} a+b \quad\;\; = 2 \\ a \quad\;\; + c = 3 \\ \quad\; b+c = 4 \end{cases} \implies (a,b,c) = (3,4,0)$$

Por tanto $(2,3,4) \underset{B}{\equiv} (3,4,0)$. Ahora, para determinar las ecuaciones cartesianas de U,
imponemos que $\operatorname{rang} \begin{pmatrix} 3 & x \\ 4 & y \\ 0 & z \end{pmatrix} = \dim(U) = 1$.

[17] Nótese que $n = \dim(V) \leq \dim(U) = r$.
[18] Esto se interpreta de la siguiente forma: U es el subespacio vectorial de V con todos los vectores cuyas coordenadas respecto de la base B cumplen todas las ecuaciones cartesianas.
[19] Esto tiene como consecuencia que si un subespacio vectorial U de V viene dado por m ecuaciones cartesianas L.I, entonces $\dim(U) = \dim(V) - m$.

Para que esto se cumpla, $\begin{vmatrix} 3 & x \\ 4 & y \end{vmatrix} = \begin{vmatrix} 3 & x \\ 0 & z \end{vmatrix} = 0$ [20]. Por tanto, las ecuaciones cartesianas de U respecto de la base B son $\begin{cases} 3y - 4x = 0 \\ 3z = 0 \end{cases} \Longrightarrow \begin{cases} x + 3y = 0 \\ z = 0 \end{cases}$ □

Ejercicio: Sea U el subespacio vectorial de $\mathbb{Q}^4$ generado por $\{(1,2,3,1),(1,1,1,1),(3,5,7,3)\}$. Calcular las ecuaciones cartesianas de U.

Ya que no se especifica la base respecto de la que calcularlas, supondremos que son las ecuaciones cartesianas respecto de la base canónica:
$B_{can} = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$.
Calculamos una base de U:

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 1 & 1 & 1 \\ 3 & 5 & 7 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & -1 & -2 & 0 \\ 0 & -1 & -2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto una base de U es $\{(1,2,3,1),(0,-1,-2,0)\}$.
Nótese que $(1,2,3,1) \underset{B_{can}}{\equiv} (1,2,3,1)$ y $(0,-1,-2,0) \underset{B_{can}}{\equiv} (0,-1,-2,0)$. Ahora imponemos que $\operatorname{rang} \begin{pmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 3 & -2 & z \\ 1 & 0 & t \end{pmatrix} = 0 \Longrightarrow \begin{vmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 3 & -2 & z \end{vmatrix} = \begin{vmatrix} 1 & 0 & x \\ 2 & -1 & y \\ 1 & 0 & t \end{vmatrix} = 0$

Por tanto, las ecuaciones cartesianas de U son: $\begin{cases} -x + 2y - z = 0 \\ x - t = 0 \end{cases}$ □

Ejercicio: Sean U y W los subespacios vectoriales de ${\mathbb{Z}_5}^3$ generados por $\{(1,1,1),(1,2,1)\}$ y $\{(1,4,3),(0,0,4)\}$ respectivamente. Calcular una base de $U \cap W$.

- Calculamos las ecuaciones cartesianas de U [21], sabiendo que $\{(1,1,1),(1,2,1)\}$ ya es una base de U porque es L.I [22]. Tras imponer que $\operatorname{rang} \begin{pmatrix} 1 & 1 & x \\ 1 & 2 & y \\ 1 & 1 & z \end{pmatrix} = 2$, obtenemos que $\begin{vmatrix} 1 & 1 & x \\ 1 & 2 & y \\ 1 & 1 & z \end{vmatrix} = 0 \Longrightarrow 4x + z = 0$.

  Por tanto, $U = \{(x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } 4x + z = 0\}$
- Calculamos las ecuaciones cartesianas de W, sabiendo que $\{(1,4,3),(0,0,4)\}$ también es base de W porque es L.I. Imponemos que $\operatorname{rang} \begin{pmatrix} 1 & 0 & x \\ 4 & 0 & y \\ 3 & 4 & z \end{pmatrix} = 2$, lo cual solo se cumple si $\begin{vmatrix} 1 & 0 & x \\ 4 & 0 & y \\ 3 & 4 & z \end{vmatrix} = 0 \Longrightarrow x + y = 0$.

  Por tanto, $W = \{(x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } x + y = 0\}$

[20] Ya que para que la matriz tenga rango 1, sus filas deben de ser L.D: por ejemplo, imponemos que las filas $(4,y)$ y $(0,z)$ sean combinación lineal de la fila $(3,x)$, lo que da lugar a dos ecuaciones linealmente independientes

[21] Ya que no se especifica, son respecto de la base canónica.

[22] Como U viene generado por el conjunto $\{(1,1,1),(1,2,1)\}$ y además éste último es L.I, entonces el conjunto es una base de U por definición.

Como $U \cap W$ es la intersección entre los vectores de U y los vectores de W, entonces $U \cap W = \left\{ (x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } \begin{matrix} 4x & & +z=0 \\ & x+y & =0 \end{matrix} \right\}$. Las 2 ecuaciones son L.I, así que tenemos que $\dim(U \cap W) = \dim({\mathbb{Z}_5}^3) - 2 = 1$. Por tanto, una base de $U \cap W$ es un elemento no nulo de dicho subespacio. Como $(1,4,1) \in U \cap W$, podemos concluir que $B = \{(1,4,1)\}$ es una base de $U \cap W$. $\square$

Ejercicio: Sea $U = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{matrix} x+ & y+z+t=0 \\ 2x+3y+z+t=0 \\ x+2y & =0 \end{matrix} \right\}$. Calcular una base de U.

Primero vemos cuántas de las ecuaciones anteriores son L.I, triangularizando [23]:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 2 & 3 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 4 & 4 & 0 \\ 0 & 1 & 4 & 4 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 4 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Tenemos que $U = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{matrix} x+y+ & z+ & t=0 \\ & y+4z+4t & =0 \end{matrix} \right\}$. Como hay 2 ecuaciones L.I, entonces tenemos que $\dim(U) = \dim({\mathbb{Z}_5}^4) - 2 = 2$. Por tanto una base de U son dos elementos L.I de U.

Como el sistema de ecuaciones por el que U viene dado es un S.C.I [24], tomamos dos parámetros $z = \lambda, t = \mu$ para obtener soluciones.

$$\left\{ \begin{matrix} x+y=4\lambda+4\mu \\ y=\lambda+\mu \end{matrix} \right\} \implies \left\{ \begin{array}{l} \lambda=1, \mu=0 \implies x=3, y=1 \implies (3,1,1,0) \in U \\ \lambda=0, \mu=1 \implies x=3, y=1 \implies (3,1,0,1) \in U \end{array} \right.$$

Por tanto[25], $B = \{(3,1,1,0),(3,1,0,1)\}$ es una base de U.

Ejercicio: Sea U el subespacio vectorial de $\mathbb{Q}^4$ generado por $\{(1,1,1,1),(1,2,3,3)\}$ y $W = \{(x,y,z,t) \in \mathbb{Q}^4 \text{ t. q. } x+y-z-t=0\}$. Calcular una base de $U+W$.

Primero calculamos una base de W a partir de la ecuación por la que viene dado. Como tenemos una ecuación L.I entonces $\dim(W) = \dim(\mathbb{Q}^4) - 1 = 3$ así que necesitamos tres elementos L.I de W para obtener una base.

Tomamos tres parámetros $y = \lambda, z = \mu, t = \nu$ para obtener soluciones a la ecuación $x+y-z-t=0 \implies x = -\lambda+\mu+\nu$

$$\left\{ \begin{array}{lll} \lambda=1, \mu=\nu=0 & \implies x=-1 & \implies (-1,1,0,0) \in W \\ \lambda=0, \mu=1, \nu=0 & \implies x=1 & \implies (1,0,1,0) \in W \\ \lambda=\mu=0, \nu=1 & \implies x=1 & \implies (1,0,0,1) \in W \end{array} \right.$$

Por tanto $B_W = \{(-1,1,0,0),(1,0,1,0),(1,0,0,1)\}$ es una base de W.

---

[23] De forma similar al método para calcular bases de subespacios vectoriales, triangularizamos la matriz ampliada del sistema de ecuaciones dado por el subespacio. Nótese que como la columna de términos independientes tiene cero en todos sus elementos, no incluirla en la matriz no afecta el resultado.

[24] Nótese que si en un sistema de ecuaciones lineales todos los términos independientes son 0, entonces el sistema siempre es compatible (a este tipo de sistemas se les llama homogéneos). Además, el sistema $\begin{cases} x+y+ & z+ & t=0 \\ & y+4z+4t & =0 \end{cases}$ tiene más incógnitas que ecuaciones, y por tanto es compatible indeterminado.

[25] Al darle los valores $(1,0)$ y $(0,1)$ a (λ,μ), obtendremos dos soluciones L.I del sistema de forma asegurada. Esto funciona de manera análoga con SS.CC.II que dependan de tres o más parámetros.

Pasamos a calcular una base de $U+W$, teniendo en cuenta que viene generado por $\{(1,1,1,1),(1,2,3,3),\ (-1,1,0,0),(1,0,1,0),(1,0,0,1)\}$:

$$\begin{pmatrix}1&1&1&1\\1&2&3&3\\-1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\0&1&2&2\\0&2&1&1\\0&-1&0&-1\\0&-1&-1&0\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\0&1&2&2\\0&0&-3&-3\\0&0&2&1\\0&0&1&2\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\0&1&2&2\\0&0&-3&-3\\0&0&0&-1\\0&0&0&1\end{pmatrix}\sim\dots$$

$$\dots\sim\begin{pmatrix}1&1&1&1\\0&1&2&2\\0&0&-3&-3\\0&0&0&-1\\0&0&0&0\end{pmatrix}\sim\begin{pmatrix}1&1&1&1\\0&1&2&2\\0&0&3&3\\0&0&0&1\\0&0&0&0\end{pmatrix}$$

Por tanto $B=\{(1,1,1,1),(0,1,2,2),(0,0,3,3),(0,0,0,1)\}$ es una base de $U+W$ [26].
□

Ejercicio: Dada la aplicación lineal $f:{\mathbb{Z}_5}^4\longrightarrow{\mathbb{Z}_5}^3$ definida por $f(x,y,z,t)=(x+y+z+t,x+y+z+2t,x+y+z)$, calcular una base de $N(f)$.

Sabemos que $N(f)=\left\{(x,y,z,t)\in{\mathbb{Z}_5}^4\ \text{t. q.}\ \begin{array}{r}x+y+z+\ t=0\\x+y+z+2t=0\\x+y+z\ \ \ \ =0\end{array}\right\}$. Ahora vemos cuántas de esas ecuaciones son L.I:

$$\begin{pmatrix}1&1&1&1&0\\1&1&1&2&0\\1&1&1&0&0\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&0&0&1&0\\0&0&0&4&0\end{pmatrix}\sim\begin{pmatrix}1&1&1&1&0\\0&0&0&1&0\\0&0&0&0&0\end{pmatrix}$$

Por tanto, $N(f)=\left\{(x,y,z,t)\in{\mathbb{Z}_5}^4\ \text{t. q.}\ \begin{array}{r}x+y+z+t=0\\t=0\end{array}\right\}$. Como hay dos ecuaciones L.I entonces tenemos que $\dim\big(N(f)\big)=\dim({\mathbb{Z}_5}^4)-2=2$, así que una base de $N(f)$ son dos elementos L.I del núcleo de f.

Como $(1,4,0,0)\in N(f)$, $(1,0,4,0)\in N(f)$ y $\operatorname{rang}\begin{pmatrix}1&4&0&0\\1&0&4&0\end{pmatrix}=2$

(ya que $\begin{vmatrix}4&0\\0&4\end{vmatrix}\neq 0$), entonces $B=\{(1,4,0,0),(1,0,4,0)\}$ es una base de $N(f)$. □

Ejercicio: 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?

Nótese que como $\{(2,3,2),(1,3,3)\}$ ya es una base de U (es L.I), entonces $\dim(U)=2$. Por tanto, como $\{(1,1,5),(2,0,5)\}$ es también L.I, entonces será una base de U si y solo si $(1,1,5)$ y $(2,0,5)$ pertenecen a U.

Calculamos las ecuaciones cartesianas de U, imponiendo que

$$\operatorname{rang}\begin{pmatrix}2&1&x\\3&3&y\\2&3&z\end{pmatrix}=2\implies\begin{vmatrix}2&1&x\\3&3&y\\2&3&z\end{vmatrix}=0\implies 3x+3y+3z=0\implies x+y+z=0.$$

[26] Nótese que ya que $\#B=4$, entonces $\dim(U+W)=4$. Por tanto $U+W=\mathbb{Q}^4$ así que cualquier base de $\mathbb{Q}^4$ es también base de $U+W$; por ejemplo, la base canónica $B_{can}=\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$.

Por tanto $U = \{(x,y,z) \in {\mathbb{Z}_7}^3 \text{ t. q. } x+y+z=0\}$. Sustituimos las coordenadas de $(1,1,5)$ y $(2,0,5)$ en la ecuación por la que viene dado U:

$$\begin{cases} x=1, y=1, z=5 \longrightarrow 1+1+5=0 \implies (1,1,5) \in U \\ x=2, y=0, z=5 \longrightarrow 2+0+5=0 \implies (2,0,5) \in U \end{cases}$$

Por consiguiente, $\{(1,1,5),(2,0,5)\}$ es una base de U. $\square$

Ejercicio: Sea U el subespacio vectorial de ${\mathbb{Z}_5}^3$ generado por $\{(1,1,1)\}$ y $W = \{(x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } x+y+z=0\}$. ¿${\mathbb{Z}_5}^3 = U \oplus W$?

Sabemos que ${\mathbb{Z}_5}^3 = U \oplus W$ si y solo si ${\mathbb{Z}_5}^3 = U + W$ y $U \cap W = \{(0,0,0)\}$.

- Como W viene dado por una ecuación L.I, entonces $\dim(W) = \dim({\mathbb{Z}_5}^3) - 1 = 2$. Una base de W es $B_W = \{(1,4,0),(1,0,4)\}$ ya que es L.I y además $(1,4,0),(1,0,4) \in U$. Por tanto, $U + W = \left\langle \{(1,1,1),(1,4,0),(1,0,4)\} \right\rangle$. Pasamos a calcular $\dim(U+W)$:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 4 & 0 \\ 1 & 0 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 3 & 4 \\ 0 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 \\ 0 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix} \implies \dim(U+W) = 3$$

  Por consiguiente, ${\mathbb{Z}_5}^3 = U + W$.

- Calculamos las ecuaciones cartesianas de U imponiendo que

$$\operatorname{rang} \begin{pmatrix} 1 & x \\ 1 & y \\ 1 & z \end{pmatrix} = 1 \implies \begin{vmatrix} 1 & x \\ 1 & y \end{vmatrix} = \begin{vmatrix} 1 & x \\ 1 & z \end{vmatrix} = 0 \implies \begin{cases} 4x + y \quad = 0 \\ 4x \quad + z = 0 \end{cases}$$

  Por tanto $U = \left\{ (x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } \begin{matrix} 4x+y \quad = 0 \\ 4x \quad + z = 0 \end{matrix} \right\}$, así que

  $U \cap W = \left\{ (x,y,z) \in {\mathbb{Z}_5}^3 \text{ t. q. } \begin{matrix} x+y+z=0 \\ 4x+y \quad = 0 \\ 4x \quad + z = 0 \end{matrix} \right\}$. Comprobamos cuántas ecuaciones L.I hay:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 4 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 4 & 0 \end{pmatrix}$$

  Las tres ecuaciones por las que viene dado $U \cap W$ son L.I. Por tanto, $\dim(U \cap W) = \dim({\mathbb{Z}_5}^3) - 3 = 0$, así que $U \cap W = \{(0,0,0)\}$.

Por tanto, como se cumplen ambas condiciones, ${\mathbb{Z}_5}^3 = U \oplus W$ $\square$

Ejercicio: Sea $B = \{(1,1,1),(1,1,0),(1,0,0)\}$ una base de ${\mathbb{Z}_5}^3$ y sea U el subespacio vectorial de ${\mathbb{Z}_5}^3$ cuyas ecuaciones cartesianas de la base B son $\begin{cases} x + \quad y + z = 0 \\ x + 2y + z = 0 \end{cases}$. ¿$(0,4,4) \in U$?

Primero calculamos las coordenadas de $(0,4,4)$ respecto de la base B:

$$a(1,1,1)+b(1,1,0)+c(1,0,0)=(0,4,4) \implies \begin{cases} a+b+c=0 \\ a+b \quad\;\; =4 \\ a \quad\;\;\; =4 \end{cases} \implies (a,b,c)=(4,0,1)$$

Por tanto, $(0,4,4) \underset{B}{\equiv} (4,0,1)$.

Si las coordenadas de un vector respecto de la base B verifican las ecuaciones de U, entonces ese vector está en U. Tras sustituir (x,y,z) por $(4,0,1)$ en las ecuaciones tenemos que

$$\begin{cases} 4+ \quad 0+1 \overset{?}{=} 0 & \checkmark \\ 4+2\cdot 0+1 \overset{?}{=} 0 & \checkmark \end{cases}$$

Por tanto, como $(4,0,1)$ verifica ambas ecuaciones, entonces $(4,0,1) \in U$ $\square$

Ejercicio: Sea U el subespacio vectorial de ${\mathbb{Z}_5}^4$ generado por $\{(1,1,1,1),(0,1,1,1),(0,0,1,1)\}$ y $W=\{(x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } x+y+z+t=0\}$. Calcular el cardinal de $U \cap W$.

Primero calculamos las ecuaciones cartesianas de U. Claramente, $\{(1,1,1,1),(0,1,1,1),(0,0,1,1)\}$ ya es una base de U [27]. Tras imponer que

$$\operatorname{rang}\begin{pmatrix} 1 & 0 & 0 & x \\ 1 & 1 & 0 & y \\ 1 & 1 & 1 & z \\ 1 & 1 & 1 & t \end{pmatrix} = 3 \implies \begin{vmatrix} 1 & 0 & 0 & x \\ 1 & 1 & 0 & y \\ 1 & 1 & 1 & z \\ 1 & 1 & 1 & t \end{vmatrix} = 0$$ y calcular el siguiente determinante:

$$\begin{vmatrix} 1 & 0 & 0 & x \\ 1 & 1 & 0 & y \\ 1 & 1 & 1 & z \\ 1 & 1 & 1 & t \end{vmatrix} = (-1)^{1+1}\cdot 1\cdot \begin{vmatrix} 1 & 0 & y \\ 1 & 1 & z \\ 1 & 1 & t \end{vmatrix} + (-1)^{1+4}\cdot x\cdot \begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix} = (t+y+4y+4z)+0 = 4z+t$$

Tenemos que $U=\{(x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } 4z+t=0\}$.

Por tanto, $U \cap W = \left\{(x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{matrix} x+y+\;\; z+t=0 \\ \qquad\quad 4z+t=0 \end{matrix}\right\}$.

$\begin{vmatrix} 1 & 1 \\ 0 & 4 \end{vmatrix} = 0 \implies \operatorname{rang}\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 4 & 1 & 0 \end{pmatrix} = 2$. Por tanto las dos ecuaciones son L.I, así que $\dim(U \cap W) = \dim({\mathbb{Z}_5}^4) - 2 = 2$.

$U \cap W$ es un espacio vectorial sobre el cuerpo $\mathbb{Z}_5$ de dimensión 2. Por tanto $U \cap W$ es isomorfo a ${\mathbb{Z}_5}^2$ y en consecuencia $\#U = \#{\mathbb{Z}_5}^2 = 5^2 = 25$ $\square$

Ejercicio: Sea U el subespacio vectorial de $\mathcal{M}_{2\times 2}(\mathbb{Z}_5)$ generado por $\left\{\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}\right\}$. Calcular las ecuaciones cartesianas de U.

Ya que no se especifica la base respecto de la que calcularlas, supondremos que son las ecuaciones cartesianas respecto de la base canónica:

$B_{can} = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

Calculamos una base de U:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 1 \\ 4 & 2 & 2 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 4 & 0 & 3 \\ 0 & 4 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 4 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

[27] La matriz formada por los vectores ya está triangularizada y ninguna de las filas es nula.

Por tanto, $\left\{\begin{pmatrix}1&2\\3&4\end{pmatrix},\begin{pmatrix}0&4\\0&3\end{pmatrix}\right\}$ es una base de U. Nótese que
$\begin{pmatrix}1&2\\3&4\end{pmatrix} \underset{B_{can}}{\equiv} (1,2,3,4)$ y $\begin{pmatrix}0&4\\0&3\end{pmatrix} \underset{B_{can}}{\equiv} (0,4,0,3)$. Ahora imponemos que

$$\operatorname{rang}\begin{pmatrix}1&0&a\\2&4&b\\3&0&c\\4&3&d\end{pmatrix}=2 \implies \begin{vmatrix}1&0&a\\2&4&b\\3&0&c\end{vmatrix}=\begin{vmatrix}1&0&a\\2&4&b\\4&3&d\end{vmatrix}=0 \implies \begin{cases}3a & +4c & =0\\ & 2b & +4d=0\end{cases}$$

Por tanto, las ecuaciones cartesianas de U respecto de B son:
$\begin{cases}3a & +4c & =0\\ & 2b & +4d=0\end{cases}$ □

Ejercicio: Sea U el subespacio vectorial de $\mathbb{Z}_5[x]_3$ generado por
$\{2x^3+3x^2+x+4,\ x^3+4x^2+3x+2\}$. Calcular las ecuaciones cartesianas de U respecto de la base $B=\{x^3+x^2+x+1,\ x^2+x+1,\ x+1,\ 1\}$.

Primero calculamos una base de U:

$$\begin{pmatrix}2&3&1&4\\1&4&3&2\end{pmatrix}\sim\begin{pmatrix}2&3&1&4\\0&0&0&0\end{pmatrix} \implies \{2x^3+3x^2+x+4\} \text{ es una base de } U$$

Calculamos las coordenadas del vector $2x^3+3x^2+x+4$ respecto de la base B:

$$\begin{aligned}
& a(x^3+x^2+x+1)+b(x^2+x+1)+c(x+1)+d=2x^3+3x^2+x+4\\
\implies\quad & ax^3+(a+b)x^2+(a+b+c)x+(a+b+c+d)=2x^3+3x^2+x+4\\
\implies\quad & \left\{\begin{matrix}a & & & =2\\ a+b & & & =3\\ a+b+c & & & =1\\ a+b+c+d & & & =4\end{matrix}\right\} \implies (a,b,c,d)=(2,1,3,3)
\end{aligned}$$

Por tanto $2x^3+3x^2+x+4 \underset{B}{\equiv} (2,1,3,3)$.
Ahora imponemos que

$$\operatorname{rang}\begin{pmatrix}2&a\\1&b\\3&c\\3&d\end{pmatrix}=1 \implies \begin{vmatrix}2&a\\1&b\end{vmatrix}=\begin{vmatrix}2&a\\3&c\end{vmatrix}=\begin{vmatrix}2&a\\3&d\end{vmatrix}=0 \implies \begin{cases}4a+2b & & & =0\\ 2a & +2c & & =0\\ 2a & & +2d & =0\end{cases}$$

Por tanto las ecuaciones cartesianas de U respecto de B son $\begin{cases}2a+b & & & =0\\ a & +c & & =0\\ a & & +d & =0\end{cases}$ □

8 Diagonalización de matrices

Este tema es relativamente corto: es una introducción a los conceptos y el procedimiento necesarios para diagonalizar una matriz. Como la diagonalización de matrices es útil de manera puntual, no se suele enseñar hasta que ya se tiene un buen entendimiento sobre matrices (y otros conceptos varios del álgebra lineal). Es por esto que la diagonalización de matrices se da en un tema aparte, en vez de ser otro apartado del tema cuatro.

Sea K un cuerpo. Una matriz cuadrada $A \in \mathcal{M}_{n\times n}(K)$ es diagonal si todas las entradas de A que no están en la diagonal principal [1] son 0 [2].

Ejemplo: La matriz $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{R})$ es diagonal.

Una matriz cuadrada $A \in \mathcal{M}_{n\times n}(K)$ es diagonalizable si existen $P, D \in \mathcal{M}_{n\times n}(K)$ t. q. D es diagonal, P es regular, y $A = P \cdot D \cdot P^{-1}$.

Nota: La diagonalización de matrices es útil para el cálculo de potencias de una matriz[3], ya que si $A \in \mathcal{M}_{n\times n}(K)$ es diagonalizable y $A = PDP^{-1}$, entonces

$$A^r = \left(PDP^{-1}\right)^r = PD\cancel{P^{-1}} \cdot \cancel{PDP^{-1}} \cdot \overset{r \text{ veces}}{\cdots} \cdot \cancel{PDP^{-1}} = P \cdot D^r \cdot P^{-1}$$

además de que si $D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$ entonces $D^r = \begin{pmatrix} {d_1}^r & 0 & \dots & 0 \\ 0 & {d_2}^r & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & {d_n}^r \end{pmatrix}$.

Un elemento $\lambda \in K$ es un valor propio de la matriz $A \in \mathcal{M}_{n\times n}(K)$ si existe $(x_1, x_2, \dots, x_n) \in K^n \setminus \{(0, 0, \dots, 0)\}$ t. q. $A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. En dicho caso, se dice que $(x_1, x_2, \dots, x_n)$ es un vector propio asociado al valor propio λ.

Teorema 1. Sean $A \in \mathcal{M}_{n\times n}(K)$ y $\lambda \in K$. Entonces λ es un valor propio de A si y solo si $|A - \lambda I_n| = 0$

El teorema anterior nos dice que los valores propios de A son las raíces del polinomio $|A - \lambda I_n| \in K[\lambda]$ [4]. A dicho polinomio se le llama el polinomio característico de A, y lo denotaremos $P_A(\lambda)$. Nótese que $\text{gr}\left(P_A(\lambda)\right) = n$ [5]

Ejercicio: Calcular el polinomio característico y los valores propios de la matriz $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

---

[1] Obviamente, la diagonal principal de una matriz de $\mathcal{M}_{n\times n}(K)$ consiste en los elementos de posición $(1, 1)$, $(2, 2)$,..., (n, n).

[2] Esto no quiere decir que los elementos que no estén en la diagonal principal no sean 0; por ejemplo, la matriz cero es diagonal también

[3] No se ha introducido el concepto de potencia de una matriz, pero es fácil de ver que si A es una matriz cuadrada entonces $A^n = A \cdot A \cdot \overset{n \text{ veces}}{\cdots} \cdot A$

[4] Este es un polinomio (en la indeterminada λ) ya que es un determinante de una matriz cuyas entradas son o elementos de K o polinomios de grado 1 de $K[\lambda]$, y las sumas y multiplicaciones entre polinomios son a su vez polinomios.

[5] Esto se debe a que todas las entradas de la diagonal principal de $A - \lambda I_n$ son polinomios de grado 1 en $K[\lambda]$, así que el producto de todas las entradas (n entradas en total) da como resultado un polinomio de grado n que se suma al resto del determinante de la matriz $A - \lambda I_n$.

$$A - \lambda I_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{pmatrix}$$

$$\implies \quad P_A(\lambda) = \begin{vmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 - 4 = 1 - 2\lambda + \lambda^2 - 4 = \lambda^2 - 2\lambda - 3$$

$$\lambda^2 - 2\lambda - 3 = 0 \implies \lambda = \frac{2 \pm \sqrt{2^2 - 4 \cdot (-3) \cdot 1}}{2} = \frac{2 \pm \sqrt{16}}{2} = \begin{cases} 3 \\ \\ -1 \end{cases}$$

Por tanto los valores propios de A son 3 y -1. $\square$

Una matriz cuadrada $A \in \mathcal{M}_{n\times n}(K)$ es triangular superior si todos los elementos de A por debajo de la diagonal principal son 0, y es triangular inferior si todos los elementos de A por encima de la diagonal principal son 0.
Una matriz triangular es una matriz $A \in \mathcal{M}_{n\times n}(K)$ t. q. A es triangular superior ó triangular inferior.

Ejemplo: Sean $A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ dos matrices de $\mathcal{M}_{3\times 3}(\mathbb{R})$. Entonces A es triangular inferior y B es triangular superior. Por tanto, ambas son matrices triangulares.

Proposición 1. Sea $A \in \mathcal{M}_{n\times n}(K)$.

1. Si A es una matriz triangular entonces los valores propios de A son los valores que aparecen en su diagonal principal.
2. Los valores propios de A coinciden con los valores propios de A^t.
3. $|A| = 0$ si y solo si 0 es uno de los valores propios de A.
4. Si A es regular y λ es uno de los valores propios de A entonces λ^{-1} es uno de los valores propios de A^{-1}.

Sea $A \in \mathcal{M}_{n\times n}(K)$ y λ uno de los valores propios de A. Entonces

$$V(\lambda) \coloneqq \left\{ (x_1, x_2, \ldots, x_n) \in K^n \text{ t. q. } \left(A - \lambda I_n\right) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}$$

es un subespacio vectorial de K^n [6] al que llamaremos el subespacio vectorial propio asociado al valor propio λ.

Ejercicio: Calcular una base para cada subespacio vectorial propio de la matriz $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

El ejercicio anterior nos dice que -1 y 3 son los valores propios de A. Ahora determinamos $V(-1)$ y $V(3)$:

$$\begin{aligned} V(-1) &= \left\{ (x,y) \in \mathbb{R}^2 \text{ t. q. } \left(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\ &= \left\{ (x,y) \in \mathbb{R}^2 \text{ t. q. } \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\ &= \left\{ (x,y) \in \mathbb{R}^2 \text{ t. q. } \begin{matrix} 2x + 2y = 0 \\ 2x + 2y = 0 \end{matrix} \right\} \\ &= \left\{ (x,y) \in \mathbb{R}^2 \text{ t. q. } x + y = 0 \right\} \end{aligned}$$

[6] Donde n es el orden de la matriz A

Tenemos una ecuación L.I, así que $\dim\big(V(-1)\big) = \dim(\mathbb{R}^2) - 1 = 1$, y por tanto $B_{-1} = \big\{(1,-1)\big\}$ es una base de $V(-1)$.

$$\begin{aligned} V(3) &= \left\{(x,y) \in \mathbb{R}^2 \ \text{ t. q. } \left(\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} - \begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix}\right)\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}0\\ 0\end{pmatrix}\right\} \\ &= \left\{(x,y) \in \mathbb{R}^2 \ \text{ t. q. } \begin{pmatrix}-2 & 2\\ 2 & -2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}0\\ 0\end{pmatrix}\right\} \\ &= \left\{(x,y) \in \mathbb{R}^2 \ \text{ t. q. } \begin{matrix}-2x + 2y = 0\\ 2x - 2y = 0\end{matrix}\right\} \\ &= \big\{(x,y) \in \mathbb{R}^2 \ \text{ t. q. } \ x - y = 0\big\} \end{aligned}$$

Tenemos una ecuación L.I, así que $\dim\big(V(3)\big) = \dim(\mathbb{R}^2) - 1 = 1$, y por tanto $B_3 = \big\{(1,1)\big\}$ es una base de $V(3)$. □

Sea $A \in \mathcal{M}_{n\times n}(K)$ una matriz con polinomio característico $P_A(\lambda)$ y sea λ_0 un valor propio de A. Entonces a la multiplicidad de la raíz λ_0 de $P_A(\lambda)$ se le llama la multiplicidad algebraica del valor propio λ_0, y a $\dim\big(V(\lambda_0)\big)$ se le llama la multiplicidad geométrica del valor propio λ_0.

Ejercicio: Calcular las multiplicidades algebraicas y geométricas de los valores propios de $A = \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Los ejercicios anteriores nos dicen que el polinomio característico de A, $P_A(\lambda) = \lambda^2 - 3\lambda - 2$, tiene como raíces 3 y -1. Además, $\dim\big(V(3)\big) = \dim\big(V(-1)\big) = 1$. Por tanto:

- Claramente ambos valores propios tienen multiplicidad geométrica 1.
- Como $P_A(\lambda)$ es un polinomio de grado 2, y tenemos 2 raíces, entonces ambas raíces tienen multiplicidad 1 [7] y entonces ambos valores propios tienen multiplicidad algebraica 1.

□

Proposición 2. Si λ es un valor propio de $A \in \mathcal{M}_{n\times n}(K)$, entonces la multiplicidad geométrica de λ es siempre menor o igual que su multiplicidad algebraica.

8.1 Criterio de diagonalización

Sea $A \in \mathcal{M}_{n\times n}(K)$.
A es diagonalizable si la suma de las multiplicidades algebraicas de A es igual a n, *y además* la multiplicidad geométrica de todo valor propio coincide con su multiplicidad algebraica.

Corolario 1. Si $A \in \mathcal{M}_{n\times n}(K)$ tiene n valores propios distintos, entonces A es diagonalizable.

Corolario 2. Toda matriz simétrica con coeficientes en $\mathbb{R}$ es diagonalizable.

8.2 Método para diagonalizar una matriz

Sea $A \in \mathcal{M}_{n\times n}(K)$. Entonces el método para diagonalizar la matriz A es el siguiente:

1. Calcular $P_A(\lambda)$ y sus raíces $\lambda_1, \lambda_2, \ldots, \lambda_k$, con multiplicidades $m_1, m_2, \ldots, m_k$ respectivamente. [8]
2. Si $m_1 + m_2 + \cdots + m_k \neq n$ entonces A no es diagonalizable. **FIN**
3. Para cada $i \in \{1, 2, \ldots, k\}$, calcular $\dim\big(V(\lambda_i)\big)$ y una base de $V(\lambda_i)$.

[7] Véase la nota al pie 15 del tema 3.
[8] Claramente, $k \leq n$; además, si $k = n$ entonces A es diagonalizable.

4. Si para algún i, $\dim\big(V(\lambda_i)\big) \neq m_i$ entonces A no es diagonalizable. **FIN**
5. Si se ha llegado hasta aquí, entonces A es diagonalizable y $A = PDP^{-1}$, donde:
   - D es la matriz diagonal con m_1 veces λ_1, m_2 veces λ_2, ..., m_k veces λ_k en la diagonal.
   - La matriz P, llamada matriz de paso, tiene, vector por vector, con las coordenadas puestas por columnas, una base de $V(\lambda_1)$, una base de $V(\lambda_2)$, ..., una base de $V(\lambda_k)$.[9]

Ejercicio: Diagonalizar la matriz $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Con todo lo que hemos hecho en los ejercicios anteriores, podemos concluir que A es diagonalizable. Además, $A = PDP^{-1}$ donde

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \text{ y } D = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}$$

Ya que los valores propios de A son -1 y 3, ambos con multiplicidad algebraica y geométrica 1; y $B_{-1} = \big\{(1,-1)\big\}$ y $B_3 = \big\{(1,1)\big\}$ son bases de $V(-1)$ y $V(3)$ respectivamente. $\square$

Ejercicio: Diagonalizar la matriz $A = \begin{pmatrix} 4 & 2 & 5 \\ 6 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}_7)$.

$P_A(\lambda) = \begin{vmatrix} 4-\lambda & 2 & 5 \\ 6 & 1-\lambda & 1 \\ 0 & 0 & 2-\lambda \end{vmatrix} = 6\lambda^3 + 5\lambda + 5$. Al ser un polinomio de $\mathbb{Z}_7[\lambda]$, tras probar los valores del 0 al 6 vemos que las raíces de $P_A(\lambda)$ son 2 y 3. Ahora calculamos sus multiplicidades:

$$\begin{cases} P'_A(\lambda) = 4\lambda^2 + 5 & \Longrightarrow \quad P'_A(2) = 0, P'_A(3) \neq 0 \\ P''_A(\lambda) = \lambda & \Longrightarrow \quad P''_A(2) \neq 0 \end{cases}$$

Por tanto el valor 2 tiene multiplicidad algebraica 2 y el valor 3 tiene multiplicidad geométrica 1. Como $2 + 1 = 3$, seguimos.

$$\begin{aligned} V(2) &= \left\{ (x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \begin{pmatrix} 2 & 2 & 5 \\ 6 & 6 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \\ &= \left\{ (x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \begin{matrix} 2x + 2y + 5z = 0 \\ 6x + 6y + \ z = 0 \end{matrix} \right\} \end{aligned}$$

$$\begin{pmatrix} 2 & 2 & 5 & 0 \\ 6 & 6 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \implies V(2) = \big\{(x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \ 2x+2y+5z = 0\big\}$$

Hay una ecuación L.I $\implies \dim\big(V(2)\big) = \dim({\mathbb{Z}_7}^3) - 1 = 2$. Una base de $V(2)$ es $B_2 = \big\{(6,1,0),(1,0,1)\big\}$. [10]

[9] El orden en el que se pone cada valor propio no importa, pero debe ser el mismo en la matriz diagonal que en la matriz de paso: por ejemplo, sea una matriz 3×3 con dos valores propios λ y μ t. q. $\dim\big(V(\lambda)\big) = 1$ y $\dim\big(V(\mu)\big) = 2$. Entonces si al diagonalizar la matriz como PDP^{-1} se tiene que $D = \begin{pmatrix} \mu & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, entonces la matriz de paso debe tener como primera columna un vector de una base de $V(\mu)$, como segunda columna el otro vector de la base de $V(\mu)$ y como tercera columna el único vector de la base de $V(\lambda)$.

[10] Como es de costumbre, esta base se obtiene parametrizando el sistema de ecuaciones que genera a $V(2)$ y obteniendo dos soluciones L.I.

$$
\begin{aligned}
V(3) &= \left\{ (x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \begin{pmatrix} 1 & 2 & 5 \\ 6 & 5 & 1 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\} \\
&= \left\{ (x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \begin{array}{r} x + 2y + 5z = 0 \\ 6x + 5y + \ z = 0 \\ 6z = 0 \end{array} \right\}
\end{aligned}
$$

$$
\begin{pmatrix} 1 & 2 & 5 & 0 \\ 6 & 5 & 1 & 0 \\ 0 & 0 & 6 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 5 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 6 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 5 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \implies V(3) = \left\{ (x,y,z) \in {\mathbb{Z}_7}^3 \ \text{ t. q. } \begin{array}{r} x + 2y + 5z = 0 \\ 6z = 0 \end{array} \right\}
$$

Hay dos ecuaciones L.I $\implies \dim\big(V(2)\big) = \dim({\mathbb{Z}_7}^3) - 2 = 1$. Una base de $V(3)$ es $B_3 = \big\{(1,3,0)\big\}$.
Todas las multiplicidades algebraicas y geométricas coinciden. Por tanto, A es diagonalizable y $A = PDP^{-1}$ donde

$$
P = \begin{pmatrix} 6 & 1 & 1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix} \text{ y } D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \square
$$

Ejercicio: Diagonalizar la matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Nótese que A es triangular y por tanto su único valor propio es el 1 con multiplicidad algebraica 2, igual al orden de la matriz. Proseguimos:

$$
\begin{aligned}
V(2) &= \left\{ (x,y) \in \mathbb{R}^2 \ \text{ t. q. } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\
&= \big\{ (x,y) \in \mathbb{R}^2 \ \text{ t. q. } \ y = 0 \big\}
\end{aligned}
$$

Como hay una ecuación L.I, entonces $\dim\big(V(1)\big) = \dim(\mathbb{R}^2) - 1 = 1 \neq 2$. Por tanto, la multiplicidad geométrica del valor propio 1 no coincide con su multiplicidad algebraica y en consecuencia A no es diagonalizable. $\square$

Ejercicio: Diagonalizar la matriz $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5)$.

Nótese que A es triangular y por tanto sus valores propios son 1 y 2, ambos con multiplicidad algebraica 2. Como $2 + 2 = 4$, proseguimos:

$$V(1) = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{pmatrix} 0 & 2 & 3 & 4 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

$$= \left\{ (x,y,z,t) \in {Z_5}^4 \text{ t. q. } \begin{array}{r} 2y+3z+4t=0 \\ 2z+3t=0 \\ z+\ t=0 \\ t=0 \end{array} \right\}$$

$$\begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 3 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto $V(1) = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{array}{r} 2y+3z+4t=0 \\ 2z+3t=0 \\ 2t=0 \end{array} \right\}$. Como hay tres ecuaciones L.I entonces $\dim\big(V(1)\big) = \dim({\mathbb{Z}_5}^4) - 3 = 1 \neq 2$.
La multiplicidad geométrica del valor propio 1 no coincide con su multiplicidad algebraica. En conclusión, A no es diagonalizable. $\square$

9 Combinatoria

Este tema, a pesar de aparecer aislado del primero, puede considerarse una continuación de éste: muchos conceptos de teoría de conjuntos reaparecen en este tema como parte de los distintos principios de la combinatoria. Además este tema es un tanto distinto a los demás, tanto en cuanto a su estructura como en cuanto a ejercicios: ya que este es una de las ramas de las matemáticas con más aplicabilidad a la vida cotidiana, la mayoría de los ejercicios son problemas concretos en lugar de ejercicios matemáticos abstractos, además de que la interpretación de los problemas suele ser bastante más complicada.

La combinatoria es la técnica que se centra en saber cuántos elementos hay en un conjunto sin contarlos de uno en uno. Por ejemplo, nosotros ya sabemos que el cardinal del conjunto $A = \{1,2,3\} \times \{a,b,c,d\}$ es $3 \cdot 4 = 12$, sin necesidad de desarrollar el producto cartesiano como $A = \big\{(1,a),(1,b),(1,c),(1,d),(2,a),(2,b),(2,c),(2,d),(3,a),(3,b),(3,c),(3,d)\big\}$.

9.1 Principios básicos de la combinatoria

Principio de inclusión-exclusión de dos conjuntos

Sean A y B conjuntos. Entonces, $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.

Ejercicio: ¿Cuántos números entre 1 y 100 (ambos incluidos) son múltiplos de 2 ó de 3?

Sean A y B el conjunto de múltiplos positivos de 2 hasta el 100 y el conjunto de múltiplos positivos de 3 hasta el 100:

$$A = \Big\{2k \ \text{ t. q. } \ k \in \mathbb{Z}, 1 \leq 2k \leq 100\Big\};\ B = \Big\{3k \ \text{ t. q. } \ k \in \mathbb{Z}, 1 \leq 3k \leq 100\Big\}$$

Entonces, la solución del problema será el número de elementos que están en A ó en B; es decir, $\#(A \cup B)$.

Nótese que $A \cap B$ contiene a los múltiplos positivos de 2 y de 3; es decir, a los múltiplos positivos de 6 hasta el 100.

$$A \cap B = \Big\{6k \ \text{ t. q. } \ k \in \mathbb{Z}, 1 \leq 6k \leq 100\Big\}$$

Calculamos los cardinales de estos tres conjuntos:

- $A = \{\underbrace{2 \cdot 1}_{2}, \underbrace{2 \cdot 2}_{4}, \underbrace{2 \cdot 3}_{6}, \ldots, \underbrace{2 \cdot 50}_{100}\} \implies \#A = 50$ [1]
- $B = \{\underbrace{3 \cdot 1}_{3}, \underbrace{3 \cdot 2}_{6}, \underbrace{3 \cdot 3}_{9}, \ldots, \underbrace{3 \cdot 33}_{99}\} \implies \#B = 33$
- $A \cap B = \{\underbrace{6 \cdot 1}_{6}, \underbrace{6 \cdot 2}_{12}, \underbrace{6 \cdot 3}_{18}, \ldots, \underbrace{6 \cdot 16}_{96}\} \implies \#(A \cap B) = 16$

Por tanto, $\#(A \cup B) = \#A + \#B - \#(A \cap B) = 50 + 33 - 16 = \boxed{\mathbf{67}}$ $\square$

Principio de inclusión-exclusión general

Sean $A_1, A_2, \ldots, A_n$ conjuntos. Entonces:

[1] Para obtener el cardinal del conjunto de múltiplos de un número $n \in \mathbb{Z}$ hasta m, se puede tomar $\dfrac{m}{n}$ y redondear hacia abajo: $\dfrac{100}{2} = 50, \dfrac{100}{3} = 33.\overline{3} \simeq 33, \dfrac{100}{6} = 16.\overline{6} \simeq 16$

$$\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{i=1}^{n}(\#A_i) - \sum_{1\le i_1<i_2\le n}\big(\#(A_{i_1}\cap A_{i_2})\big)+$$
$$+\cdots+(-1)^{k+1}\sum_{1\le i_1<i_2<\cdots<i_k\le n}\big(\#(A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_k})\big)+\cdots+$$
$$+(-1)^{n+1}\#(A_1\cap A_2\cap\cdots\cap A_n)$$

Nota: [2] [3]

- Si A, B y C son tres conjuntos, entonces

$$\#(A\cup B\cup C) = \#A+\#B+\#C-\Big(\#(A\cap B)+\#(A\cap C)+\#(B\cap C)\Big)+\#(A\cap B\cap C)$$

- Si A, B, C y D son cuatro conjuntos, entonces

$$\#(A\cup B\cup C\cup D) = \#A+\#B+\#C+\#D-\Big(\#(A\cap B)+\#(A\cap C)+\#(A\cap D)+\#(B\cap C)+\#(B\cap D)+\#(C\cap D)\Big)+$$
$$+\Big(\#(A\cap B\cap C)+\#(A\cap B\cap D)+\#(A\cap C\cap D)+\#(B\cap C\cap D)\Big)-\#(A\cap B\cap C\cap D)$$

Ejercicio: ¿Cuántos números entre 1 y 100 (ambos incluidos) son múltiplos de 2, de 3 ó de 5?

Sean los conjuntos $A=\Big\{2k \text{ t. q. } k\in\mathbb{Z}, 1\le 2k\le 100\Big\}$;
$B=\Big\{3k \text{ t. q. } k\in\mathbb{Z}, 1\le 3k\le 100\Big\}$; $C=\Big\{5k \text{ t. q. } k\in\mathbb{Z}, 1\le 5k\le 100\Big\}$.
La solución del problema será el cardinal de $A\cup B\cup C$.
De las definiciones anteriores obtenemos que $A\cap B=\Big\{6k \text{ t. q. } k\in\mathbb{Z}, 1\le 6k\le 100\Big\}$,
$A\cap C=\Big\{10k \text{ t. q. } k\in\mathbb{Z}, 1\le 10k\le 100\Big\}$, $B\cap C=\Big\{15k \text{ t. q. } k\in\mathbb{Z}, 1\le 15k\le 100\Big\}$
y $A\cap B\cap C=\Big\{30k \text{ t. q. } k\in\mathbb{Z}, 1\le 30k\le 100\Big\}$. [4]
Claramente, $\#A=50$, $\#B=33$, $\#C=20$, $\#(A\cap B)=16$, $\#(A\cap C)=10$,
$\#(B\cap C)=6$ y $\#(A\cap B\cap C)=3$. Por tanto,

$$\#(A\cup B\cup C) = \#A+\#B+\#C-\Big(\#(A\cap B)+\#(A\cap C)+\#(B\cap C)\Big)+\#(A\cap B\cap C)$$
$$= 50+33+20-(16+10+6)+3=\boxed{\mathbf{74}} \quad \square$$

Principio del complementario
Si $A\subset X$, entonces $\#(X\setminus A)=\#X-\#A$ [5]

[2] La fórmula anterior es probablemente la más complicada que se ha dado en todo el curso. Afortunadamente, basta con solamente saber los casos especiales para 3 y 4 conjuntos (a continuación). Sin embargo, lo que la fórmula dice es lo siguiente: El cardinal de la unión de n conjuntos es la suma de los cardinales de los conjuntos individuales, menos la suma de los cardinales de todas las intersecciones de dos conjuntos, más la suma de los cardinales de todas las intersecciones de tres conjuntos, ..., hasta el cardinal de la intersección de todos los conjuntos (alternando de signo).

[3] La notación $\sum_{i=1}^{n}(X_i)$ significa lo mismo que $X_1+X_2+\cdots+X_n$, lo cual también se puede denotar como $\sum_{1\le i\le n}(X_i)$.

[4] Esto se consigue de manera análoga al ejercicio anterior: $B\cap C$, por ejemplo, contiene a los múltiplos positivos de 15 hasta el 100. Además, como $B\cap C=\{15\cdot 1, 15\cdot 2,\ldots,15\cdot 6\}$ entonces $\#(B\cap C)=6$.

[5] Normalmente, si el contexto implica que trabajamos sobre el conjunto X, a $X\setminus A$ se le llama el complementario de A (denotado $A^{\complement}$), de ahí el nombre.

Ejercicio: ¿Cuántos números de tres cifras no son múltiplos de 3 ni de 7?

Sea X el conjunto de números enteros de tres cifras: $X = \{100, 101, 102, \ldots, 999\}$. Es claro que $\#X = 900$.
Si definimos los conjuntos A y B como $A = \Big\{x \in X \ \text{ t. q. } \ x = 3k \ \text{ t. q. } \ k \in \mathbb{Z}\Big\}$ y $B = \Big\{x \in X \ \text{ t. q. } \ x = 7k \ \text{ t. q. } \ k \in \mathbb{Z}\Big\}$ respectivamente, podemos afirmar que $A \subseteq X$ y $B \subseteq X$ y por tanto $A \cup B \subseteq X$.
La solución del problema será el cardinal del conjunto de los elementos $x \in X$ para los que no se cumple que $x \in A$ ó que $x \in B$; es decir, el número que buscamos es $\#\big(X \setminus (A \cup B)\big)$.
Como $A \cup B \subseteq X$, tenemos por el principio del complementario que $\#\big(X \setminus (A \cup B)\big) = \#X - \#(A \cup B)$. Pasamos ahora a calcular el cardinal de $A \cup B$ usando el principio de inclusión-exclusión: [6]

- $A = \{\underbrace{3 \cdot 34}_{102}, \ldots, \underbrace{3 \cdot 333}_{999}\} \implies \#A = 300$
- $B = \{\underbrace{7 \cdot 15}_{105}, \ldots, \underbrace{7 \cdot 142}_{994}\} \implies \#B = 128$
- $A \cap B = \{x \in X \ \text{ t. q. } \ x = 21k \ \text{ t. q. } \ k \in \mathbb{Z}\} = \{\underbrace{21 \cdot 5}_{105}, \ldots, \underbrace{21 \cdot 47}_{987}\} \implies$ $\#(A \cap B) = 43$

Por tanto,
$\#(A \cup B) = 300 + 128 - 43 = 385 \implies \#\big(X \setminus (A \cup B)\big) = 900 - 385 = \boxed{\mathbf{515}}$ □

Principio del producto[7]
Sean $A_1, A_2, \ldots, A_n$ conjuntos. Entonces se cumple que

$$\#(A_1 \times A_2 \times \cdots \times A_n) = \#A_1 \cdot \#A_2 \ldots \#A_n$$

Ejercicio: Las placas de matrícula de los vehículos en cierto país constan de 4 letras (elegidas entre 25), seguidas de 3 números (elegidos entre 10). ¿Cuántas placas de matrícula distintas pueden formarse?

Sean L y N los conjuntos de letras y de números de los cuales se elige para formar matrículas, respectivamente. Claramente $\#L = 25$ y $\#N = 10$. Una matrícula de este país se puede considerar como un conjunto ordenado de 4 letras y después 3 números, es decir, una 7-tupla perteneciente al conjunto $L \times L \times L \times L \times N \times N \times N$. Entonces el número de matrículas distintas que pueden formarse es:

$$\#(L{\times}L{\times}L{\times}L{\times}N{\times}N{\times}N) = \#L{\cdot}\#L{\cdot}\#L{\cdot}\#L{\cdot}\#N{\cdot}\#N{\cdot}\#N = 25^4{\cdot}10^3 = \boxed{\mathbf{390\,625\,000}}$$ □

Sea $r \in \mathbb{Q}$. Entonces definimos y denotamos las funciones suelo y techo de q, respectivamente, como:

- $\lfloor r \rfloor \coloneqq \max\Big\{k \in \mathbb{Z} \ \text{ t. q. } \ k \leq r\Big\}$
- $\lceil r \rceil \coloneqq \min\Big\{k \in \mathbb{Z} \ \text{ t. q. } \ k \geq r\Big\}$ [8]

[6] Cuidado, el truco de la nota al pie 1 no funciona en este caso ya que el conjunto X empieza a partir del 100, así que no queda otra que ver hasta qué número se puede multiplicar sin pasarse del 1000.

[7] Esto aparece también en el tema 1, pero aparece también aquí porque también es un principio de la combinatoria.

[8] Es decir, $\lfloor r \rfloor$ es el mayor número entero menor o igual a r, y $\lceil r \rceil$ es el menor número entero mayor o igual a r. Por ejemplo, $\lfloor 3.8 \rfloor = 3$ y $\lceil 3.1 \rceil = 4$, al igual que $\lfloor 1 \rfloor = \lceil 1 \rceil = 1$.

Principio de las cajas ó Principio de Dirichlet

Si se distribuyen m objetos en n grupos, entonces existe un grupo que contiene $\left\lceil \frac{m}{n} \right\rceil$ objetos o más, y otro grupo que contiene $\left\lfloor \frac{m}{n} \right\rfloor$ objetos o menos.

Ejercicio: ¿Cuál es el mínimo número de alumnos que debe de tener una asignatura para que al menos 6 alumnos tengan la misma nota, sabiendo que las notas siempre serán números enteros entre el 0 y el 10?

Sea x el número de alumnos. Repartimos a los x alumnos en 11 grupos: el grupo de los alumnos con un 0, el grupo de los alumnos con un 1, así hasta el grupo de los alumnos con un 10. Por el principio de las cajas, sabemos que va a haber un grupo con $\left\lceil \frac{x}{11} \right\rceil$ alumnos o más, es decir, que al menos $\left\lceil \frac{x}{11} \right\rceil$ alumnos sacarán la misma nota. Para que se cumpla lo que nos pida el enunciado necesitamos que $\left\lceil \frac{x}{11} \right\rceil \geq 6$, lo cual se cumple si $x \geq 56$. [9]

Por tanto, el número mínimo de alumnos que deben cursar la asignatura es 56. □

9.2 Variaciones

Variaciones simples

Diremos que una k-tupla $(a_1, a_2, \ldots, a_k)$ es simple si $\#\{a_1, a_2, \ldots, a_k\} = k$ [10]

Sea A un conjunto de cardinal m, y $k \in \mathbb{N}$. El número de k-tuplas simples que se pueden formar con los elementos de A es:

- Si $m < k$, se pueden formar 0 k-tuplas simples.
- Si $m \geq k$, entonces definimos $\mathrm{V}_{m,k}$ como: [11]

$$\mathrm{V}_{m,k} \coloneqq \frac{m!}{(m-k)!}$$

$\mathrm{V}_{m,k}$ también indica el número de aplicaciones inyectivas $f : K \longrightarrow M$ t. q. $\#K = k$ y $\#M = m$.

Ejercicio: ¿Cuántos números de tres cifras distintas podemos formar con los dígitos 5, 6, 7, 8 y 9?

Un número de tres cifras distintas que usa los dígitos del 5 al 9 puede interpretarse como una terna simple $(m, n, \tilde{n}) \in \{5, 6, 7, 8, 9\}^3$. Entonces, la solución del problema es el número de ternas simples que se pueden formar con los elementos de $\{5, 6, 7, 8, 9\}$. como el conjunto tiene 5 elementos, tenemos que:

$$\mathrm{V}_{5,3} = \frac{5!}{2!} = \frac{120}{2} = \boxed{\mathbf{60}} \quad \square$$

Otra forma de hacer el ejercicio:

Para formular un número de tres cifras como pide el enunciado, rellenamos tres casillas. A la primera casilla le podemos dar cualquiera de los 5 elementos de $\{5, 6, 7, 8, 9\}$. Sin embargo, como las cifras deben ser distintas, a la segunda solo le podemos dar uno de 4 valores, y similarmente la última casilla recibe uno de 3 valores distintos. Entonces el número total de posibilidades para rellenar las tres casillas es $5 \cdot 4 \cdot 3 = \boxed{\mathbf{60}}$ □

[9] Ya que $\left\lceil \frac{56}{11} \right\rceil = \lceil 5.0909\ldots \rceil = 6$, pero $\left\lceil \frac{55}{11} \right\rceil = \lceil 5 \rceil = 5$.

[10] Es decir, si ninguno de los componentes de la k-tupla se repite. Por ejemplo, la 4-tupla $(1, 2, 3, 4)$ es simple, pero la 5-tupla (a, b, c, a, d) no es simple.

[11] La expresión $n!$ denota el factorial de un número natural n: Si $n \in \mathbb{N}$, entonces $n! \coloneqq n(n-1)(n-2)\ldots 3 \cdot 2 \cdot 1$. Además se define 0! como 1. Por ejemplo, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. Nótese que para cualquier $0 \leq k \leq n \in \mathbb{N}$, se cumple que $n! = n \cdot (n-1) \cdot (n-2) \ldots k!$

Ejercicio: ¿De cuántas formas se pueden sentar 4 personas en un microbús de 15 plazas?

Sea P el conjunto de las 4 personas y A el conjunto de los 15 asientos. Entonces una manera de sentar a las 4 personas en los asientos del microbús es una aplicación inyectiva $f : P \longrightarrow A$[12]. Por tanto hay tantas maneras como aplicaciones inyectivas de P en A; es decir, la solución del ejercicio es

$$\mathrm{V}_{15,4} = \frac{15!}{11!} = \frac{15 \cdot 14 \cdot 13 \cdot 12 \cancel{\cdot 11 \cdot 10 \ldots}}{\cancel{11 \cdot 10 \ldots}} = 15 \cdot 14 \cdot 13 \cdot 12 = \boxed{\mathbf{32\,760}} \quad \square$$

Otra forma de hacer el ejercicio:

Para determinar una manera de sentar a las cuatro personas, a cada una le asignamos una "casilla" con su asiento. Entonces a la primera "casilla" le podemos dar cualquiera de los 15 asientos, a la segunda le podemos dar 14 asientos, a la tercera 13 y a la cuarta 12. Entonces el número total de posibilidades es
$15 \cdot 14 \cdot 13 \cdot 12 = \boxed{\mathbf{32\,760}} \quad \square$

Ejercicio: ¿Cuántos números de tres cifras distintas podemos formar con los dígitos 0, 1, 2, 3 y 4?

En principio se podrían formar la misma cantidad de números que con los dígitos de 5 a 9 (es decir, 60). Sin embargo, un número de tres cifras que empieza con 0 no es realmente de 3 cifras. Por tanto, tenemos que descontar todos los números de tres cifras distintas que empiezan por 0, y por tanto sus otras dos cifras se eligen de 4 valores, dando lugar a $\mathrm{V}_{4,2}$ números de tres cifras distintas que empiezan por 0:

$$\mathrm{V}_{5,3} - \mathrm{V}_{4,2} = 60 - \frac{4!}{2!} = 60 - \frac{24}{2} = \boxed{\mathbf{48}} \quad \square$$

Otra forma de hacer el ejercicio:

De nuevo rellenamos tres casillas para hacer un número de tres cifras. Sin embargo, a la primera no le podemos dar el valor 0, así que elegimos entre 4 dígitos. Como en la segunda no tenemos la misma restricción de no poner cero, podemos volver a poner uno de entre 4 valores[13]. Finalmente en la tercera podemos poner cualquiera de los tres dígitos restantes. Por tanto, el número total de posibilidades es $4 \cdot 4 \cdot 3 = \boxed{\mathbf{48}} \quad \square$

Variaciones con repetición

Sea A un conjunto de cardinal m y $k \in \mathbb{N}$. El número de k-tuplas que se pueden formar con los elementos de A es:

$$\mathrm{V}^{\mathrm{R}}_{m,k} \coloneqq m^k$$

$\mathrm{V}^{\mathrm{R}}_{m,k}$ también indica el número de aplicaciones $f : K \longrightarrow M$ t. q. $\#K = k$ y $\#M = m$ [14].

Ejercicio: ¿Cuántos números de tres cifras podemos construir con los dígitos 1 y 2?

Si interpretamos un número de tres cifras como una terna $(m, n, \tilde{n}) \in \{1, 2\}^3$, entonces es claro que la solución del ejercicio es

$$\mathrm{V}^{\mathrm{R}}_{2,3} = 2^3 = \boxed{\mathbf{8}} \quad \square$$

Otra forma de hacer el ejercicio:

Si rellenamos tres casillas para formar el número de tres cifras, es claro que a todas las casillas podemos darle uno de los dos valores, ya que no tenemos la condición de que no se repitan los dígitos. Entonces el número de posibilidades es $2 \cdot 2 \cdot 2 = \boxed{\mathbf{8}} \quad \square$

[12] Ya que a cada persona se le asigna un asiento distinto, sin repetir (asumimos que para la resolución del ejercicio varias personas no pueden sentarse en el mismo asiento).

[13] Es decir, el cero más los otros tres valores que la primera casilla no escogió

[14] Se incluyen las aplicaciones inyectivas y no inyectivas.

Ejercicio: ¿Cuántos números de tres cifras podemos construir con los dígitos 0, 1 y 2?

Sabemos que el número de ternas $(m, n, \tilde{n}) \in \{0, 1, 2\}^3$ que se pueden formar es $\mathrm{V}^{\mathrm{R}}_{3,3} = 3^3 = 27$. Sin embargo, las ternas cuyo primer elemento es el cero no cuentan como números de tres cifras. Por tanto descontamos el número de ternas que tienen cero como primer elemento (de las cuales hay $\mathrm{V}^{\mathrm{R}}_{3,2}$ ya que se pueden elegir libremente los otros dos elementos). La solución del problema es

$$\mathrm{V}^{\mathrm{R}}_{3,3} - \mathrm{V}^{\mathrm{R}}_{3,2} = 3^3 - 3^2 = 27 - 9 = \boxed{\mathbf{18}} \quad \square$$

Otra forma de hacer el ejercicio:

Rellenamos tres casillas de nuevo. La primera no puede tener el dígito 0, por lo que elegimos entre dos valores. La segunda y la tercera no tienen esa restricción así que se les pueden dar tres valores. Por tanto el número total de posibilidades es $2 \cdot 3 \cdot 3 = \boxed{\mathbf{18}} \quad \square$

Ejercicio: ¿Cuántos polinomios de grado menor o igual a 2 tiene $\mathbb{Z}_5[x]$?

Un polinomio de $\mathbb{Z}_5[x]$ con grado menor o igual que dos es de la forma $ax^2 + bx + c$ t. q. $a, b, c \in \mathbb{Z}_5$. Entonces, un polinomio se puede interpretar como una terna $(a, b, c) \in {\mathbb{Z}_5}^3$ [15]. Por tanto, el número de polinomios que se pueden formar es $\mathrm{V}^{\mathrm{R}}_{5,3} = 5^3 = \boxed{\mathbf{125}} \quad \square$

Otra forma de hacer el ejercicio:

Rellenamos tres casillas para los tres coeficientes de un polinomio de grado menor o igual que dos. A las tres casillas le podemos dar uno de 5 valores, por lo que el número de posibilidades es $5 \cdot 5 \cdot 5 = \boxed{\mathbf{125}} \quad \square$

Ejercicio: ¿Cuántos polinomios de grado dos tiene $\mathbb{Z}_5[x]$?

Un polinomio de $\mathbb{Z}_5[x]$ de grado dos es de la forma $ax^2 + bx + c$ t. q. $a, b, c \in \mathbb{Z}_5, a \neq 0$. Si lo interpretamos como una terna $(a, b, c) \in {\mathbb{Z}_5}^3$, tenemos que asegurarnos de que $a \neq 0$, así que descontamos todas las ternas cuyo primer elemento es cero. Como el número de ternas en general de ${\mathbb{Z}_5}^3$ es $\mathrm{V}^{\mathrm{R}}_{5,3}$ y el número de ternas que empiezan por cero es $\mathrm{V}^{\mathrm{R}}_{5,2}$, entonces la solución del problema es $\mathrm{V}^{\mathrm{R}}_{5,3} - \mathrm{V}^{\mathrm{R}}_{5,2} = 125 - 25 = \boxed{\mathbf{100}} \quad \square$

Otra forma de hacer el ejercicio:

Rellenamos tres casillas para los tres coeficientes de un polinomio de grado dos. La primera casilla no puede valer 0, así que escogemos entre 4 valores. Las otras dos pueden tener cualquiera de los cinco valores así que el número total de posibilidades es $4 \cdot 5 \cdot 5 = \boxed{\mathbf{100}} \quad \square$

Ejercicio: ¿Cuántos polinomios mónicos de grado menor o igual a 2 tiene $\mathbb{Z}_5[x]$?

Para ver cuántos polinomios mónicos de grado menor o igual a 2 hay en $\mathbb{Z}_5[x]$, vemos cuántos hay de grado 2, de grado 1 y de grado 0:

- Un polinomio mónico de grado 2 en $\mathbb{Z}_5[x]$ es de la forma $x^2 + ax + b$ t. q. $a, b \in \mathbb{Z}_5$. Como tanto a como b pueden tener 5 valores, entonces hay $5 \cdot 5 = 25$ polinomios.
- Similarmente, un polinomio mónico de grado uno en $\mathbb{Z}_5[x]$ es de la forma $x + a$ t. q. $a \in \{0, 1, 2, 3, 4\}$. Entonces hay 5 polinomios.
- El único polinomio mónico de grado cero en $\mathbb{Z}_5[x]$ es 1.

Por tanto, la solución del problema es $25 + 5 + 1 = \boxed{\mathbf{31}} \quad \square$

[15] Se puede resolver el ejercicio directamente aquí, ya que como $\#{\mathbb{Z}_5}^3 = 125$ entonces se pueden formar 125 ternas distintas, es decir, 125 polinomios distintos

9.3 Permutaciones

Permutaciones simples

Sea A un conjunto de cardinal m. El número de m-tuplas simples que se pueden formar con los elementos de A [16] es:

$$\mathrm{P}_m \coloneqq m!$$

Esto es un caso particular de las vaariaciones simples: $\mathrm{V}_{m,m} = \dfrac{m!}{(m-m)!} = \dfrac{m!}{0!} = m! = \mathrm{P}_m$.

P_m también indica el número de aplicaciones biyectivas $f : M \longrightarrow M'$ t. q. $\#M = \#M' = m$.

Ejercicio: ¿De cuántas maneras podemos ordenar 5 libros en una estantería?

Sea $L = \{l_1, l_2, l_3, l_4, l_5\}$ el conjunto de los 5 libros. Entonces una manera de ordenar los 5 libros es una 5-tupla simple de L^5. Por tanto existen $\mathrm{P}_5 = 5! = \boxed{\mathbf{120}}$ maneras distintas de ordenar los libros. $\square$.

Otra forma de hacer el ejercicio:

Colocamos los 5 libros en 5 posiciones distintas. En la primera posición puedo colocar cualquiera de los 5 libros, en la segunda uno de los cuatro restantes, en la tercera uno de los tres que quedan, en la cuarta uno de los dos que quedan, y en la última posición solamente queda un libro. Entonces el número de posibilidades es $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = \boxed{\mathbf{120}}$ $\square$

Permutaciones con repetición

Sea A un conjunto de cardinal r y $\alpha_1, \alpha_2, \ldots, \alpha_r, m \in \mathbb{N} \setminus \{0\}$ t. q. $\alpha_1 + \alpha_2 + \cdots + \alpha_r = m$. El número de m-tuplas que se pueden formar con los elementos de A tales que una coordenada se repita α_1 veces, otra se repita α_2 veces, ..., y otra coordenada se repita α_r veces es:

$$\mathrm{P}_m^{\alpha_1,\alpha_2,\ldots,\alpha_r} \coloneqq \frac{m!}{\alpha_1! \cdot \alpha_2! \ldots \alpha_r!}$$

Ejercicio: ¿Cuántos números de 16 cifras se pueden formar con 3 unos, 5 doses y 8 treses?

Interpretando un número de 16 cifras como una 16-tupla, tenemos que calcular el número de 16-tuplas de $\{1, 2, 3\}^{16}$ en las que el 1 se repita tres veces, el 2 se repita 5 veces y el 3 se repita 8 veces:

$$\mathrm{P}_{16}^{3,5,8} = \frac{16!}{3! \cdot 5! \cdot 8!} = \frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot \cancel{8!}}{6 \cdot 120 \cdot \cancel{8!}} = \boxed{\mathbf{720\,720}} \quad \square$$

Ejercicio: ¿Cuántos números de 16 cifras se pueden formar con 3 unos, 5 doses, 6 treses y 2 ceros?

En principio sería, de manera igual al ejercicio anterior, $\mathrm{P}_{16}^{3,5,6,2}$. Sin embargo, esto incluye a los números que empiezan por cero (los cuales no son de 16 cifras). Por tanto, debemos descontar todos los números que empiezan por 0 seguidos de las otras 15 cifras (es decir, 3 unos, 5 doses, 6 treses y otro cero) en cualquier orden. Por tanto la solución del ejercicio es: [17]

$$\mathrm{P}_{16}^{3,5,6,2} - \mathrm{P}_{15}^{3,5,6,1} = \frac{16!}{3! \cdot 5! \cdot 6! \cdot 2!} - \frac{15!}{3! \cdot 5! \cdot 6! \cdot 1!} = \boxed{\mathbf{17\,657\,640}} \quad \square$$

Ejercicio: ¿De cuántas maneras diferentes se pueden ordenar las letras de la palabra "CACATÚA"?

[16] Es decir, el número de maneras de ordenar los m elementos de A

[17] Nótese que no es necesario poner el 1 del final, ya que la única parte que afecta es dividir por $1! = 1$ el resultado.

Una ordenación de la palabra "CACATÚA" es una 7-tupla del conjunto $\{\mathrm{C}, \mathrm{A}, \mathrm{T}, \acute{\mathrm{U}}\}^7$ donde la C se repite 2 veces, la A se repite 3, y las otras dos letras se repiten una vez. Entonces el número total de ordenaciones es

$$\mathrm{P}_7^{2,3,1,1} = \mathrm{P}_7^{2,3} = \frac{7!}{2! \cdot 3!} = \boxed{\mathbf{420}} \quad \square$$

9.4 Combinaciones

Combinaciones simples

Sea A un conjunto de cardinal $m \geq k \in \mathbb{N}$. El número de subconjuntos de A con cardinal k es:

$$\mathrm{C}_{m,k} = \binom{m}{k} \coloneqq \frac{m!}{k! \cdot (m-k)!}$$

Ejercicio: Se extraen 5 cartas de una baraja de 40. ¿Cuántas jugadas distintas pueden obtenerse?

Una jugada de 5 cartas se puede interpretar como un subconjunto con cardinal 5 del conjunto de las 40 cartas. Por tanto, el número posible de jugadas es:

$$\binom{40}{5} = \frac{40!}{5! \cdot 35!} = \frac{40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot \cancel{35!}}{120 \cdot \cancel{35!}} = \boxed{\mathbf{658\,008}} \quad \square$$

Ejercicio: Cierto club deportivo está formado por 15 mujeres y 12 hombres. Sabiendo que un comité está formado por cuatro personas, ¿cuántos comités con exactamente dos mujeres puede formar este club?

Para formar un comité, tomamos dos espacios: al primero le asignamos un subconjunto de dos mujeres de las 15 del club, y al segundo le asignamos un subconjunto de $4 - 2 = 2$ hombres de los 12 del club. Como en el primer espacio podemos elegir entre $\binom{15}{2} = 105$ subconjuntos y en el segundo podemos elegir entre $\binom{12}{2} = 66$ subconjuntos [18], entonces el número de posibilidades es $105 \cdot 66 = \boxed{\mathbf{6\,930}} \quad \square$

Ejercicio: ¿De cuántas formas se pueden acertar exactamente 9 resultados en una quiniela de 14? [19]

Tomamos 6 casillas. A la primera le asignamos el subconjunto de los 9 resultados que acertamos. Por tanto, hay $\binom{14}{9}$ posibilidades para rellenar la primera casilla. En las otras $14 - 9 = 5$ casillas, ponemos la manera en la que fallamos los resultados restantes. Cada resultado se puede fallar de dos maneras así que hay 2 posibilidades para cada casilla. Entonces el número total de posibilidades es

$$\binom{14}{9} \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2002 \cdot 2^5 = \boxed{\mathbf{64\,064}} \quad \square$$

[18] $\binom{m}{k}$ también se puede interpretar como el número de maneras de las cuales se pueden elegir k elementos de un grupo de m elementos.

[19] Para este ejercicio es necesario saber que una quiniela es un juego de azar en el que le presenta un número de partidos al jugador y éste debe adivinar el resultado de cada uno: si gana un equipo, gana el otro o empatan los dos. Por tanto se puede fallar un resultado de dos formas distintas.

Combinaciones con repetición

Supongamos que disponemos de un número ilimitado de bolas de m colores distintos, y tomamos k bolas para ponerlas en una caja. Entonces el número de cajas distintas de k bolas que se pueden formar es:

$$\mathrm{C}^R_{m,k} \coloneqq \binom{m+k-1}{k} = \frac{(m+k-1)!}{k!\cdot(m-k)!}$$

$\mathrm{C}^R_{m,k}$ también indica el cardinal del conjunto $\big\{(a_1,a_2,\dots,a_m)\in\mathbb{N}^m \ \text{ t. q. } \ a_1+a_2+\cdots+a_m=k\big\}$.

Ejercicio: En una heladería se sirven helados de 20 sabores diferentes. ¿Cuántas compras distintas de 12 helados se pueden hacer?

Una compra de 12 helados de entre 20 sabores puede interpretarse como tomar una caja de 12 bolas teniendo bolas de 20 colores. Por tanto el número de compras que se puede hacer es

$$\mathrm{C}^R_{20,12} = \binom{31}{12} = \frac{31!}{12!\cdot 19!} = \frac{31\cdot 30\cdot 29\dots 20\cdot \cancel{19!}}{12!\cdot \cancel{19!}} = \boxed{\mathbf{4\,552\,275}} \quad \square$$

Ejercicio: Se lanzan tres dados simultáneamente. ¿Cuántas jugadas distintas se pueden obtener?

Lanzar tres dados[20] se puede interpretar como tomar una caja de 3 bolas teniendo bolas de 6 colores distintos. Entonces el número de jugadas posibles es:

$$\mathrm{C}^R_{6,3} = \binom{8}{3} = \boxed{\mathbf{56}} \quad \square$$

Ejercicio: ¿Cuántas soluciones enteras tiene la ecuación $x+y+z+t=24$ tales que $x,y,z,t\geq 2$?

Nótese que si $(x,y,z,t)\in\{2,3,4,\dots\}^4$ cumple que

$$x+y+z+t=24 \tag{1}$$

entonces también cumple que

$$(x-2)+(y-2)+(z-2)+(t-2)=16 \tag{2}$$

y como $(x,y,z,t)\in\{2,3,\dots\}^4$, entonces $(x-2,y-2,z-2,t-2)\in\{0,1,2,\dots\}=\mathbb{N}^4$. Por tanto, el número de elementos de $\{2,3,4,\dots\}^4$ que cumplen (1) es el mismo número de elementos de $\mathbb{N}^4$ que cumplen (2). Entonces la solución del ejercicio es

$$\#\big\{(x,y,z,t)\in\mathbb{N}^4 \ \text{ t. q. } \ x+y+z+t=16\big\} = \mathrm{C}^R_{4,16} = \binom{19}{16} = \boxed{\mathbf{969}} \quad \square$$

Ejercicio: ¿Cuántos números de tres cifras con los dígitos del 1 al 7 existen tales que la suma de sus dígitos sea 10?

Tomando un número de tres cifras con los dígitos del 1 al 7 como una terna $(a,b,c)\in\{1,2,3,4,5,6,7\}^3$ y haciendo como en el ejercicio anterior, entonces tenemos que la solución del problema es

$$\begin{aligned} & \#\big\{(a,b,c)\in\{1,2,3,4,5,6,7\}^3 \ \text{ t. q. } \ a+b+c=10\big\} \\ = \ & \#\big\{(a,b,c)\in\{1,2,3,4,5,6,7\}^3 \ \text{ t. q. } \ (a-1)+(b-1)+(c-1)=7\big\} \\ = \ & \#\big\{(a,b,c)\in\{0,1,2,3,4,5,6\}^3 \ \text{ t. q. } \ a+b+c=7\big\} \end{aligned}$$

[20] Asumimos que los dados tienen seis caras.

Nótese[21] que

$$\big\{(a,b,c)\in\mathbb{N}^3 \ \text{ t. q. } \ a{+}b{+}c=7\big\}=\big\{(a,b,c)\in\{0,1,\dots,6\}^3 \ \text{ t. q. } \ a{+}b{+}c=7\big\}\cup\big\{(7,0,0),(0,7,0),(0,0,7)\big\}$$

Llamemos X, A y B a los conjuntos de la igualdad anterior respectivamente, de modo que $X=A\cup B$. Entonces podemos ver que A y B son subconjuntos de X, y además $A=X\setminus B$. Entonces, por el principio del complementario, tenemos que $\#A=\#(X\setminus B)=\#X-\#B$, y por tanto

$$\#\big\{(a,b,c)\in\{0,1,\dots,6\}^3 \ \text{ t. q. } \ a{+}b{+}c=7\big\}=\#\big\{(a,b,c)\in\mathbb{N}^3 \ \text{ t. q. } \ a{+}b{+}c=7\big\}-\#\big\{(7,0,0),(0,7,0),(0,0,7)\big\}$$

Por lo que la solución del problema es

$$\#\big\{(a,b,c)\in\mathbb{N}^3 \ \text{ t. q. } \ a+b+c=7\big\}-3=\mathrm{C}^R_{3,7}-3=36-3=\boxed{\mathbf{33}} \quad \square$$

[21] Estas transformaciones las hacemos con el fin de tener una m-tupla de $\mathbb{N}^m$ que cumpla la condición

10 Apéndice

Este tema no trata sobre una sola materia en particular, es una colección de secciones menos extensas relacionadas con el resto de temas (principalmente los temas 1, 2 y 3).
(Nota: este curso no hemos podido dar el tema entero en clase, por lo que algunas de las explicaciones pueden estar incompletas.)

10.1 Sistemas de numeración

Sea b un número entero mayor o igual a 2. Entonces todo $n \in \mathbb{N} \setminus \{0\}$ se puede poner de forma única como

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0$$

donde $k \in \mathbb{N}$, $a_0, a_1, \ldots, a_k \in \mathbb{Z}_b$ [1] y $a_k \neq 0$.
A la $(k+1)$-tupla $(a_k, a_{k-1}, \ldots, a_1, a_0)$ la llamaremos la expresión del número n en base b. La expresión del número cero en cualquier base se define como (0). [2]
Ejemplo: $(2, 2, 1)$ es la expresión en base 3 del número 25, ya que

$$(2,2,1)_3 = 2 \cdot 3^2 + 2 \cdot 3^1 + 1 = 2 \cdot 9 + 2 \cdot 3 + 1 = 18 + 6 + 1 = 25$$

Ejercicio: ¿Qué número tiene la expresión $(1, 0, 1, 0, 1, 0)$ en base 2?

$$(101010)_2 \ ^3 = 1 \cdot 2^5 + 0 + 1 \cdot 2^3 + 0 + 1 \cdot 2^1 = 32 + 8 + 2 = \boxed{\mathbf{42}} \quad \square$$

Método para pasar de base 10 a base b
Si tenemos un número $n \in \mathbb{N}$, el método para hallar su expresión en base b es el siguiente:

1. Dividir n entre b. El resto será el último dígito de la expresión, y nos quedamos con el cociente, al que llamamos $n_1 = n$ div b.
2. Dividir n_1 entre b. El resto es el penúltimo dígito de la expresión, y nos quedamos con el cociente $n_2 = n_1$ div b.
3. Seguir repitiendo este paso hasta que $n_k < b$. Entonces n_k es el primer dígito de la expresión.

Ejemplos:

- Expresar el número 1538 en base 7:

$$\left\{ \begin{array}{l} 1538 \text{ div } 7 = 219 \\ 1538 \text{ mod } 7 = 5 \end{array} \right\} \underset{(\ldots,5)}{\Longrightarrow} \left\{ \begin{array}{l} 219 \text{ div } 7 = 31 \\ 219 \text{ mod } 7 = 2 \end{array} \right\} \underset{(\ldots,2,5)}{\Longrightarrow} \left\{ \begin{array}{l} 31 \text{ div } 7 = 4 < 7 \\ 31 \text{ mod } 7 = 3 \end{array} \right\} \Longrightarrow 1538 = (4325)_7 \quad \square$$

- Expresar el número 2315 en base 12:

$$\left\{ \begin{array}{l} 2315 \text{ div } 12 = 192 \\ 2315 \text{ mod } 12 = 11 \end{array} \right\} \underset{(\ldots,11)}{\Longrightarrow} \left\{ \begin{array}{l} 192 \text{ div } 12 = 16 \\ 192 \quad \text{mod } 12 = 0 \end{array} \right\} \underset{(\ldots,0,11)}{\Longrightarrow} \left\{ \begin{array}{l} 16 \text{ div } 12 = 1 \\ 16 \quad \text{mod } 12 = 4 \end{array} \right\} \Longrightarrow 2315 = (1,4,0,11)_{12} \quad \square$$

[1] Es decir, a_0, a_1, ... y a_k (también llamados dígitos) son todos números enteros entre 0 y $b-1$.
[2] A lo largo de esta sección, para indicar que una $(k+1)$-tupla $(a_k, a_{k-1}, \ldots, a_1, a_0)$ es la expresión en base b de un número, se denotará $n = (a_k, a_{k-1}, \ldots, a_1, a_0)_b$
[3] Al escribir la expresión en base $b \leq 10$ de un número, a veces se omiten las comas, ya que un dígito en el sistema de numeración que usamos (es decir, base 10) corresponde con ese mismo dígito en base b y por tanto se puede denotar como un número normal (siempre indicando la base). Sin embargo si $b > 10$ entonces es necesario usar comas para delimitar los dígitos ya que tenemos más dígitos posibles que en base 10. Existe la alternativa de usar las letras A, B, C,... para los dígitos 10, 11, 12,... (por ejemplo, el número $(12, 4, 16, 15, 8)_{17}$ se expresaría de la forma $(\text{C4GF8})_{17}$) pero no funciona para bases grandes como 40.

Método para pasar de base b a base b'

Para pasar de una expresión de un número n en base b a su expresión en base b' (obviamente $b \neq b'$), calculamos primero su expresión en base 10 y luego hallamos la expresión en base b'.

Ejercicio: La expresión en base 3 de un número es 12101. Calcular su expresión en base 5.

Tenemos que el número es $1 \cdot 3^4 + 2 \cdot 3^3 + 1 \cdot 3^2 + 0 + 1 = 81 + 54 + 9 + 1 = 145$.
Ahora calculamos su expresión en base 5.

$$\left\{ \begin{array}{l} 145 \text{ div } 5 = 29 \\ 145 \text{ mod } 5 = 0 \end{array} \right\} \underset{(\ldots,0)}{\Longrightarrow} \left\{ \begin{array}{l} 29 \text{ div } 5 = 5 \\ 29 \text{ mod } 5 = 4 \end{array} \right\} \underset{(\ldots,4,0)}{\Longrightarrow} \left\{ \begin{array}{l} 5 \text{ div } 5 = 1 \\ 5 \text{ mod } 5 = 0 \end{array} \right\}$$

Por tanto, $(12101)_3 = (1040)_5$ $\square$

Método para pasar de base b a base b^r

Si $r \in \mathbb{N}$, entonces para pasar la expresión de un número de base b a base b^r no es necesario convertir la expresión primero a base 10 y luego a base b^r. Un dígito en base b^r corresponderá a r dígitos en base b [4]. Por tanto, para convertir la expresión de un número en base b a su expresión en base b^r, agrupamos sus dígitos de r en r desde la derecha y cada grupo lo pasamos a base 10 (ya que es un solo dígito así que se representa normalmente).

Ejercicio: Calcular la expresión en base 8 del número $(10010101110110001010101)_2$.

$8 = 2^3$, por lo que para hallar la expresión en base 8 agrupamos los dígitos de 3 en 3:

$$(10010101110110001010101)_2 \rightarrow \underbrace{(10)}_{2}, \underbrace{(010)}_{2}, \underbrace{(101)}_{5}, \underbrace{(110)}_{6}, \underbrace{(110)}_{6}, \underbrace{(001)}_{1}, \underbrace{(010)}_{2}, \underbrace{(101)}_{5}$$

Y cada uno de esos grupos es un dígito distinto en su lugar correspondiente. Por tanto,

$$(10010101110110001010101)_2 = (22566125)_8 \quad \square$$

Ejercicio: Calcular la expresión en base 3 del número $(874316)_9$. [5]

Como $3^2 = 9$, entonces cada dígito de la expresión que nos dan corresponde a dos dígitos en base 3. Convertimos cada dígito individual a base 3 [6]:

$$\left. \begin{array}{l} 8 = (22)_3 \\ 7 = (21)_3 \\ 4 = (11)_3 \\ 3 = (10)_3 \\ 1 = (01)_3 \\ 6 = (20)_3 \end{array} \right\} \Longrightarrow (874316)_9 = (222111100120)_3 \quad \square$$

Suma y producto en base b

Si nos dan la expresión de dos números en base b y nos piden su suma o su producto, entonces una forma de hacerlo es convertir ambos números a base 10, operar con ellos normalmente y pasar el resultado a base b, pero también se puede realizar el cálculo directamente en base b, teniendo en cuenta que sólo tenemos los dígitos entre 0 y $b-1$ y por tanto al pasar de $b-1$ tenemos que "llevar" cifras.

[4] Por ejemplo, un dígito en base 16 (hexadecimal) corresponde a 4 dígitos en base 2 (binaria) ya que $16 = 2^4$: el número $(8,6)_{16}$ es el mismo número que $(1,0,0,0,\ 0,1,1,0)_2$.

[5] Al igual que se puede pasar de base b a base b^r de modo especial, se puede pasar de base b^r a base b, teniendo en cuenta que un dígito en base b^r corresponde a r dígitos en base b.

[6] Nótese que esto es menos complicado ya que un solo dígito es relativamente pequeño así que los cambios de base se pueden hacer de forma casi directa

Ejemplos:

- Calcular $(43243 + 3413)_5$

$$\begin{array}{rr} & 4\,3\,2\,4\,3 \\ + & 0\,3\,4\,1\,3 \\ \hline & 1\,0\,2\,2\,1\,1 \end{array}$$

Empezamos desde la derecha: $(3+3)_5 = (11)_5$ [7], así que nos "llevamos" un 1 y el último dígito de la suma es 1. $(4+1+1)_5 = (11)_5$, por lo que nos volvemos a "llevar" 1 y ponemos otro dígito 1. En el tercer dígito desde la derecha tenemos que $(2+4+1)_5 = (12)_5$. De nuevo nos "llevamos" 1 y el tercer último dígito es un 2. $(3+3+1)_5 = (12_5)$, y entonces nos llevamos un 1 por última vez y ponemos otro 2 en el resultado. Finalmente, en el primer dígito tenemos que $(4+0+1)_5 = (10)_5$. Como no quedan más dígitos a la izquierda, entonces no nos llevamos nada y ponemos el $(10)_5$ al principio del resultado.
En conclusión, $(43243 + 3413)_5 = (102211)_5$ $\square$

- Calcular $(2341 \times 34)_5$

Convertimos ambos factores a base 10: [8]

$$\left.\begin{array}{r} (2341)_5 = 2\cdot 5^3 + 3\cdot 5^2 + 4\cdot 5 + 1 = 346 \\ (34)_5 = 3\cdot 5 + 4 = 19 \end{array}\right\} \Longrightarrow (2341\times 34)_5 = 346\times 19 = 6574$$

Y ahora hallamos la expresión en base 5 del número 6574:

$$\left\{\begin{array}{l} 6574 \text{ div } 5 = 1314 \\ 6574 \bmod 5 = 4 \end{array}\right\} \underset{(\ldots,4)}{\Longrightarrow} \left\{\begin{array}{l} 1314 \text{ div } 5 = 262 \\ 1314 \bmod 5 = 4 \end{array}\right\} \underset{(\ldots,4,4)}{\Longrightarrow} \left\{\begin{array}{l} 262 \text{ div } 5 = 52 \\ 262 \bmod 5 = 2 \end{array}\right\} \underset{(\ldots,2,4,4)}{\Longrightarrow} \ldots$$

$$\ldots \Longrightarrow \left\{\begin{array}{l} 52 \text{ div } 5 = 10 \\ 52 \bmod 5 = 2 \end{array}\right\} \underset{(\ldots,2,2,4,4)}{\Longrightarrow} \left\{\begin{array}{l} 10 \text{ div } 5 = 2 < 5 \\ 10 \bmod 5 = 0 \end{array}\right\}$$

Por tanto, $(2341 \times 34)_5 = (202244)_5$ $\square$

Ejercicio: Encontrar la base b (si existe) en la que $(3,4,3,2)_b \times (3,4)_b = (1,5,6,6,5,1)_b$.

Nótese que como tenemos el dígito 6 entonces $b \geq 7$. Pasamos a resolver el ejercicio.
Por la definición de expresión de un número en base b tenemos que

$$\left.\begin{array}{r} (3,4,3,2)_b = 3b^3 + 4b^2 + 3b + 2 \\ (3,4)_b = 3b + 4 \end{array}\right\} \Longrightarrow (3,4,3,2)_b \times (3,4)_b = (3b^3+4b^2+3b+2)\cdot(3b+4)$$

$$(1,5,6,6,5,1)_b = 1\cdot b^5 + 5b^4 + 6b^3 + 6b^2 + 5b + 1$$

Por tanto tenemos que hallar un número entero b que verifique que

$$\begin{array}{rrcl} & (3b^3 + 4b^2 + 3b + 2)\cdot(3b+4) & = & b^5 + 5b^4 + 6b^3 + 6b^2 + 5b + 1 \\ \Longrightarrow & 9b^4 + 24b^3 + 25b^2 + 18b + 8 & = & b^5 + 5b^4 + 6b^3 + 6b^2 + 5b + 1 \\ \Longrightarrow & 0 & = & b^5 - 4b^4 - 18b^3 - 19b^2 - 13b - 7 \end{array}$$

[7] Ya que $3 + 3 = 6$ y $6 = (11)_5$. Estos pequeños cálculos intermedios se omitirán a partir de ahora.

[8] También se puede hacer el cálculo directamente en base 5, usando el método de multiplicación de primaria pero teniendo en cuenta que se "lleva" a partir del 4, al igual que en el ejemplo anterior. La realización de esta multiplicación en base 5 se deja como ejercicio para el lector.

Como solo buscamos valores enteros de b, entonces buscamos raíces del polinomio $b^5 - 4b^4 - 18b^3 - 19b^2 - 13b - 7 \in \mathbb{Z}[b]$ mediante el método de Ruffini. Si hay raíces enteras, entonces serán divisores del término independiente -7.
Los divisores de -7 son $-7, -1, 1$ y 7. Sin embargo, como tenemos la condición de que $b \geq 7$, entonces vemos si el 7 es raíz. Si no, no existirá una base b para la que se cumpla la igualdad dada.

$$7^5 - 4\cdot 7^4 - 18\cdot 7^3 - 19\cdot 7^2 - 13\cdot 7 - 7 \stackrel{?}{=} 0 \implies 16807 - 9604 - 6174 - 931 - 91 - 7 \stackrel{?}{=} 0 \quad \checkmark$$

Por tanto, la igualdad del enunciado es cierta en base 7. Es decir,

$$(3432)_7 \times (34)_7 = (156651)_7 \quad \square$$

Proposición 1. Si $a_1, a_2, \ldots, a_k, m \in \mathbb{Z}$, entonces se cumple que

1. $(a_1 + a_2 + \cdots + a_k) \bmod m = \Big(a_1 \bmod m + a_2 \bmod m + \cdots + a_k \bmod m\Big) \bmod m$
2. $(a_1 \cdot a_2 \cdots a_k) \bmod m = \Big((a_1 \bmod m)(a_2 \bmod m)\cdots(a_k \bmod m)\Big) \bmod m$

Ejercicio: Demostrar que un número escrito en base 10 es múltiplo de 3 si y solo si la suma de sus cifras también es múltiplo de 3.

Sea $n \in \mathbb{N}$ un número cuya expresión en base 10 es $(a_n, a_{n-1}, \ldots, a_1, a_0)$. Entonces tenemos que demostrar[9] que n es múltiplo de 3 si y solo si $a_n + a_{n-1} + \cdots + a_1 + a_0$ es múltiplo de 3.

$$\begin{aligned}
& n \text{ es múltiplo de } 3 \\
\iff\ & n \bmod 3 = 0 \\
\iff\ & (a_n, a_{n-1}, \ldots, a_1, a_0)_{10} \bmod 3 = 0 \\
\iff\ & \big(10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0\big) \bmod 3 = 0 \\
\iff\ & \Big((10^n a_n) \bmod 3 + (10^{n-1} a_{n-1}) \bmod 3 + \cdots + (10a_1) \bmod 3 + a_0 \bmod 3\Big) \bmod 3 = 0 \quad (1)
\end{aligned}$$

Vamos a centrarnos en un sumando genérico de la expresión anterior para simplificarlo: $(10^k a_k) \bmod 3$. Por el punto 2 de la proposición anterior tenemos que:

$$\begin{aligned}
& (10^k a_k) \bmod 3 \\
= \ & (10 \cdot 10 \cdot \overset{k \text{ veces}}{\cdots} \cdot 10 \cdot a_k) \bmod 3 \\
= \ & \Big(10 \bmod 3 \cdot 10 \bmod 3 \cdots 10 \bmod 3 \cdot a_k \bmod 3\Big) \bmod 3
\end{aligned}$$

Como $10 \bmod 3 = 1$, entonces esto se simplifica a

$$\begin{aligned}
& (1 \cdot 1 \cdots 1 \cdot a_k \bmod 3) \bmod 3 \\
= \ & a_k \bmod 3
\end{aligned}$$

Y por tanto, podemos simplificar la expresión en (1):

$$\begin{aligned}
& \Big((10^n a_n) \bmod 3 + (10^{n-1} a_{n-1}) \bmod 3 + \cdots + (10a_1) \bmod 3 + a_0 \bmod 3\Big) \bmod 3 = 0 \quad (1) \\
\iff\ & \Big(a_n \bmod 3 + a_{n-1} \bmod 3 + \cdots + a_1 \bmod 3 + a_0 \bmod 3\Big) \bmod 3 = 0 \\
\iff\ & \Big(a_n + a_{n-1} + \cdots + a_1 + a_0\Big) \bmod 3 = 0 \\
\iff\ & a_n + a_{n-1} + \cdots + a_1 + a_0 \text{ es múltiplo de } 3
\end{aligned}$$

Por tanto, como hemos demostrado, un número es divisible por 3 si y solo si los dígitos de su expresión en base 10 suman un múltiplo de 3. $\square$

[9] Claramente para la demostración usaremos la proposición anterior.

Ejercicio: Demostrar que un número escrito en base 10 es múltiplo de 5 si y solo si termina en 0 o en 5.

Sea $n \in \mathbb{N}$ un número cuya expresión en base 10 es $(a_n, a_{n-1}, \ldots, a_1, a_0)$. Entonces tenemos que demostrar que n es múltiplo de 5 si y solo si $a_0 = 0$ ó $a_0 = 5$.

$$\begin{aligned}
& n \text{ es múltiplo de } 5 \\
\iff \quad & n \bmod 5 = 0 \\
\iff \quad & (a_n, a_{n-1}, \ldots, a_1, a_0)_{10} \bmod 5 = 0 \\
\iff \quad & \left(10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0\right) \bmod 5 = 0 \\
\iff \quad & \left((10^n a_n) \bmod 5 + (10^{n-1} a_{n-1}) \bmod 5 + \cdots + (10a_1) \bmod 5 + a_0 \bmod 5\right) \bmod 5 = 0 \qquad (1)
\end{aligned}$$

Un sumando genérico de (1) tiene la siguiente forma:

$$\begin{aligned}
& (10^k a_k) \bmod 5 \\
= \quad & (10 \cdot 10 \cdot \overset{k \text{ veces}}{\cdots} \cdot 10 \cdot a_k) \bmod 5 \\
= \quad & \left(10 \bmod 5 \cdot 10 \bmod 5 \cdots 10 \bmod 5 \cdot a_k \bmod 5\right) \bmod 5
\end{aligned}$$

Como $10 \bmod 5 = 0$, entonces $(10^k a_k) \bmod 5$ es igual a 0 si $k \geq 1$, y si $k = 0$ (en cuyo caso el sumando sería solamente $a_0 \bmod 5$) entonces se deja igual. Por tanto, simplificamos la expresión en (1) de la siguiente manera:

$$\begin{aligned}
& \left((10^n a_n) \bmod 5 + (10^{n-1} a_{n-1}) \bmod 5 + \cdots + (10a_1) \bmod 5 + a_0 \bmod 5\right) \bmod 5 = 0 \qquad (1) \\
\iff \quad & \left(0 + 0 + \cdots + 0 + a_0 \bmod 5big\right) \bmod 5 = 0 \\
\iff \quad & (a_0 \bmod 5) \bmod 5 = 0 \\
\iff \quad & a_0 \bmod 5 = 0 \qquad (2)
\end{aligned}$$

Como a_0 es un dígito en base 10, entonces no puede ser mayor que 9. Por tanto la condición de (2) se cumple si y solo si $a_0 \in \{0, 5\}$, es decir, un número escrito en base 10 es múltiplo de 5 si y solo si su última cifra es 0 ó 5. $\square$

Ejercicio: ¿Cuándo es un número escrito en base 8 múltiplo de 7?

(Solución intencionalmente en blanco)

Ejercicio: ¿Cuándo es un número escrito en base 8 múltiplo de 4?

(Solución intencionalmente en blanco)

Ejercicio: Calcular todos los números naturales que al escribirlos en base 8 terminan en 12 y al escribirlos en base 9 terminan en 25.

Sea $x \in \mathbb{N}$ un número que cumple las condiciones del enunciado. entonces podemos ver que $x = (a_{n_1}, \ldots, a_3, a_2, 1, 2)_8$ y $x = (b_{n_2}, \ldots, b_3, b_2, 2, 5)_9$.
Nótese que

- La relación entre las expresiones en base 8 y base $64 = 8^2$ de un número nos dice que un dígito en base 64 corresponde a dos dígitos en base 8. Por tanto, si $x = (\ldots, 1, 2)_8$ entonces la expresión en base 64 de x terminará en $1 \cdot 8 + 2 = 10$.
- La relación entre las expresiones en base 9 y base $81 = 9^2$ de un número nos dice que un dígito en base 81 corresponde a dos dígitos en base 9. Por tanto, si $x = (\ldots, 2, 5)_9$ entonces la expresión en base 81 de x terminará en $2 \cdot 9 + 5 = 23$.

Entonces tenemos que $x = (c_{n_3}, \ldots, c_1, 10)_{64} = (d_{n_4}, \ldots, d_1, 23)_{81}$. Por tanto: [10]

[10] Nótese que si a_0 es el último dígito de la expresión en base b de un número x, entonces $x \equiv a_0 \pmod{b}$ debido al procedimiento que sigue.

$$\left\{\begin{array}{lllll} x = c_{n_3}\cdot 64^{n_3} + \cdots + c_1\cdot 64 + 10 & \Longrightarrow & x = 64\cdot(c_{n_3}\cdot 64^{n_3-1} + \cdots + c_1) + 10 & \Longrightarrow & \ldots \\ x = d_{n_4}\cdot 81^{n_4} + \cdots + d_1\cdot 81 + 23 & \Longrightarrow & x = 81\cdot(d_{n_4}\cdot 81^{n_4-1} + \cdots + d_1) + 23 & \Longrightarrow & \ldots \end{array}\right.$$

$$\left.\begin{array}{lllll} \Longrightarrow & x \bmod 64 = 10 & \Longrightarrow & x \equiv 10 \pmod{64} & (1) \\ \Longrightarrow & x \bmod 81 = 23 & \Longrightarrow & x \equiv 23 \pmod{81} & (2) \end{array}\right\}$$

Nos queda un sistema de ecuaciones en congruencias que resolvemos normalmente: Las soluciones de (1) son de la forma $10 + 64k$ t. q. $k \in \mathbb{Z}$. Por tanto, tras sustituir en (2) nos queda que

$$\begin{array}{ll} & (64k + 10) \equiv 23 \pmod{81} \\ \Longrightarrow & 64k \equiv 13 \pmod{81} \end{array}$$

Como $\text{m. c. d}\{64, 81\} = 1 \mid 13$ entonces la ecuación tiene solución. Si encontramos $u, v \in \mathbb{Z}$ t. q. $64u + 81v = 1$, entonces $13u \bmod 81$ será una solución de la congruencia. Pasamos a aplicar el algoritmo extendido de Euclides a 64 y 81:

$$\begin{array}{ccccccccccccc} (a_0, a_1) & = & (81, 64) & \overset{q=1}{=} & (64, 17) & \overset{q=3}{=} & (17, 13) & \overset{q=1}{=} & (13, 4) & \overset{q=3}{=} & (4, 1) & \overset{q=4}{=} & (1, 0) \\ (s_0, s_1) & = & (1, 0) & = & (0, 1) & = & (1, -3) & = & (-3, 4) & = & (4, -15) & = & (-15, \ldots) \\ (t_0, t_1) & = & (0, 1) & = & (1, -1) & = & (-1, 4) & = & (4, -5) & = & (-5, 19) & = & (19, \ldots) \end{array}$$

El algoritmo nos proporciona la igualdad $64 \cdot 19 + 81 \cdot (-15) = 1$. Por tanto $(13 \cdot 19) \bmod 81 = 247 \bmod 81 = 4 \implies k = 4$ es una solución de la ecuación de congruencias. Por tanto las soluciones de la segunda ecuación en k son de la forma $4 + 81n$ t. q. $n \in \mathbb{Z}$
Ahora sustituimos de vuelta en x: $x = 10 + 64k = 10 + 64(4 + 81n) = 266 + 5376n$
Por tanto las soluciones del sistema de congruencias vienen dadas por el conjunto

$$S_0 = \Big\{266 + 5376n \text{ t. q. } n \in \mathbb{Z}\Big\}$$

Pero como el enunciado solo nos pide las soluciones naturales, entonces recortamos los valores que puede tomar n para que el número final sea un elemento de $\mathbb{N}$. Como $266 + 5376n$ es positivo solo si $n \geq 0 \implies n \in \mathbb{N}$ entonces la solución del problema es

$$S = S_0 \cap \mathbb{N} = \Big\{266 + 5376n \text{ t. q. } n \in \mathbb{N}\Big\} \quad \square$$

10.2 La función φ de Euler

Sea $m \in \mathbb{N} \setminus \{0, 1\}$. Entonces la función φ de Euler del número m viene definida como la cantidad de enteros positivos menores que m que son primos relativos con m, es decir:

$$\varphi(m) \coloneqq \#\Big\{x \in \{1, 2, \ldots, m-1\} \text{ t. q. } \text{m. c. d}\{m, x\} = 1\Big\}$$

Ejemplo:

$$\varphi(9) = \#\Big\{x \in \{1, 2, 3, \ldots, 9\} \text{ t. q. } \text{m. c. d}\{x, 9\} = 1\Big\} = \#\{1, 2, 4, 5, 7, 8\} = 6$$

Nótese que si p es un número primo entonces $\varphi(p) = p - 1$ [11]

[11] Ya que todos los enteros positivos $n < p$ cumplen que $\text{m. c. d}\{p, n\} = 1$, y el cardinal del conjunto $\{1, 2, 3, \ldots, p-1\}$ es $(p-1) + 1 - 1 = p - 1$.

Teorema 1.

1. Si p es un número primo y $n \in \mathbb{N} \setminus \{0\}$, entonces $\varphi(p^n) = p^n - p^{n-1}$
2. Si $m, n \in \mathbb{N} \setminus \{0, 1\}$ y $\text{m. c. d}\{m, n\} = 1$, entonces $\varphi(m \cdot n) = \varphi(m)\varphi(n)$
3. si $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ es la descomposición en primos de un número $m \in \mathbb{N}$, entonces [12]

$$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$$

Ejemplo: Para calcular $\varphi(48)$, hallamos su descomposición en primos:
$48 = 6 \cdot 8 = 2 \cdot 3 \cdot 2^3 = 2^4 \cdot 3$. Por tanto,

$$\varphi(48) = \varphi(2^4 \cdot 3) = (2^4 - 2^3)(3^1 - 3^0) = 8 \cdot 2 = 16$$

Teorema 2 (Teorema de Euler-Fermat)**.** Sean $a, m \in \mathbb{N} \setminus \{0, 1\}$ t. q. $\text{m. c. d}\{a, m\} = 1$. Entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$ [13]

Ejercicio: Calcular el resto de dividir 53^{168} entre 48.

Como $53 \bmod 48 = 5$, entonces $53^{168} \bmod 48 = 5^{168} \bmod 48$. Esto a su vez es igual al valor de 5^{168} en $\mathbb{Z}_{48}$.
El teorema de Euler-Fermat nos dice que, como $\text{m. c. d}\{5, 48\} = 1$, entonces $5^{\varphi(48)} \equiv 1 \pmod{48}$. $\varphi(48) = 16$, así que tenemos que

$$5^{16} \equiv 1 \pmod{48} \implies 5^{16} \bmod 48 = 1 \implies 5^{16} = 1 \text{ en } \mathbb{Z}_{48}$$

Por tanto, como $168 = 16 \cdot 10 + 8$, entonces en $\mathbb{Z}_{48}$ se cumple que:

$$5^{168} = 5^{16 \cdot 10 + 8} = (5^{16})^{10} \cdot 5^8 = 1^{10} \cdot 5^8 = 5^8$$

Ahora calculamos el valor de 5^8 en $\mathbb{Z}_{48}$:

$$5^2 = 25 \implies 5^4 = (25 \cdot 25) \bmod 48 = 1 \implies 5^8 = 1 \cdot 1 = 1$$

Por tanto, el resto de dividir 53^{168} entre 48 es 1. □

10.3 Ecuaciones diofánticas lineales con tres incógnitas

Comenzaremos esta sección mostrando un método alternativo para resolver ecuaciones diofánticas lineales con dos incógnitas, el cual nos servirá para resolver las de tres incógnitas más fácilmente.
Ejercicio: Resolver la ecuación diofántica $12x + 15y = 42$.

Como $\text{m. c. d}\{12, 15\} = 3 \mid 42$, entonces la ecuación del enunciado tiene solución, y además tiene las mismas soluciones que la ecuación

$$\begin{aligned} & 4x + 5y = 14 \qquad (1) \\ \implies \quad & 4x - 14 = -5y \\ \implies \quad & 4x - 14 = 5 \cdot (-y) \end{aligned}$$

[12] Esto es una consecuencia de los otros dos puntos del teorema, ya que si $p_1, p_2, \ldots, p_r$ son números primos distintos, entonces $\text{m. c. d}\{p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}\} = 1$.

[13] Esto no quiere decir que $a^{\varphi(m)}$ sea el entero positivo más pequeño que verifique esto. Por ejemplo, en el ejercicio siguiente, el teorema de Euler-Fermat nos da que $5^{16} \equiv 1 \pmod{48}$ pero más tarde vemos que $5^4 \bmod 48 = 1 \implies 5^4 \equiv 1 \pmod{48}$

Por tanto, tenemos que $4x - 14$ es un múltiplo de 5 (ya que en una ecuación diofántica todas las soluciones tienen valores enteros). Convertimos la ecuación en una congruencia:

$$\begin{array}{ll} & 4x - 14 = 5(-y) \\ \Longrightarrow & 4x - 14 \text{ es múltiplo de } 5 \\ \Longrightarrow & (4x - 14) \bmod 5 = 0 \\ \Longrightarrow & 4x - 14 \equiv 0 \pmod 5 \\ \Longrightarrow & 4x \equiv 14 \pmod 5 \\ \Longrightarrow & 4x \equiv 4 \pmod 5 \qquad (2) \end{array}$$

Como $x = 1$ es una solución de (2), entonces el conjunto formado por todas las soluciones de dicha ecuación es $\Big\{1 + 5k \text{ t. q. } k \in \mathbb{Z}\Big\}$. Ahora sustituimos $x = 1 + 5k$ en la ecuación (1):

$$\begin{array}{ll} & 4x + 5y = 14 \qquad (1) \\ \Longrightarrow & 4(1 + 5k) + 5y = 14 \\ \Longrightarrow & 5y = 14 - 4(1 + 5k) \\ \Longrightarrow & 5y = 14 - 4 - 20k \\ \Longrightarrow & 5y = 10 - 20k \\ \Longrightarrow & y = 2 - 4k \end{array}$$

Por tanto, el conjunto de todas las soluciones a la ecuación del enunciado es:

$$S = \Big\{(1 + 5k, 2 - 4k) \text{ t. q. } k \in \mathbb{Z}\Big\} \quad \square$$

Pasamos ahora a ver el método de resolución de ecuaciones diofánticas lineales con 3 incógnitas:
Ejercicio: Resolver la ecuación diofántica $8x + 12y + 18z = 14$.

Como $\text{m. c. d}\{8, 12, 18\} = 2 \mid 14$, entonces la ecuación dada tiene solución, y tiene las mismas soluciones que la ecuación

$$4x + 6y + 9z = 7 \qquad (1)$$

Para resolver esta ecuación haremos un cambio de variable.
Como $\text{m. c. d}\{4, 6\} = 2$ entonces hacemos el cambio de variable $2u = 4x + 6y$ por lo que nos queda la ecuación

$$2u + 9z = 7 \qquad (1')$$

Ahora resolvemos esta ecuación como una ecuación diofántica con dos incógnitas:

$$\begin{array}{ll} & 2u + 9z = 7 \qquad (1') \\ \Longrightarrow & 2u - 7 = 9(-z) \\ \Longrightarrow & 2u - 7 \equiv 0 \pmod 9 \\ \Longrightarrow & 2u \equiv 7 \pmod 9 \qquad (2) \end{array}$$

Como $u = 8$ es una solución de (2), entonces toda solución de esta ecuación es de la forma $8 + 9k$ t. q. $k \in \mathbb{Z}$. Ahora sustituimos en $(1')$:

$$
\begin{aligned}
& 2u + 9z = 7 \qquad (1') \\
\Longrightarrow \quad & 2(8 + 9k) + 9z = 7 \\
\Longrightarrow \quad & 9z = 7 - 16 - 18k \\
\Longrightarrow \quad & 9z = -9 - 18k \\
\Longrightarrow \quad & z = -1 - 2k
\end{aligned}
$$

Del cambio de variable $2u = 4x + 6y \implies u = 2x + 3y$ obtenemos la ecuación

$$2x + 3y = 8 + 9k \tag{3}$$

Esta es otra ecuación diofántica lineal con dos incógnitas [14]. Pasamos a resolver (3):

$$
\begin{aligned}
& 2x + 3y = 8 + 9k \qquad (3) \\
\Longrightarrow \quad & 3y - (8 + 9k) = 2(-x) \\
\Longrightarrow \quad & 3y - (8 + 9k) \equiv 0 \pmod 2 \\
\Longrightarrow \quad & 3y \equiv 8 + 9k \pmod 2 \\
\Longrightarrow \quad & y \equiv (8 + 9k) \bmod 2 \pmod 2 \\
\Longrightarrow \quad & y \equiv k \pmod 2 \qquad (4)
\end{aligned}
$$

Claramente $y = k$ es una solución de (4). Por tanto, todas las soluciones tendrán la forma $k + 2m$ t. q. $m \in \mathbb{Z}$. Ahora sustituimos en (3):

$$
\begin{aligned}
& 2x + 3y = 8 + 9k \qquad (3) \\
\Longrightarrow \quad & 2x + 3(k + 2m) = 8 + 9k \\
\Longrightarrow \quad & 2x = 8 + 9k - 3k - 6m \\
\Longrightarrow \quad & 2x = 8 + 6k - 6m \\
\Longrightarrow \quad & x = 4 + 3k - 3m
\end{aligned}
$$

Tras hallar los valores de x, y y z [15], podemos concluir que el conjunto de soluciones de la ecuación del enunciado es

$$S = \Big\{(4 + 3k - 3m,\ k + 2m,\ -1 - 2k) \text{ t. q. } k, m \in \mathbb{Z}\Big\} \quad \square$$

Nota: En el ejercicio anterior nos quedó la ecuación en congruencias $y \equiv k \pmod 2$, la cual se podía resolver directamente. En general, la ecuación resultante es de la forma $ay \equiv bk + c \pmod m$. Para calcular una solución a esta ecuación, la resolvemos como si fuera una congruencia normal: hallamos $u, v \in \mathbb{Z}$ t. q. $au + mv = 1$ mediante el algoritmo extendido de Euclides, y entonces una solución de la congruencia es $(bk + c)u \bmod m$.
Por ejemplo, si tenemos que resolver la ecuación $3y \equiv 2k + 1 \pmod 7$, entonces le aplicamos el algoritmo extendido de Euclides a 7 y 3 para hallar una solución de la congruencia. La igualdad resultante es $3 \cdot (-2) + 7 \cdot 1 = 1$, por lo que una solución de la ecuación es

$$y = -2(2k + 1) \bmod 7 = (-4k - 2) \bmod 7 = 3k + 5.$$

Por tanto, las soluciones de la ecuación $3y \equiv 2k + 1 \pmod 7$ son de la forma $3k + 5 + 7m$ t. q. $m \in \mathbb{Z}$.
Ejercicio: Resolver la ecuación diofántica $33x - 21y + 15z = 24$

(Solución intencionalmente en blanco)

[14] Aquí, k es un parámetro, no hay que hallar su valor.
[15] Nótese que esta vez la solución depende de dos parámetros.

10.4 Orden producto cartesiano

Sean $(A_1, \underset{1}{\leq}), (A_2, \underset{2}{\leq}), \ldots, (A_n, \underset{n}{\leq})$ conjuntos ordenados. Entonces en el conjunto $A_1 \times A_2 \times \cdots \times A_n$ se define la relación de orden $\underset{p}{\leq}$ de la siguiente manera:
Si $(a_1, a_2, \ldots a_n), (b_1, b_2, \ldots, b_n) \in A_1 \times A_2 \times \cdots \times A_n$, entonces

$$(a_1, a_2, \ldots a_n) \underset{p}{\leq} (b_1, b_2, \ldots, b_n) \iff a_1 \underset{1}{\leq} b_1, \quad a_2 \underset{2}{\leq} b_2, \ldots, \quad a_n \underset{n}{\leq} b_n$$

A este orden se le llama orden producto cartesiano de los órdenes $\underset{1}{\leq}, \underset{2}{\leq}, \ldots, \underset{n}{\leq}$.
Ejemplo: Dados los conjuntos ordenados $(\mathbb{Z}, \underset{u}{\leq})$ y $(\mathbb{N}, \underset{m}{\leq})$ [16], dotamos al conjunto $\mathbb{Z} \times \mathbb{N}$ del orden producto cartesiano de $\underset{u}{\leq}$ y $\underset{m}{\leq}$. Es decir, si $(a, n), (b, m) \in \mathbb{Z} \times \mathbb{N}$, entonces

$$(a, n) \underset{p}{\leq} (b, m) \iff a \underset{u}{\leq} b \text{ y } n \underset{m}{\leq} m$$

En el conjunto ordenado $(\mathbb{Z} \times \mathbb{N}, \underset{p}{\leq})$ tenemos que $(-2, 3) \underset{p}{\leq} (0, 6)$ y $(-2, 3) \underset{p}{\not\leq} (0, 4)$,
ya que $-2 \underset{u}{\leq} 0$ y $3 \underset{m}{\leq} 6$ pero $3 \underset{m}{\not\leq} 4$.
Ejercicio: Dado el conjunto ordenado $(\mathbb{Z} \times \mathbb{N}, \underset{p}{\leq})$ donde $\underset{p}{\leq}$ es el orden producto cartesiano visto en el ejemplo anterior, calcular los elementos notables de $B = \{(2, 3), (3, 6), (-1, 1), (4, 7)\}$.

- Los maximales de B son $(3, 6)$ y $(4, 7)$, ya que ambos son "mayores" [17] que $(2, 3)$ y $(-1, 1)$, y además $(3, 6) \underset{p}{\not\leq} (4, 7)$ y $(4, 7) \underset{p}{\not\leq} (3, 6)$. Por tanto, ambos pares ordenados cumplen la definición de maximal.
- El único minimal de B es el $(-1, 1)$, ya que el único par "menor o igual" que éste es justamente el $(-1, 1)$.
- Por lo que hemos visto antes, B no tiene máximo, y el mínimo de B es también el $(1, 1)$.
- Una cota superior de B es un par ordenado $(a, n) \in \mathbb{Z} \times \mathbb{N}$ que cumpla que $4 \underset{u}{\leq} a$ [18] y que n sea múltiplo de 1, de 3, de 6 y de 7. Por tanto el conjunto de cotas superiores de B es $C_S = \{(a, n) \in \mathbb{Z} \times \mathbb{N} \text{ t. q. } 4 \underset{u}{\leq} a \text{ y } n = 42k \text{ t. q. } k \in \mathbb{N}\}$.
- Una cota inferior de B es un par ordenado $(a, n) \in \mathbb{Z} \times \mathbb{N}$ que cumpla que $a \underset{u}{\leq} -1$ y n sea divisor de 1, de 3, de 6 y de 7. Como el único divisor común de estos números es 1 entonces el conjunto de cotas inferiores de B es $C_I = \{(a, 1) \in \mathbb{Z} \times \mathbb{N} \text{ t. q. } a \underset{u}{\leq} -1\}$.
- El supremo de B es el mínimo de C_S, es decir, el $(4, 42)$.
- El ínfimo de B es el máximo de C_I, es decir, el $(-1, 1)$.

□

10.5 Orden lexicográfico

El orden usual en $\mathbb{N}^n$ $(n \in \mathbb{N} \setminus \{0, 1\})$ es el orden producto cartesiano de n órdenes usuales. Es decir, si $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{N}^n$, entonces

$$(a_1, a_2, \ldots, a_n) \underset{u}{\leq} (b_1, b_2, \ldots, b_n) \iff a_1 \underset{u}{\leq} b_1, a_2 \underset{u}{\leq} b_2, \ldots, a_n \underset{u}{\leq} b_n$$

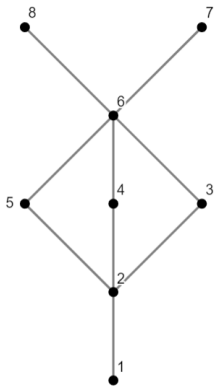
[16] Donde $\underset{u}{\leq}$ es el orden usual y $\underset{m}{\leq}$ es el orden de multiplicidad (véase en el tema 1).
[17] Claramente, con "(a, m) es mayor que (b, n)" queremos decir $(b, n) \underset{p}{\leq} (a, m)$
[18] Ya que el 4 es el mayor número entero (en cuanto al orden usual) de B

Sin embargo el conjunto ordenado $(\mathbb{N}^n, \underset{u}{\leq})$ no es totalmente ordenado, ya que $(2,3),(1,4) \in \mathbb{N}^2$ pero $(2,3) \underset{u}{\not\leq} (1,4)$ y $(1,4) \underset{u}{\not\leq} (2,3)$.
Existen órdenes en $\mathbb{N}^n$ que son totales. Por ejemplo, el orden lexicográfico $\underset{lex}{\leq}$, que se define de la siguiente manera: $(a_1, a_2, \ldots, a_n) \underset{lex}{\leq} (b_1, b_2, \ldots b_n)$ si y solo si $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ o si la primera coordenada no nula de la n-tupla $(a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n)$ es negativa.
Ejercicio: Ordenar según el orden lexicográfico de menor a mayor los elementos del conjunto $\{(1,1,1),(0,1,1),(0,0,2),(2,3,1),(1,0,4)\}$.

$$(0,0,2) \underset{lex}{\leq} (0,1,1) \underset{lex}{\leq} (1,0,4) \underset{lex}{\leq} (1,1,1) \underset{lex}{\leq} (2,3,1)$$

10.6 Representación gráfica de órdenes

Un conjunto ordenado $(A, \leq)$ se puede representar gráficamente de la siguiente manera: poniendo todos los elementos del conjunto como puntos y uniendo dichos puntos de manera que para todo $a, b \in A$, $a \leq b$ si y solo si existe un camino solamente ascendente yendo desde el punto que representa a a al punto que representa a b.
Ejemplo: Dado el conjunto ordenado $\left(\{1,2,3,4,5,6,7,8\}, \underset{x}{\leq}\right)$, representado mediante el siguiente gráfico:



Tenemos que $2 \underset{x}{\leq} 7$ y $3 \underset{x}{\not\leq} 4$.
Ejercicio: Dado el conjunto ordenado del ejemplo anterior, calcular los elementos notables de $B = \{2,3,4\}$.

- Los maximales de B son el 3 y el 4. [19]
- El único minimal de B es el 2.
- B no tiene máximo, y el mínimo de B es el 2 también.
- Una cota superior de B es un elemento de $\{1,2,3,4,5,6,7,8\}$ desde el que existe un camino descendente a todos los elementos de B. Por tanto el conjunto de cotas superiores de B es $C_S = \{6,7,8\}$.
- Análogamente, una cota inferior de B es un elemento de $\{1,2,3,4,5,6,7,8\}$ desde el que existe un camino ascendente a todos los elementos de B, y por consiguiente el conjunto de cotas inferiores de B es $C_I = \{1,2\}$

[19] Los elementos notables de un subconjunto ordenado son bastante más fáciles de ver cuando el orden viene representado gráficamente: El 3 y el 4 son los que están más "arriba" en el gráfico, y por tanto son maximales, por ejemplo.

- El supremo de B es el mínimo de C_S, y éste es a su vez el 6.
- El ínfimo de B es el máximo de C_I, el cual es el 2.

□

10.7 El cuerpo de los números complejos

El conjunto de los números complejos se define como

$$\mathbb{C} \coloneqq \Big\{ a + b \cdot i \ \text{ t. q. } \ a, b \in \mathbb{R} \Big\}$$

donde i (la unidad imaginaria) viene definida por la ecuación $i^2 = -1$ [20]. Si $a + bi \in \mathbb{C}$ y $a, b \in \mathbb{R}$, entonces se dice que a es la parte real y b es la parte imaginaria de dicho número complejo.
En $\mathbb{C}$, la operación $+$ y $\cdot$ se definen de la siguiente manera para todo $a + bi, c + di \in \mathbb{C}$:

- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi) \cdot (c + di) = a(c + di) + bi(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$ [21]

Proposición 2. $(\mathbb{C}, +, \cdot)$ es un cuerpo.

Nota: El elemento neutro de la suma es $0 = 0 + 0i$, y el elemento neutro del producto es $1 = 1 + 0i$. Los elementos inversos para la suma y el producto de $a + bi \in \mathbb{C}$ son $-(a + bi) = (-a) + (-b)i$ y (si $a + bi \neq 0$) $(a + bi)^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2} i$ [22], respectivamente.

Teorema 3 (Teorema fundamental del Álgebra)**.** Si $a(x) \in \mathbb{C}[x]$ es un polinomio de grado mayor o igual que 1, entonces $a(x)$ tiene al menos una raíz. [23]

Corolario 1. Un polinomio $a(x) \in \mathbb{C}[x]$ es irreducible si y solo si $\operatorname{gr}\big(a(x)\big) = 1$.

Sea $a + bi \in \mathbb{C}$. Entonces definimos el conjugado de $a + bi$ como el número complejo $a - bi$.

Proposición 3. Sea $f : \mathbb{C} \longrightarrow \mathbb{C}$ la aplicación definida por $f(a + bi) = a - bi$. Entonces f verifica las siguientes propiedades:

1. $f\big((a + bi) + (c + di)\big) = f(a + bi) + f(c + di)$
2. $f\big((a + bi)(c + di)\big) = f(a + bi) \cdot f(c + di)$
3. $f(x) = x$ para todo $x \in \mathbb{R}$ [24] $\implies f(0) = 0$

Corolario 2. Si $\alpha + \beta i$ es una raíz de un polinomio $a(x) \in \mathbb{R}[x]$, entonces $\alpha - \beta i$ también es raíz de $a(x)$. [25]

Corolario 3. Si un polinomio $a(x) \in \mathbb{R}[x]$ es irreducible entonces $\operatorname{gr}\big(a(x)\big) \in \{1, 2\}$.

Nota:

1. Todo polinomio de grado 1 de $\mathbb{R}[x]$ es irreducible.
2. Un polinomio de grado 2 de $\mathbb{R}[x]$ es irreducible si y solo si no tiene raíces reales.

---

[20] O, si se prefiere, $i = \sqrt{-1}$.

[21] Esto viene de operar con los números complejos como si fueran polinomios de $\mathbb{R}[i]$, teniendo en cuenta que $i^2 = -1$ y por tanto $ac + bdi^2 = ac + (-1) \cdot bd = ac - bd$.

[22] Ya que $(a + bi) \cdot \left(\dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2} i \right) = \dfrac{a^2}{a^2 + b^2} - \cancel{\dfrac{abi}{a^2 + b^2}} + \cancel{\dfrac{bi \cdot a}{a^2 + b^2}} + \dfrac{b^2}{a^2 + b^2} = \dfrac{a^2 + b^2}{a^2 + b^2} = 1$

[23] Más precisamente, un polinomio $a(x) \in \mathbb{C}[x]$ de grado $n \geq 1$ tiene exactamente n raíces (contando una raíz múltiple de multiplicidad m como si fueran m raíces.)

[24] Nótese que $\mathbb{R} \subseteq \mathbb{C}$ ya que todo número real puede considerarse como un número complejo con parte imaginaria 0.

[25] Este corolario también es conocido como el teorema de la raíz conjugada compleja.

10.8 Irreducibilidad en $\mathbb{Q}[x]$

Determinar la reducibilidad o irreducibilidad de un polinomio con coeficientes racionales es una cuestión difícil. No obstante, existen algoritmos y otros procesos que pueden determinar en casos concretos si un polinomio de $\mathbb{Q}[x]$ es irreducible o no. En esta sección daremos dos de los principales criterios que se usan para resolver este tipo de cuestiones.

Criterio de Eisenstein

Si $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ es un polinomio tal que $\text{gr}\big(a(x)\big) \geq 2$ y existe un número primo p tal que

$$p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1} \text{ pero } p \nmid a_n$$

entonces el polinomio $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ es irreducible. [26]

Ejercicio: Demostrar que el polinomio $x^7 + 6x^5 + 2x^3 + 4x^2 + 2 \in \mathbb{Q}[x]$ es irreducible.

> Aplicamos el criterio de Eisenstein con el número primo 2. Como $2 \mid 2$, $2 \mid 4$, $2 \mid 6$ y $2 \nmid 1$ [27], entonces el polinomio dado es irreducible. $\square$

Ejercicio: Demostrar que si $n \in \mathbb{N} \setminus \{0, 1\}$ y p es un número primo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

> Sea $a(x) = x^n - p \in \mathbb{Q}[x]$. Entonces si aplicamos el criterio de Eisenstein con el número primo p, vemos que $p \mid p$ pero $p \nmid 1$ y por tanto $a(x)$ es irreducible en $\mathbb{Q}[x]$. Como un polinomio irreducible de grado mayor o igual a 2 no tiene raíces, entonces podemos afirmar que $a(x)$ no tiene raíces racionales y por tanto $\sqrt[n]{p} \notin \mathbb{Q}$. $\square$

Ejercicio: Sea $n \in \mathbb{N} \setminus \{0\}$. Demostrar que existen infinitos polinomios irreducibles de grado n en $\mathbb{Q}[x]$.

> Si $n = 1$, entonces es fácil de ver que hay infinitos polinomios irreducibles de grado 1, ya que todo polinomio de grado 1 es irreducible y hay infinitos polinomios de grado 1 en $\mathbb{Q}[x]$.
>
> Para $n > 1$, tomamos el conjunto $P = \Big\{x^n - p \text{ t. q. } p \text{ es un número primo}\Big\} \subseteq \mathbb{Q}[x]$. Como hemos demostrado en el ejercicio anterior, todos los polinomios de P son irreducibles. Como hay infinitos números primos, entonces podemos afirmar que $\#P = \infty$ y por tanto existen infinitos polinomios irreducibles de grado n en $\mathbb{Q}[x]$. $\square$

Criterio de reducción

Sea p un número primo positivo, $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, y $\overline{a}(x) = \overline{a_n} x^n + \overline{a_{n-1}} x^{n-1} + \cdots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_p[x]$, donde $\overline{a_i} = a_i \bmod p$ para todo $i \in \{0, 1, \ldots, n-1, n\}$. Si $\text{gr}\big(\overline{a}(x)\big) = \text{gr}\big(a(x)\big)$ y $\overline{a}(x)$ es irreducible en $\mathbb{Z}_p[x]$, entonces $a(x)$ es irreducible en $\mathbb{Q}[x]$. [28]

Ejercicio: Demostrar que el polinomio $a(x) = x^4 + 17x^3 + 5x^2 + 3x + 1 \in \mathbb{Q}[x]$ es irreducible.

> Aplicando el criterio de reducción con el número primo 2, tenemos que $a(x)$ será irreducible si el polinomio $\overline{a}(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible. Como $\overline{a}(x)$ no tiene raíces y es de grado 4, entonces será irreducible si no lo divide ningún polinomio mónico e irreducible de grado 2 en $\mathbb{Z}_2[x]$. Como el único polinomio que cumple estas condiciones es $x^2 + x + 1$ y $(x^2 + x + 1) \nmid (x^4 + x^3 + x^2 + x + 1)$, entonces podemos afirmar que $\overline{a}(x)$ es irreducible y por tanto $a(x)$ también es irreducible. $\square$

[26] Nótese que como $\mathbb{Z} \subseteq \mathbb{Q}$ entonces $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ y por tanto si $a(x) \in \mathbb{Z}[x]$ entonces $a(x)$ también es un polinomio de $\mathbb{Q}[x]$.

[27] También se tiene que $2 \mid 0$ (ya que el polinomio es en realidad $x^7 + 0x^6 + 6x^5 + 0x^4 + 2x^3 + 4x^2 + 0x + 2$) pero no hace falta decirlo ya que todo número entero divide al cero.

[28] Es decir, si existe algún número primo p para el que $a(x)$ con sus coeficientes módulo p es irreducible en $\mathbb{Z}_p[x]$, entonces $a(x)$ es irreducible en $\mathbb{Q}[x]$ (En caso de tener coeficientes fraccionarios, se debe multiplicar para tener coeficientes enteros).

10.9 Ecuaciones en congruencias en anillos de polinomios

Sea K un cuerpo y $a(x), b(x), m(x) \in K[x]$. Entonces diremos que
$a(x) \equiv b(x) \pmod{m(x)}$ si $m(x) \mid \big(a(x) - b(x)\big)$.
Una ecuación en congruencias de grado 1 en $K[x]$ es una ecuación de la forma
$a(x) \cdot X \equiv b(x) \pmod{m(x)}$ [29].

Teorema 4. Sea la siguiente ecuación en congruencias en $K[x]$

$$a(x)X \equiv b(x) \pmod{m(x)} \tag{1}$$

Entonces (1) cumple las siguientes propiedades:

1. La ecuación (1) tiene solución si y solo si $\mathrm{m.\,c.\,d}\big\{a(x), m(x)\big\} \mid b(x)$.
2. Si $d(x) = \mathrm{m.\,c.\,d}\big\{a(x), b(x)\big\}$ y $d(x) \mid b(x)$, entonces (1) tiene las mismas soluciones que la ecuación $\dfrac{a(x)}{d(x)}X \equiv \dfrac{b(x)}{d(x)} \left(\mod \dfrac{m(x)}{d(x)}\right)$.
3. Si $\mathrm{m.\,c.\,d}\big\{a(x), m(x)\big\} = 1$ y $u(x)$ es una solución de (1), entonces el conjunto formado por todas las soluciones de (1) es $\Big\{u(x) + k(x) \cdot m(x) \ \text{ t. q. } \ k(x) \in K[x]\Big\}$.
4. La ecuación $a(x)X + c(x) \equiv b(x) \pmod{m(x)}$ tiene las mismas soluciones que la ecuación $a(x)X \equiv b(x) - c(x) \pmod{m(x)}$
5. La ecuación (1) tiene las mismas soluciones que la ecuación $\big(a(x) \bmod m(x)\big)X \equiv b(x) \bmod m(x) \left(\mod m(x)\right)$
6. Si $u(x), v(x) \in K(x)$ y $a(x) \cdot u(x) + m(x) \cdot v(x) = 1$, entonces $\big(b(x)u(x)\big) \bmod m(x)$ es una solución de (1).

Ejercicio: Resolver la ecuación $(x+1)X \equiv x \pmod{x^2}$ en $\mathbb{Z}_2[x]$.

Como $\mathrm{m.\,c.\,d}\{x+1, x^2\} = (x+1)^0 \cdot \big(x^2\big)^0 = 1 \mid x$ [30], entonces la ecuación tiene solución. Pasamos a buscar $u(x), v(x) \in \mathbb{Z}_2[x]$ tales que $(x+1)u(x) + x^2 v(x) = 1$, usando el algoritmo extendido de Euclides:

$$\begin{array}{ccccccc}
\big(a_0(x), a_1(x)\big) & = & (x^2, x+1) & \overset{q(x)=x+1}{=} & (x+1, 1) & = & (1, 0) \\
\big(s_0(x), s_1(x)\big) & = & (1, 0) & = & (0, 1) & = & (1, \dots) \\
\big(t_0(x), t_1(x)\big) & = & (0, 1) & = & (1, x+1) & = & (x+1, \dots)
\end{array}$$

El algoritmo nos da la igualdad $x^2 \cdot 1 + (x+1)(x+1) = 1$. Por tanto, $\big(x \cdot (x+1)\big) \bmod x^2 = x$ es una solución de la ecuación, y por consiguiente el conjunto de todas las soluciones es:

$$S = \Big\{x + k(x) \cdot x^2 \ \text{ t. q. } \ k(x) \in \mathbb{Z}_2[x]\Big\} \quad \square$$

10.10 Sistemas de ecuaciones en congruencias en anillos de polinomios

Ejercicio:[31] Resolver el siguiente sistema en $\mathbb{Z}_2[x]$: $\begin{cases} (x+1)X \equiv x \pmod{x^2} & (1) \\ x \cdot X \equiv x+1 \pmod{x^2+x+1} & (2) \end{cases}$

[29] donde $X \in K[x]$ es la incógnita

[30] Esto se debe a que ambos polinomios están ya descompuestos en irreducibles.

[31] Al igual que la sección 6 del tema 2, esta sección y la siguiente solo incluyen ejercicios a modo de ejemplo, ya que es prácticamente igual a resolver el mismo tipo de problemas normales en $\mathbb{Z}$.

Antes de todo nótese que $\text{m. c. d}\{x^2, x+1\} = 1$ y $\text{m. c. d}\{x, x^2+x+1\} = 1$, así que ambas ecuaciones tienen solución y están simplificadas.
Como hemos calculado en el ejercicio anterior, las soluciones de (1) son de la forma $X = x + x^2k(x)$ t. q. $k(x) \in \mathbb{Z}_2[x]$. Sustituimos esto en (2):

$$\begin{aligned}
& x\big(x + x^2k(x)\big) \equiv x+1 \pmod{x^2+x+1} \\
\implies\quad & x^2 + x^3k(x) \equiv x+1 \pmod{x^2+x+1} \\
\implies\quad & x^3k(x) \equiv x^2+x+1 \pmod{x^2+x+1} \\
\implies\quad & k(x) \equiv 0 \pmod{x^2+x+1} && \Big(\text{Ya que } x^3 \bmod (x^2+x+1) = 1\Big) \\
\implies\quad & k(x) = 0 + (x^2+x+1)m(x) \text{ t. q. } m(x) \in \mathbb{Z}_2[x]
\end{aligned}$$

Por tanto, como $X = x + x^2k(x)$ y $k(x) = (x^2+x+1)m(x)$, entonces
$X = x + x^2(x^2+x+1)m(x) \implies X = (x^4+x^3+x^2)m(x) + x$ $\square$

10.11 Ecuaciones diofánticas en anillos de polinomios

Ejercicio: Resolver la ecuación diofántica $(x^2+1)X + x^2Y = x+2$ en $\mathbb{Z}_3[x]$.

Usamos el mismo método que para resolver ecuaciones diofánticas normales: transformamos en una congruencia y sustituimos el resultado en la ecuación original para resolver la otra incógnita [32]. Nótese que $\text{m. c. d}\{x^2+1, x^2\} = 1$, así que la ecuación tiene solución.

$$\begin{aligned}
& (x^2+1)X + x^2Y = x+2 \\
\implies\quad & (x^2+1)X - (x+2) = 2Y \cdot x^2 \\
\implies\quad & x^2 \mid \big((x^2+1)X - (x+2)\big) \\
\implies\quad & (x^2+1)X - (x+2) \equiv 0 \pmod{x^2} \\
\implies\quad & (x^2+1)X \equiv x+2 \pmod{x^2} \\
\implies\quad & X \equiv x+2 \pmod{x^2} && \Big(\text{Ya que } (x^2+1) \bmod x^2 = 1\Big) \\
\implies\quad & X = x+2+k(x)\cdot x^2 \text{ t. q. } k(x) \in \mathbb{Z}_3[x]
\end{aligned}$$

Ahora sustituimos el valor de X en la ecuación:

$$\begin{aligned}
& X = x+2+k(x)\cdot x^2 \\
\implies\quad & (x^2+1)\big[x+2+x^2k(x)\big] + x^2Y = x+2 \\
\implies\quad & x^2Y = x+2+2(x^2+1)\big(x+2+x^2k(x)\big) \\
\implies\quad & x^2Y = (x+2) + (x+2)(2x^2+2) + x^2k(x)\cdot(2x^2+2) \\
\implies\quad & x^2Y = (x+2)(2x^2) + x^2k(x)\cdot(2x^2+2) \\
\implies\quad & Y = 2(x+2) + (2x^2+2)k(x) \\
\implies\quad & Y = 2x+1-(x^2+1)k(x)
\end{aligned}$$

Por tanto, el conjunto de soluciones a la ecuación es

$$S = \Big\{\Big(x+2+x^2k(x), 2x+1-(x^2+1)k(x)\Big) \text{ t. q. } k(x) \in \mathbb{Z}_3[x]\Big\} \quad \square$$

[32] También se pueden resolver con el algoritmo extendido de Euclides.

Ejercicio: Resolver en el anillo $\mathbb{Z}_7[x]_{x^3+2x^2+2x+1}$ la ecuación
$(3x^2+4)A+3x+1=(2x^2+5)A+x+5$

$$\begin{array}{ll} & (3x^2+4)A+3x+1=(2x^2+5)A+x+5 \\ \Longrightarrow & \big((3x^2+4)-(2x^2+5)\big)A=x+5-(3x+1) \\ \Longrightarrow & (x^2+6)A=5x+4 \end{array}$$

Calculamos el máximo común divisor de los polinomios x^2+6 y x^3+2x^2+2x+1 mediante el algoritmo de Euclides:

$$\big(a_0(x),a_1(x)\big)=(x^3+2x^2+2x+1,x^2+6)=(x^2+6,3x+3)=(3x+3,0)$$

Por tanto, $3x+3$ es un mcd de x^2+6 y x^3+2x^2+2x+1
$\Longrightarrow$ m. c. d$\{x^3+2x^2+2x+1,x^2+6\}=x+1\neq 1 \Longrightarrow \nexists (x^2+6)^{-1}$ en
$\mathbb{Z}_7[x]_{x^3+2x^2+2x+1}$.
Transformamos la ecuación en una congruencia

$(x^2+6)A=5x+4$ en $Z_7[x]_{x^3+2x^2+2x+1} \Longrightarrow (x^2+6)A\equiv 5x+4 \pmod{x^3+2x^2+2x+1}$

Sin embargo, como m. c. d$\{x^3+2x^2+2x+1,x^2+6\}=x+1$ y $(x+1)\nmid(5x+4)$, la congruencia no tiene solución y por tanto la ecuación no tiene solución. $\square$

10.12 Interpolación

Sea K un cuerpo y sean $(\alpha_1,\beta_1),(\alpha_2,\beta_2),\ldots,(\alpha_n,\beta_n)\in K^2$ t. q. $\alpha_1,\alpha_2,\ldots,\alpha_n$ sean todos distintos. La interpolación [33] consiste en hallar un polinomio $a(x)\in K[x]$ t. q.
$a(\alpha_1)=\beta_1,\ a(\alpha_2)=\beta_2,\ldots,\ a(\alpha_n)=\beta_n$.

Teorema 5 (Teorema de Lagrange)**.** Existe un único polinomio $a(x)\in K[x]$ t. q. gr$\big(a(x)\big)<n$ y $a(\alpha_1)=\beta_1,\ a(\alpha_2)=\beta_2,\ldots,\ a(\alpha_n)=\beta_n$. Además, dicho polinomio es el siguiente:

$$a(x)=\beta_1\cdot L_1(x)+\beta_2\cdot L_2(x)+\cdots+\beta_n\cdot L_n(x)$$

donde, para todo $i\in\{1,2,\ldots,n\}$,

$$L_i(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)\Big[(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)\Big]^{-1}$$

Ejercicio: Calcular $a(x)\in\mathbb{Z}_7[x]$ t. q. $a(1)=3,a(2)=0,a(4)=3$.

Por el teorema de Lagrange, sabemos que

$$a(x)=3L_1(x)+0L_2(x)+3L_3(x)$$

es uno de los polinomios que cumplen estas condiciones. Pasamos a calcular $L_1(x)$ y $L_3(x)$ [34]:

$$\begin{cases} L_1(x)=(x-2)(x-4)\Big[(1-2)(1-4)\Big]^{-1}=\ 5(x^2+x+1)\ =5x^2+5x+5 \\ L_2(x)=(x-1)(x-2)\Big[(4-1)(4-2)\Big]^{-1}=6(x^2+4x+2)=6x^2+3x+5 \end{cases}$$

Por tanto, $a(x)=(x^2+x+1)+4(x^2+4x+2)=5x^2+3x+2$ $\square$

[33] Técnicamente, la interpolación polinómica.
[34] $L_2(x)$ no lo calculamos porque viene multiplicado por cero en la expresión.

Método de Newton

Sea K un cuerpo, $(\alpha_1,\beta_1),(\alpha_2,\beta_2),\ldots,(\alpha_n,\beta_n)\in K^2$ t. q. $\alpha_1,\alpha_2,\ldots,\alpha_n$ sean todos distintos y $a(x)\in K[x]$. Entonces la condición de que

$$a(\alpha_1)=\beta_1,\ a(\alpha_2)=\beta_2,\ldots,\ a(\alpha_n)=\beta_n$$

es equivalente a que $a(x)$ sea solución del sistema de congruencias

$$\begin{cases} X\equiv\beta_1 & (\bmod\ x-\alpha_1)\\ X\equiv\beta_2 & (\bmod\ x-\alpha_2)\\ \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots\ \vdots\ \vdots\\ X\equiv\beta_n & (\bmod\ x-\alpha_n)\end{cases}$$

Ejercicio: Calcular todos los polinomios $a(x)\in\mathbb{Z}_7[x]$ t. q. $a(1)=3, a(2)=0, a(4)=3$.

Esto es equivalente a calcular todas las soluciones del sistema

$$\begin{cases} X\equiv 3 \pmod{x-1} & (1)\\ X\equiv 0 \pmod{x-2} & (2)\\ X\equiv 3 \pmod{x-4} & (3)\end{cases}$$

Las soluciones de (1) son obviamente de la forma
$X=3+(x+6)k(x)$ t. q. $k(x)\in\mathbb{Z}_7[x]$. Sustituyendo en (2) tenemos que

$$\begin{aligned} & 3+(x+6)k(x)\equiv 0 \pmod{x-2}\\ \Longrightarrow\quad & (x+6)k(x)\equiv 4 \pmod{x+5}\\ \Longrightarrow\quad & k(x)\equiv 4 \pmod{x+5}\\ \Longrightarrow\quad & k(x)=4+(x+5)m(x)\ \text{ t. q. }\ m(x)\in\mathbb{Z}_7[x]\end{aligned}$$

Por tanto, $k(x)=4+(x+5)m(x)\implies X=3+(x+6)\big(4+(x+5)m(x)\big)$
$\implies X=4x+6+(x+5)(x+6)m(x)$. Sustituimos en (3):

$$\begin{aligned} & 4x+6+(x+5)(x+6)m(x)\equiv 3 \pmod{x-4}\\ \Longrightarrow\quad & (x+5)(x+6)m(x)\equiv 3x+4 \pmod{x+3}\\ \Longrightarrow\quad & (x^2+4x+2)m(x)\equiv 3x+4 \pmod{x+3}\\ \Longrightarrow\quad & 6\cdot m(x)\equiv 2 \pmod{x+3}\\ \Longrightarrow\quad & 6\cdot 6\cdot m(x)\equiv 6\cdot 2 \pmod{x+3}\\ \Longrightarrow\quad & m(x)\equiv 5 \pmod{x+3}\\ \Longrightarrow\quad & m(x)=5+(x+3)n(x)\ \text{ t. q. }\ n(x)\in\mathbb{Z}_7[x]\end{aligned}$$

Por consiguiente,
$m(x)=5+(x+3)n(x)\implies X=4x+6+(x+5)(x+6)\big(5+(x+3)n(x)\big)$
$\implies X=4x+6+5(x+5)(x+6)+(x+3)(x+5)(x+6)n(x)=5x^2+3x+2+(x^3+6)n(x)$
y, en consecuencia, el conjunto de soluciones del sistema es

$$S=\Big\{5x^2+3x+2+(x^3+6)n(x)\ \text{ t. q. }\ n(x)\in\mathbb{Z}_7[x]\Big\}$$

y entonces S es también el conjunto de todos los polinomios que verifican las condiciones del enunciado.

11 EXTRA: Examen ordinario 2024

Esta sección contiene la resolución del examen ordinario de 2024 (el que hizo el prof. José Carlos Rosales, no el del departamento).

Ejercicio 1: Sea $X = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. Sobre $X \times X$ definimos la siguiente relación binaria:

$$(a, b)\ \mathrm{R}\ (c, d) \text{ si } |a - b| = |c - d|$$

a) Demostrar que R es una relación de equivalencia.

b) Calcular $\big[(-2, 3)\big]$.

c) Determinar el cardinal del conjunto cociente $\dfrac{X \times X}{\mathrm{R}}$.

Vamos a empezar demostrando que R es una relación de equivalencia.

- Para todo $(a, b) \in X^2$ se cumple que $|a - b| = |a - b|$. Por tanto $(a, b)\ \mathrm{R}\ (a, b)$ para cualquier $(a, b) \in X^2$ y entonces R cumple la propiedad reflexiva.
- Sean $(a, b), (c, d) \in X^2$ t. q. $(a, b)\ \mathrm{R}\ (c, d) \implies |a - b| = |c - d|$ $\implies |c - d| = |a - b| \implies (c, d)\ \mathrm{R}\ (a, b)$. Por tanto R cumple la propiedad simétrica.
- Sean $(a, b), (c, d), (e, f) \in X^2$ t. q. $(a, b)\ \mathrm{R}\ (c, d)$ y $(c, d)\ \mathrm{R}\ (e, f)$. Entonces $\left.\begin{cases} |a - b| = |c - d| \\ |c - d| = |e - f| \end{cases}\right\} \implies |a - b| = |e - f| \implies (a, b)\ \mathrm{R}\ (e, f)$. Por tanto R cumple la propiedad transitiva.

Como R cumple las propiedades reflexiva, simétrica y transitiva, entonces podemos afirmar que R es una relación de equivalencia.
Pasamos ahora a calcular $\big[(-2, 3)\big]$:

$$\big[(-2, 3)\big] = \Big\{(a, b) \in X^2 \text{ t. q. } (a, b)\ \mathrm{R}\ (-2, 3)\Big\} = \Big\{(a, b) \in X^2 \text{ t. q. } |a - b| = 5\Big\}$$

$$= \Big\{(5, 0), (0, 5), (-5, 0), (0, -5), (4, -1), (-1, 4), (-4, 1), (1, -4), (2, -3), (-3, 2), (-2, 3), (3, -2)\Big\}$$

Para determinar el cardinal del conjunto cociente, vamos a analizar cuántas clases de equivalencia puede haber. Como hemos visto en el apartado anterior, el conjunto $\big[(-2, 3)\big]$ contiene a todos los $(a, b) \in X^2$ para los cuales $|a - b|$ tiene el valor de 5. De manera similar, cada clase de equivalencia sobre R corresponderá a los $(a, b) \in X^2$ tales que $|a - b| = n$ para algún número natural n; y como el mayor valor que puede alcanzar $|a - b|$ t. q. $(a, b) \in X^2$ es 10 (por ejemplo, de la pareja $(5, -5)$), entonces hay una clase de equivalencia para los $(a, b) \in X^2$ tales que $|a - b| = 0$, $|a - b| = 1$, …, $|a - b| = 10$. Podemos afirmar entonces que

$$\#\frac{X^2}{\mathrm{R}} = \#\{0, 1, 2, \ldots, 10\} = 11 \quad \square$$

Ejercicio 2: Calcular todos los números naturales que al dividirlos entre 7 dan de resto 1 y que al expresarlos en base 5 terminan en 312.

Vamos a expresar esto como un sistema de congruencias. Sea $x \in \mathbb{N}$ un número natural que cumple las condiciones del enunciado.

- Si $x \bmod 7 = 1$ entonces es claro que $x \equiv 1 \pmod 7$
- Si x termina en 312 al expresarlo en base 5, entonces al expresarlo en base $5^3 = 125$ terminará en $3 \cdot 5^2 + 1 \cdot 5 + 2 = 82$. Por tanto $x = (a_n, \ldots, a_1, 82)_{125} \implies x = a_n \cdot 125^n + \cdots + a_1 \cdot 125 + 82 =$ $125 \cdot (a_n \cdot 125^{n-1} + \cdots + a_1) + 82 \implies x \equiv 82 \pmod{125}$

Tenemos el siguiente sistema de congruencias: $\begin{cases} x \equiv 1 \pmod 7 & (1) \\ x \equiv 82 \pmod{125} & (2) \end{cases}$.
Claramente las soluciones de (1) son de la forma $1 + 7k$ t. q. $k \in \mathbb{Z}$. Tras sustituir en (2) obtenemos que

$$\begin{aligned} & 1 + 7k \equiv 82 \pmod{125} \\ \Longrightarrow \quad & 7k \equiv 81 \pmod{125} \end{aligned}$$

Como $\text{m. c. d}\{7, 125\} = 1 \mid 81$ entonces la congruencia tiene solución. Si hallamos $u, v \in \mathbb{Z}$ t. q. $7u + 125v = 1$ entonces $(81u) \bmod 125$ será una solución de la congruencia. Usamos el Algoritmo extendido de Euclides:

$$\begin{array}{ccccccccc} (a_0, a_1) & = & (125, 7) & \overset{q=17}{=} & (7, 6) & \overset{q=1}{=} & (6, 1) & \overset{q=6}{=} & (1, 0) \\ (s_0, s_1) & = & (1, 0) & = & (0, 1) & = & (1, -1) & = & (-1, \dots) \\ (t_0, t_1) & = & (0, 1) & = & (1, -17) & = & (-17, 18) & = & (18, \dots) \end{array}$$

El algoritmo nos da la igualdad $7 \cdot 18 - 1 \cdot 125 = 1$, y por tanto
$(18 \cdot 81) \bmod 125 = 1440 \bmod 125 = 83$ es una solución, así que las soluciones (en k) de (2) son de la forma $k = 83 + 125m$ t. q. $m \in \mathbb{Z}$.
Como $x = 1 + 7k$ y $k = 83 + 125m$ entonces $x = 1 + 7(83 + 125m) = 582 + 875m$.
El conjunto de todas las soluciones a la congruencia es

$$S_0 = \left\{ 582 + 875m \text{ t. q. } m \in \mathbb{Z} \right\}$$

Sin embargo, el ejercicio solo nos pide los números *naturales* que son solución del sistema. Por tanto, solo nos quedamos con los valores de m que hacen que $x \in \mathbb{N}$:

$$S = S_0 \cap \mathbb{N} = \left\{ 582 + 875m \text{ t. q. } m \in \mathbb{N} \right\} \quad \square$$

Ejercicio 3: Calcular un elemento α de $\mathbb{Z}_5[x]_{x^4+x+1}$ tal que

$$3x^2(\alpha + 1) = x^3 + 3x^2 + 3x + 3\alpha$$

Vamos a despejar α en la ecuación:

$$\begin{aligned} & 3x^2(\alpha + 1) = x^3 + 3x^2 + 3x + 3\alpha \\ \Longrightarrow \quad & 3x^2\alpha + 3x^2 = x^3 + 3x^2 + 3x + 3\alpha \\ \Longrightarrow \quad & 3x^2\alpha + 2\alpha = x^3 + 3x \\ \Longrightarrow \quad & (3x^2 + 2)\alpha = x^3 + 3x \\ \Longrightarrow \quad & \alpha = (3x^2 + 2)^{-1} \cdot (x^3 + 3x) \end{aligned}$$

Vamos a comprobar que existe el inverso de $3x^2 + 2 \in \mathbb{Z}_5[x]_{x^4+x+1}$, calculando el m.c.d de $3x^2 + 2$ y $x^4 + x + 1$ con el algoritmo de Euclides:

$$\big(a_0(x), a_1(x)\big) = (x^4 + x + 1, 3x^2 + 2) = (3x^2 + 2, x + 2) = (x + 2, 4) = (4, 0)$$

Como 4 es un m.c.d de $3x^2 + 2$ y $x^4 + x + 1$, entonces
$\text{m. c. d}\left\{x^4 + x + 1, 3x^2 + 2\right\} = 1$ y por tanto $\exists (3x^2 + 2)^{-1}$. Para calcularlo hallamos $u(x), v(x) \in \mathbb{Z}_5[x]$ t. q. $(3x^2 + 2)u(x) + (x^4 + x + 1)v(x) = 1$ mediante el algoritmo extendido de Euclides, aprovechando que ya hemos hecho las divisiones.

$$\begin{array}{lcccl}
\big(a_0(x), a_1(x)\big) & = & (x^4+x+1, 3x^2+2) & \overset{q(x)=2x^2+1}{=} & (3x^2+2, x+2) \quad \dots \\
\big(s_0(x), s_1(x)\big) & = & (1,0) & = & (0,1) \quad \dots \\
\big(a_0(x), a_1(x)\big) & = & (0,1) & = & (1, 3x^2+3) \quad \dots
\end{array}$$

$$\begin{array}{lcccl}
\dots & \overset{q(x)=3x+4}{=} & (x+2, 4) & = & (4,0) \\
\dots & = & (1, 2x+1) & = & (2x+1, \dots) \\
\dots & = & (3x^2+3, x^3+3x^2+x+4) & = & (x^3+3x^2+x+4, \dots)
\end{array}$$

El algoritmo nos da la igualdad
$(x^4+x+1)(2x+1)+(3x^2+2)(x^3+3x^2+x+4)=4$
$\implies (x^4+x+1)(3x+4)+(3x^2+2)(4x^3+2x^2+4x+1)=4\cdot 4=1$. Por tanto el inverso de $3x^2+2$ en $\mathbb{Z}_5[x]_{x^4+x+1}$ es $4x^3+2x^2+4x+1$. Finalmente, tenemos que

$$\alpha = (4x^3+2x^2+4x+1)(x^3+3x) = (4x^6+2x^5+x^4+2x^3+2x^2+3x) \bmod (x^4+x+1) = 3x^3+x^2+4 \quad \square$$

Ejercicio 4: Dada la aplicación lineal $f : {\mathbb{Z}_5}^4 \longrightarrow {\mathbb{Z}_5}^3$ definida por

$$f(x,y,z,t) = (x+y+z+t, 2x+y, 3x+2y+z+t)$$

a) ¿Es f un epimorfismo?

b) Calcular el cardinal de $N(f)$

Sabemos que f es un epimorfismo si se cumple que $\mathrm{Im}(f) = {\mathbb{Z}_5}^3$. Vamos a comprobarlo:
Como ${\mathbb{Z}_5}^4 = \Big\langle \big\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\big\} \Big\rangle$, entonces
$\mathrm{Im}(f) = \Big\langle \big\{f(1,0,0,0), f(0,1,0,0), f(0,0,1,0), f(0,0,0,1)\big\} \Big\rangle$
$= \Big\langle \big\{(1,2,3),(1,1,2),(1,0,1),(1,0,1)\big\} \Big\rangle$. Vamos a triangularizar para hallar la dimensión de $\mathrm{Im}(f)$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 4 \\ 0 & 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 4 \\ 0 & 0 & 0 \end{pmatrix} \implies \dim\big(\mathrm{Im}(f)\big) = 2$$

Como $\dim\big(\mathrm{Im}(f)\big) \neq \dim({\mathbb{Z}_5}^3)$, entonces es obvio que $\mathrm{Im}(f) \neq {\mathbb{Z}_5}^3$ y por tanto f no es un epimorfismo. Pasamos ahora a calcular el cardinal de $N(f)$.
Nótese que como f es una aplicación lineal entonces se cumple que $\dim({\mathbb{Z}_5}^4) = \dim\big(\mathrm{Im}(f)\big) + \dim\big(N(f)\big)$. Sabemos que $\dim({\mathbb{Z}_5}^4) = 4$ y $\dim\big(\mathrm{Im}(f)\big) = 2$ y por tanto $\dim\big(N(f)\big) = 2$.
$N(f)$ es un espacio vectorial sobre el cuerpo $\mathbb{Z}_5$ de dimensión 2. Por tanto, $N(f)$ es isomorfo a ${\mathbb{Z}_5}^2$ y por consiguiente $\#N(f) = \#{\mathbb{Z}_5}^2 = 5^2 = 25 \quad \square$

Ejercicio 5: Sea $U = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{array}{c} x+\ y+\ z+t=0 \\ 2x+3y+2z+t=0 \end{array} \right\}$ y W el subespacio de ${\mathbb{Z}_5}^4$ generado por $\big\{(1,1,1,1),(1,2,3,1),(2,1,4,3)\big\}$. Calcular una base de $U \cap W$.

Para ello vamos a calcular las ecuaciones cartesianas de W. Empezamos hallando una base de W:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 4 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 4 & 1 \end{pmatrix}$$

Por tanto, $B_W = \{(1,1,1,1),(0,1,2,0),(0,0,4,1)\}$ es una base de W y $\dim(W) = 3$. Ahora imponemos que

$$\operatorname{rang}\begin{pmatrix}1&0&0&x\\1&1&0&y\\1&2&4&z\\1&0&1&t\end{pmatrix} = 3 \implies \begin{vmatrix}1&0&0&x\\1&1&0&y\\1&2&4&z\\1&0&1&t\end{vmatrix} = 0$$

Calculamos el determinante resultante mediante el desarrollo de Laplace:

$$\begin{vmatrix}1&0&0&x\\1&1&0&y\\1&2&4&z\\1&0&1&t\end{vmatrix} = 1\cdot(-1)^{1+1}\cdot\begin{vmatrix}1&0&y\\2&4&z\\0&1&t\end{vmatrix} + x\cdot(-1)^{1+4}\cdot\begin{vmatrix}1&1&0\\1&2&4\\1&0&1\end{vmatrix} = (4t+2y+4z)+4x\cdot 0 = 2y+4z+4t$$

Por tanto, $W = \{(x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } 2y+4z+4t=0\}$, y entonces $U \cap W = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{array}{r} x+y+z+t=0 \\ 2x+3y+2z+t=0 \\ 2y+4z+4t=0 \end{array} \right\}$. Vamos a ver cuántas de las tres ecuaciones son L.I:

$$\begin{pmatrix}1&1&1&1&0\\2&3&2&1&0\\0&2&4&4&0\end{pmatrix} \sim \begin{pmatrix}1&1&1&1&0\\0&1&0&4&0\\0&2&4&4&0\end{pmatrix} \sim \begin{pmatrix}1&1&1&1&0\\0&1&0&4&0\\0&0&4&1&0\end{pmatrix}$$

Las tres ecuaciones son L.I. Como $U \cap W$ es un subespacio vectorial de ${\mathbb{Z}_5}^4$ dado por 3 ecuaciones L.I, entonces $\dim(U \cap W) = \dim({\mathbb{Z}_5}^4) - 3 = 1$ y entonces una base de $U \cap W$ contiene una solución no nula del sistema $\begin{cases} x+y+z+t=0 \\ y+4t=0 \\ 4z+t=0 \end{cases}$. Claramente la 4-tupla $(x,y,z,t) = (2,1,1,1)$ verifica el sistema y por tanto una base de $U \cap W$ es $B = \{(2,1,1,1)\}$. $\square$

Ejercicio 6: Diagonalizar, en caso de ser posible, la matriz

$$A = \begin{pmatrix}1&2&3&4\\0&2&3&4\\0&0&2&4\\0&0&0&2\end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5)$$

Notemos que A es una matriz triangular, y por tanto sus valores propios son el 1 y el 2 con multiplicidades algebraicas 1 y 3 respectivamente. Como $1+3=4$ (el orden de la matriz A), pasamos a calcular los subespacios vectoriales propios de A.

$$V(1) = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{pmatrix} 0 & 2 & 3 & 4 \\ 0 & 1 & 3 & 4 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$
$$= \left\{ (x,y,z,t) \in {Z_5}^4 \text{ t. q. } \begin{aligned} 2y + 3z + 4t &= 0 \\ y + 3z + 4t &= 0 \\ z + 4t &= 0 \\ t &= 0 \end{aligned} \right\}$$

Vemos cuántas de las ecuaciones son L.I:

$$\begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 1 & 3 & 4 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Como $V(1)$ es un subespacio vectorial de ${\mathbb{Z}_5}^4$ dado por tres ecuaciones L.I, entonces $\dim\big(V(1)\big) = \dim({\mathbb{Z}_5}^4) - 3 = 1$. Además, $B_1 = \big\{(1,0,0,0)\big\}$ es una base de $V(1)$ ya que es una solución no nula del sistema que caracteriza a $V(1)$.

$$V(2) = \left\{ (x,y,z,t) \in {\mathbb{Z}_5}^4 \text{ t. q. } \begin{pmatrix} 4 & 2 & 3 & 4 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$
$$= \left\{ (x,y,z,t) \in {Z_5}^4 \text{ t. q. } \begin{aligned} 4x + 2y + 3z + 4t &= 0 \\ 3z + 4t &= 0 \\ 4t &= 0 \end{aligned} \right\}$$

Como la matriz $\begin{pmatrix} 4 & 2 & 3 & 4 & 0 \\ 0 & 0 & 3 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 \end{pmatrix}$ ya está triangularizada y ninguna de las filas es cero, entonces las tres ecuaciones son L.I. Como $V(2)$ es un subespacio vectorial de ${\mathbb{Z}_5}^4$ dado por 3 ecuaciones L.I, entonces
$\dim\big(V(1)\big) = \dim({\mathbb{Z}_5}^4) - 3 = 1 \neq 3$.
Las multiplicidades geométrica y algebraica del valor propio 2 no coinciden. Por tanto, A no es diagonalizable. $\square$

Ejercicio 7: Tenemos 16 caramelos (todos iguales) que queremos repartir entre cuatro niños de forma que todos los niños tengan al menos un caramelo. ¿De cuántas formas podemos repartirlos?

Si llamamos x, y, z y t al número de caramelos que recibe cada uno de los cuatro niños, entonces una forma cualquiera de repartir los caramelos sería una 4-tupla $(x,y,z,t) \in \mathbb{N}^4$ t. q. $x + y + z + t = 16$.

Sin embargo, como queremos que cada niño reciba al menos un caramelo, entonces le damos un caramelo a cada niño y llamamos x', y', z' y t' al número de caramelos que recibe cada niño, obviando el primer caramelo que le acabamos de dar. Entonces, el número de maneras de repartir los caramelos de modo que cada uno tenga un caramelo como mínimo será

$$\begin{aligned}&\#\Big\{(x',y',z',t')\in\mathbb{N}^4 \ \text{ t. q. } (x'+1)+(y'+1)+(z'+1)+(t'+1)=16\Big\}\\&=\#\Big\{(x',y',z',t')\in\mathbb{N}^4 \ \text{ t. q. } x'+y'+z'+t'=12\Big\}\end{aligned}$$

Y el cardinal de este conjunto lo podemos calcular mediante combinaciones con repetición:

$$\#\Big\{(x',y',z',t')\in\mathbb{N}^4 \ \text{ t. q. } x'+y'+z'+t'=12\Big\}=\mathrm{C}^R_{4,12}=\binom{15}{12}=455 \quad \square$$