Matemática II – 2019

Capitán Sarmiento
Alejandro Díaz-Caro

versión 2019-03-18

Sobre la materia

Contenidos y cronograma

Fechas	**Temas**
18 de marzo	Sistemas de ecuaciones lineales
25 de marzo	Matrices (Suma, producto, inversa)
1ro de abril	Determinante, Rango, Rouché-Forbenius
8 de abril	Aritmética entera
15 de abril	Aritmética modular
22 de abril	Repaso
29 de abril	*Consulta*
6 de mayo	**Primer parcial**
13 de mayo	Estructuras algebraicas
20 de mayo	Morfismos
27 de mayo al 3 de junio	Espacios vectoriales
10 de junio	*Consulta*
17 de junio	**Segundo parcial**
24 de junio	*Consulta*
1ro de julio	**Recuperatorio**
15 de julio	*Integrador*

Bibliografía

Sistemas de ecuaciones lineales y matrices
J. Stweart, L. Redlin, S. Watson, Precálculo, 5ta ed., Cengage Learning Editores, 2007 (Secciones 9.1 a 9.7)

Aritmética entera y modular
R. Grimaldi, Matemáticas discreta y combinatoria: una introducción con aplicaciones, 3ra ed., Addison-Wesley, 1997 (Secciones 4.3 y 14.3)

Magma, monoides, semigrupos, grupos e isomorfismos
J. Fraleígh, Álgebra abstracta, primer curso, Addison-Wesley, 1988 (Parte 1)

Espacios vectoriales
J. de Burgos, Álgebra lineal, 3ra ed., Mc Graw Hill, 2006 (Secciones 5.1 a 5.3, 5.6 y apéndices 7 y 8)

Índice general

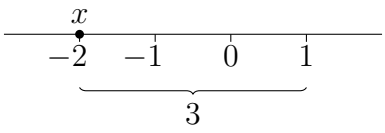
Capítulo 1

Sistemas de ecuaciones lineales y matrices

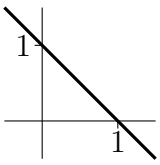
1.1. Sistemas de ecuaciones

1.1.1. Definiciones

La ecuación $x + 3 = 1$ se puede representar gráficamente de la siguiente manera:



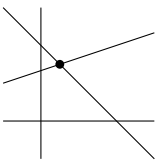
La ecuación $x + y = 1$, o, lo que es lo mismo, $y = 1 - x$, representa una recta en el plano:



Si pedimos a la vez los valores de x e y que satisfacen dos ecuaciones, obtenemos:

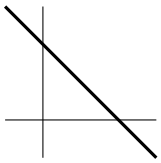
- Un punto, si las rectas se interceptan en un punto:

$$\begin{cases} x + y &= 1 \\ x - 3y &= -2 \end{cases}$$



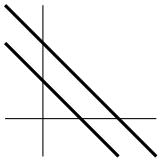
- Una recta, si ambas ecuaciones representan la misma recta.

$$\begin{cases} x + y &= 1 \\ 2x + 2y &= 2 \end{cases}$$



- Ninguna solución, si se trata de rectas paralelas.

$$\begin{cases} x + y &= 1 \\ 2x + 2y &= 1 \end{cases}$$



Si tenemos tres ecuaciones con tres incógnitas, tendremos:

- Un punto
- Una recta o un plano
- Nada

Es decir, siempre las soluciones posibles son una única, infinitas, o ninguna, y esas son todas las posibilidades.

1.1.2. Resolución directa

La técnica de *resolución directa* consiste en despejar una variable en una ecuación, y luego reemplazarla en otra ecuación. En la segunda, se tendrá una variable menos. Luego se repite en la tercera ecuación, etc.

Ejemplo 1.

$$\begin{cases} x + y + z = 1 & \text{(1.1a)} \\ x + 2y = 1 & \text{(1.1b)} \\ x + y + 2z = 2 & \text{(1.1c)} \end{cases}$$

De (1.1a) despejamos x y obtenemos

$$x = 1 - y - z \tag{1.2}$$

Reemplazamos (1.2) en (1.1b), y despejamos y:

$$\begin{aligned} \overbrace{(1 - y - z)}^{x} + 2y &= 1 \\ 1 + y - z &= 1 \\ y &= 1 - 1 + z \\ y &= z \end{aligned} \tag{1.3}$$

Reemplazamos (1.2) y (1.3) en (1.1c), y despejamos z:

$$\overbrace{(1-\underbrace{z}_{y}-z)}^{x}+\overbrace{z}^{y}+2z=2$$

$$\begin{aligned} 1-2z+3z &= 2 \\ 1+z &= 2 \\ z &= 1 \end{aligned} \tag{1.4}$$

Con (1.4) en (1.3), obtenemos

$$y = 1 \tag{1.5}$$

Y con (1.4) y (1.5) en (1.2), obtenemos

$$x = 1-1-1 = -1$$

Es decir, la solución es el punto $(-1, 1, 1)$.

1.1.3. Método de Gauss

El método de Gauss es el siguiente:

1. El primer paso es dividir la ecuación por el valor necesario para que el coeficiente de la primer variable sea 1.

2. El segundo paso es restar a veces la primer ecuación por la segunda, siendo a el coeficiente que acompaña a la primer variable. Luego restamos a' veces la primer ecuación por la segunda, siendo a' el coeficiente que acompaña a la primer variable. Repetimos hasta llegar a la última ecuación.

3. Nos olvidamos de la primer ecuación, y repetimos los pasos 1 y 2 sobre el resto de las ecuaciones hasta que no queden más ecuaciones.

4. Invertimos el orden: restamos b veces la última ecuación a la ante última, siendo b el coeficiente que acompaña a la última variable de la ante última ecuación. Repetimos de la misma manera hasta llegar a la primera ecuación.

Ejemplo 2. Retomamos el ejemplo anterior.

$$\left\{\begin{array}{rcrcl} x+ & y+ & z & = & 1 \\ x+ & 2y & & = & 1 \\ x+ & y+ & 2z & = & 2 \end{array}\right. \xrightarrow{e2-e1} \left\{\begin{array}{rcrcl} x+ & y+ & z & = & 1 \\ & y- & z & = & 0 \\ x+ & y+ & 2z & = & 2 \end{array}\right. \xrightarrow{e3-e1} \left\{\begin{array}{rcrcl} x+ & y+ & z & = & 1 \\ & y- & z & = & 0 \\ & & z & = & 1 \end{array}\right.$$

$$\xrightarrow{e2+e3} \left\{\begin{array}{rcrcl} x+ & y+ & z & = & 1 \\ & y & & = & 1 \\ & & z & = & 1 \end{array}\right. \xrightarrow{e1-e3} \left\{\begin{array}{rcrcl} x+ & y & & = & 0 \\ & y & & = & 1 \\ & & z & = & 1 \end{array}\right. \xrightarrow{e1-e2} \left\{\begin{array}{rcrcl} x & & & = & -1 \\ & y & & = & 1 \\ & & z & = & 1 \end{array}\right.$$

El siguiente es un ejemplo de un sistema sin solución.

Ejemplo 3.

$$\left\{\begin{array}{rcrcr} 2x+&y&&=&-1\\ x+3y-&z&=&&1\\ 2x+6y-2z&&=&&1\end{array}\right. \overset{e1/2}{\longrightarrow} \left\{\begin{array}{rcrcr} x+\frac{1}{2}y&&&=&-\frac{1}{2}\\ x+3y-&z&=&&1\\ 2x+6y-2z&&=&&1\end{array}\right. \overset{e2-e1}{\longrightarrow} \left\{\begin{array}{rcrcr} x+\frac{1}{2}y&&&=&-\frac{1}{2}\\ \frac{5}{2}y-&z&=&&\frac{3}{2}\\ 2x+6y-2z&&=&&1\end{array}\right.$$

$$\overset{e3-2e1}{\longrightarrow} \left\{\begin{array}{rcrcr} x+\frac{1}{2}y&&&=&-\frac{1}{2}\\ \frac{5}{2}y-&z&=&&\frac{3}{2}\\ 5y-2z&&=&&2\end{array}\right. \overset{\frac{2}{5}e2}{\longrightarrow} \left\{\begin{array}{rcrcr} x+\frac{1}{2}y&&&=&-\frac{1}{2}\\ y-\frac{2}{5}z&=&&&\frac{3}{5}\\ 5y-2z&=&&&2\end{array}\right. \overset{e3-5e2}{\longrightarrow} \left\{\begin{array}{rcrcr} x+\frac{1}{2}y&&&=&-\frac{1}{2}\\ y-\frac{2}{5}z&=&&&\frac{3}{5}\\ 0&=&&&-1\end{array}\right.$$

Hemos terminado en una ecuación imposible: $0 = -1$, lo cual significa que el sistema no tiene solución, o que es *incompatible*.

El siguiente es un ejemplo de un sistema con múltiples soluciones.

Ejemplo 4.

$$\left\{\begin{array}{rcrcr} x+&y+&z&=&\frac{1}{2}\\ x+&y&&=&3\\ 2x+2y+2z&&&=&1\end{array}\right. \overset{e2-e1}{\longrightarrow} \left\{\begin{array}{rcrcr} x+&y+&z&=&\frac{1}{2}\\ &-&z&=&\frac{5}{2}\\ 2x+2y+2z&&&=&1\end{array}\right. \overset{e3-2e1}{\longrightarrow} \left\{\begin{array}{rcrcr} x+y+z&&&=&\frac{1}{2}\\ &-&z&=&\frac{5}{2}\\ 0&&&=&0\end{array}\right.$$

$$\overset{-e2}{\longrightarrow} \left\{\begin{array}{rcrcr} x+y+z&&&=&\frac{1}{2}\\ &&z&=&-\frac{5}{2}\\ 0&&&=&0\end{array}\right. \overset{e1-e2}{\longrightarrow} \left\{\begin{array}{rcrcr} x+y&&&=&3\\ &&z&=&-\frac{5}{2}\\ 0&&&=&0\end{array}\right.$$

Las infinitas soluciones son las del conjunto

$$\{(x,y,z) \mid x+y=-2 \wedge z=-\tfrac{5}{2}\} \quad = \quad \{(x,-2-x,-\tfrac{5}{2}) \mid x \in \mathbb{R}\}$$

1.2. Matrices

1.2.1. Definición

Definición 1.2.1. Una matriz es un arreglo bidimensional de números ordenados en filas y columnas. Una matriz de n filas y m columnas, se dice que es una matriz de $n \times m$. Al conjunto de matrices de $n \times m$ se lo denota por $\mathbb{M}_{n\times m}$.

Ejemplo 5.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4{,}1 & 5 & 6 \end{pmatrix} \in \mathbb{M}_{2\times 3} \qquad B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix} \in \mathbb{M}_{1\times 5}$$

El elemento a_{23} de A es 6. A veces escribimos $A = (a_{ij})$ para darle un nombre a los elementos.

1.2.2. Operaciones

Suma

La operación de suma entre matrices se define como la operación

$$+ : \mathbb{M}_{n\times m} \times \mathbb{M}_{n\times m} \longrightarrow \mathbb{M}_{n\times m}$$

tal que $A + B = C$ con $A = (a_{ij})$, $B = (b_{ij})$ y $C = (a_{ij} + b_{ij})$.

Ejemplo 6.

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

Ejercicio. Sean

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 3 & 2 & 1 \\ 2 & 3 & 2 \\ 2 & 0 & 4 \end{pmatrix} \qquad \text{y} \qquad B = \begin{pmatrix} 0 & 1 & 4 \\ 1 & 4 & 0 \\ 2 & 1 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

Calcular $A + B$.

Propiedades.

$A + B = B + A$	Conmutatividad
$(A + B) + C = A + (B + C)$	Asociatividad
$A + 0 = 0 + A = A$	Existencia de elemento neutro
$A + (-A) = 0$	Existencia de inverso

Donde

$$0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

Producto por escalar

La operación de producto por escalar se define como la operación

$$. : \mathbb{R} \times \mathbb{M}_{n\times m} \longrightarrow \mathbb{M}_{n\times m}$$

tal que $\lambda A = B$ con $\lambda \in \mathbb{R}$, $A = (a_{ij})$ y $B = (\lambda a_{ij})$.

Ejemplo 7.

$$2\begin{pmatrix} 1 & 8 & -3 \\ 4 & -2 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 16 & -6 \\ 8 & -4 & 12 \end{pmatrix}$$

Ejercicio. Calcular

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

Propiedades.

$(\lambda\mu)A = \lambda(\mu A)$	Asociatividad
$\lambda(A + B) = \lambda A + \lambda B$	Distributividad respecto a suma de matrices
$(\lambda + \mu)A = \lambda A + \mu A$	Distributividad respecto a suma de escalares
$1A = A$	Existencia de elemento neutro

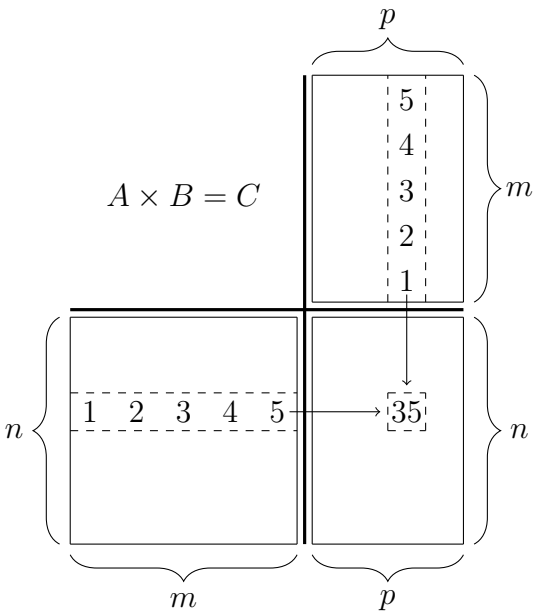
Producto de matrices

La operación de producto de matrices se define como la operación

$$\times : \mathbb{M}_{n\times m} \times \mathbb{M}_{m\times p} \longrightarrow \mathbb{M}_{n\times p}$$

tal que $A \times B = C$ con $A = (a_{ik})$, $B = (b_{kj})$ y $C = (\sum_{k=1}^{m} a_{ik}b_{kj})$.

Método sencillo de cálculo



$$1 \times 5 + 4 \times 2 + 3 \times 3 + 2 \times 4 + 1 \times 5 = 35$$

Ejemplo 8. Calcular $A \times B$ con

$$A = \begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 1 \end{pmatrix} \qquad y \qquad B = \begin{pmatrix} 5 & 1 \\ 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{array}{c|c} & \begin{pmatrix} 5 & 1 \\ 2 & 1 \\ 1 & 0 \end{pmatrix} \\ \hline \begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 7 & 1 \\ 2 & 2 \end{pmatrix} \end{array}$$

Ejercicio. Calcular $A \times B$ con

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \qquad y \qquad B = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$$

Observación. Muchas veces vamos a omitir el símbolo $\times$, escribiendo AB en lugar de $A \times B$.

Propiedades.

$A(BC) = (AB)C$	Asociatividad
$(A+B)C = AC + BC$	Distributividad a derecha respecto a la suma
$A(B+C) = AB + AC$	Distributividad a izquierda respecto a la suma
$(\lambda A)B = \lambda(AB) = A(\lambda B)$	Asociatividad y conmutatividad con escalares

Observación. **El producto de matrices no es conmutativo**

Ejemplo 9.

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

Definición 1.2.2. A la matriz $I_n = (\iota_{ij}) \in \mathbb{M}_{n\times n}$ tal que $\iota_{ii} = 1$ y $\iota_{ij} = 0$ si $i \neq j$, se le llama *matriz identidad*. A veces escribimos sólo I cuando la dimensión de la matriz es evidente.

Teorema 1.2.1. Para toda matriz $A \in \mathbb{M}_{n\times n}$, $AI_n = I_nA = A$.

Inversa

La inversa de una matriz $A \in \mathbb{M}_{n\times n}$, denotada A^{-1}, es la matriz tal que

$$AA^{-1} = A^{-1}A = I_n$$

Donde

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Observación. **No toda matriz tiene inversa**. Que A sea una matriz cuadrada es una condición necesaria para la existencia de la inversa

Ejemplo 10.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad A^{-1} \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$$

Método para calcular la inversa: Gauss o método del testigo

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \xrightarrow{l_2-3l_1} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right) \xrightarrow{l_2/-2} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & 3/2 & -1/2 \end{array}\right) \xrightarrow{l_1-2l_2} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & 3/2 & -1/2 \end{array}\right)$$

Propiedades.

1. Si una matriz tiene inversa, es única
2. $(AB)^{-1} = B^{-1}A^{-1}$
3. $(A^{-1})^{-1} = A$
4. $(\lambda A)^{-1} = \lambda^{-1}A^{-1}$

Demostración. 1. Supongamos que B y C son inversas de A. Entonces,

$$AB = BA = I$$
$$AC = CA = I$$

Por lo tanto, $B = BI = B(AC) = (BA)C = IC = C$.

2. $AB(B^{-1}A^{-1}) = A(BB^{-1}A^{-1} = AIA^{-1} = AA^{-1} = I$
   $(B^{-1}A^{-1})AB = B^{-1}(A^{-1}A)B = B^{-1}IB = B^{-1}B = I.$
3. $(A^{-1})^{-1} = A$ porque $A^{-1}A = AA^{-1} = I$.
4. $\lambda A(\lambda^{-1}A^{-1}) = A(\lambda\lambda^{-1}A^{-1}) = AA^{-1} = I$
   $(\lambda^{-1}A^{-1})\lambda A = A^{-1}(\lambda^{-1}\lambda A) = A^{-1}A = I.$ □

Ejemplo 11. Algunas matrices que no tienen inversa

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 2 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix} \quad \begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 2 & 4 & 6\end{pmatrix}$$

Ejercicios.

1. Calcular la inversa de estas matrices (cuando sea posible)

   a) $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$ *b*) $\begin{pmatrix}a & 1\\ 2 & 3\end{pmatrix}$

2. Resolver la siguiente ecuación (deducir X): $AX = B$, con

$$A = \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix}-4 & 6\\ 3 & -3\end{pmatrix}$$

3. Calcular la inversa cuando sea posible

   a) $\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$ *c*) $\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 0 & 1 & 0\end{pmatrix}$ *e*) $\begin{pmatrix}1 & 0 & 1\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}$

   b) $\begin{pmatrix}1 & 0 & 1\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$ *d*) $\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}$ *f*) $\begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}$

1.3. Matrices y sistemas de ecuaciones

1.3.1. Determinante

El determinante de una matriz es un número nos permite saber si ésta tiene inversa o no. Si el determinante es 0, la matriz no tiene inversa.

Definición 1.3.1. Notamos $A_{/ij}$ a la matriz A donde se ha eliminado la fila i y la columna j.

Ejemplo 12. Si $A = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix}$ $A_{/23} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$

Definición 1.3.2 (Determinante)**.** El determinante de una matriz $A \in \mathbb{M}_n$ se define recursivamente sobre n:
Si $n = 1$, entonces $|A| = a_{11}$.
Si $n > 1$, entonces $|A| = \sum_{k=1}^{n} (-1)^{k+1} a_{1k} |A_{/1k}|$.

Ejemplo 13.

1. $\begin{vmatrix} 2 & 3 \\ -1 & 2 \end{vmatrix} = 2 \times 2 - 3 \times (-1) = 7$
2. $\begin{vmatrix} 2 & 3 & 0 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \end{vmatrix} = 2 \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} - 3 \begin{vmatrix} 0 & 2 \\ 3 & 5 \end{vmatrix} + 0 \begin{vmatrix} 0 & 1 \\ 3 & 4 \end{vmatrix} = 2 \times (1 \times 5 - 2 \times 4) - 3 \times (0 \times 5 - 2 \times 3) + 0 = 12$

Ejercicios. Calcular el determinante de:

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

Propiedades.

1. $|A| = 0$ si:
   - Posee 2 filas o columnas iguales.
     Ejemplo 14.
     $$\begin{pmatrix} 2 & 3 & 2 \\ 3 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix}$$
   - Todos los elementos de una fila son nulos.
     Ejemplo 15.
     $$\begin{pmatrix} 2 & 3 & 2 \\ 3 & 2 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

- Los elementos de una fila son combinación lineal de otras.
  Ejemplo 16.
  $$\begin{pmatrix} 2 & 3 & 2 \\ 1 & 2 & 4 \\ 3 & 5 & 6 \end{pmatrix}$$
  (notar que $l3 = l1 + l2$).

2. Si a una matriz se cambia el orden de 2 filas o columnas, su determinante sólo cambia de signo:
   Ejemplo 17.
   $$\begin{vmatrix} 2 & 1 & 2 \\ 1 & 2 & 0 \\ 3 & 5 & 6 \end{vmatrix} = - \begin{vmatrix} 1 & 2 & 0 \\ 2 & 1 & 2 \\ 3 & 5 & 6 \end{vmatrix}$$

3. $|AB| = |A||B|$.

Teorema 1.3.1. $\exists A^{-1}$ sí y sólo sí $|A| \neq 0$.

1.3.2. Rango

Definición 1.3.3. Una línea de una matriz es *linealmente dependiente* de otras si es posible obtenerla como una combinación lineal de las otras. Caso contrario, es *linealmente independiente*.

Ejemplo 18. En la matriz
$$\begin{pmatrix} 2 & 3 & 2 \\ 1 & 2 & 4 \\ 3 & 5 & 6 \end{pmatrix}$$
la línea 3 es linealmente dependiente de las líneas 1 y 2. La línea 1 es linealmente independiente de la línea 2 o de la línea 3, en cambio es linealmente dependiente de ambas.

Definición 1.3.4 (Rango)**.** El rango de una matriz es el número de líneas linealmente independientes de las demás.

Cálculo del rango. El rango se obtiene con el método de Gauss: el número de escalones al final del método es el rango.

Ejemplo 19. Sea $A = \begin{pmatrix} 2 & 3 & 2 \\ 1 & 2 & 4 \\ 3 & 5 & 6 \end{pmatrix}$. Calculamos el rango con ayuda del método de Gauss:

$$\begin{pmatrix} 2 & 3 & 2 \\ 1 & 2 & 4 \\ 3 & 5 & 6 \end{pmatrix} \xrightarrow{l_1/2} \begin{pmatrix} 1 & 3/2 & 1 \\ 1 & 2 & 4 \\ 3 & 5 & 6 \end{pmatrix} \xrightarrow{l_2 - l_1} \begin{pmatrix} 1 & 3/2 & 1 \\ 0 & 1/2 & 3 \\ 3 & 5 & 6 \end{pmatrix} \xrightarrow{l_3 - 3l_1} \begin{pmatrix} 1 & 3/2 & 1 \\ 0 & 1/2 & 3 \\ 0 & 1/2 & 3 \end{pmatrix} \xrightarrow{2l_2} \begin{pmatrix} 1 & 3/2 & 1 \\ 0 & 1 & 6 \\ 0 & 1/2 & 3 \end{pmatrix}$$

$$\xrightarrow{l_3 - l_2/2} \begin{pmatrix} 1 & 3/2 & 1 \\ 0 & 1 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

$\therefore r(A) = 2$

Ejercicio. Calcular el rango de la siguiente matrices:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & 0 & 2 \end{pmatrix}$$

Teorema 1.3.2. $A \in \mathbb{M}_{n\times n} \Rightarrow r(A) \leq n$.

Teorema 1.3.3. $A \in \mathbb{M}_{n\times n}$ invertible $\Leftrightarrow r(A) = n$.

1.3.3. Teorema de Rouché-Frobenius

Considerar el siguiente sistema de ecuaciones:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \vdots & \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n \end{cases}$$

Describimos el sistema mediante la matriz

$$(A|b) = \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \dots & a_{nn} & b_n \end{array}\right)$$

que se obtiene por la yuxtaposición de $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ y $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.
A la matriz A se la llama *matriz incompleta* y a la matriz $(A|b)$ *matriz completa.*

Teorema 1.3.4 (Rouché-Forbenius)**.** Existen soluciones para un sistema de ecuaciones sí y sólo sí el rango de la matriz completa asociada es igual al rango de la matriz incompleta. Más aún, si $A \in \mathbb{M}_{n\times n}$ y $r(A) = n$, entonces la solución es única, en otro caso, existen infinitas soluciones.

Ejemplo 20.

$$\begin{cases} 2x + y &= 3 \\ x + 2y &= 1 \end{cases}$$

$$\left(\begin{array}{cc|c} 2 & 1 & 3 \\ 1 & 2 & 1 \end{array}\right) \xrightarrow{l_1/2} \left(\begin{array}{cc|c} 1 & 1/2 & 3/2 \\ 1 & 2 & 1 \end{array}\right) \xrightarrow{l_2-l_1} \left(\begin{array}{cc|c} 1 & 1/2 & 3/2 \\ 0 & 3/2 & -1/2 \end{array}\right) \xrightarrow{2l_2/3} \left(\begin{array}{cc|c} 1 & 1/2 & 3/2 \\ 0 & 1 & -1/3 \end{array}\right)$$

$$r(A) = r(A|b) = 2$$

Por lo tanto existe una única solución al sistema.

Ejercicio. Utilizar el Teorema 1.3.4 para determinar el número de soluciones de cada uno de los siguientes sistemas de ecuaciones.

$$\begin{cases} 2x + y = 3 \\ 4x + 2y = 1 \end{cases} \qquad \begin{cases} 2x + 3y = 3 \\ y + 2z = 1 \\ 3x + 4y + 5z = 0 \end{cases}$$

Observación. Al segundo sistema del ejercicio anterior lo podemos escribir como $AX = B$, con

$$A = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix} \qquad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \qquad B = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$$

ya que $AX = \begin{pmatrix} 2x+3y \\ y+2z \\ 3x+4y+5z \end{pmatrix}$.

Por lo tanto, si A es invertible, es decir, si su rango es 3 (ver Teorema 1.3.3), y el sistema tiene una única solución, es decir, el rango de la matriz completa $(A|B)$ también es 3 (ver Teorema 1.3.4), entonces la solución al sistema es $X = A^{-1}B$.

1.4. Ejercicios del capítulo

1.1. Hallar el conjunto de soluciones de los siguientes sistemas de ecuaciones lineales:

$$\begin{cases} x + y + 2z = 5 \\ x - y - z = 0 \\ x + z = 3 \end{cases} \quad \begin{cases} x + y - z = 0 \\ x - y = 0 \\ x + y + z = 0 \end{cases} \quad \begin{cases} x + 3y + 2z = 1 \\ 2x - 2y = 2 \\ x + y + z = 2 \end{cases}$$

$$\begin{cases} 2x + y + z = 3 \\ 3x - y - 2z = 0 \\ x + y - z = -2 \\ x + 2y + z = 0 \end{cases} \quad \begin{cases} 2x + y + z = 3 \\ 3x - y - 2z = 0 \\ x + y - z = -2 \\ x + 2y - z = 0 \end{cases}$$

$$\begin{cases} x + y + z = 3 \\ x - y - z = 4 \end{cases} \quad \begin{cases} x + y + z = 3 \\ 5x + 5y + 5z = 4 \end{cases} \quad \begin{cases} x - y - z = -7 \\ 2x + y = 5 \\ -3x + z = 2 \end{cases}$$

$$\begin{cases} x - 2y + 3z = 0 \\ 2x + 3y - z = 0 \\ 3x + y + 2z = 0 \end{cases} \quad \begin{cases} x + 2y + 3z = 4 \\ x + 4y + 9z = 16 \\ x + 8y + 27z = 64 \end{cases} \quad \begin{cases} x + 2y + z = 2 \\ 3x - 2y - z = 5 \\ 2x - 5y + 3z = -4 \\ x + 4y + 6z = 0 \end{cases}$$

1.2. Resolver los siguientes sistemas en función de a, b y c:

$$\begin{cases} x + (a+1)y = a+2 \\ ax + (a+4)y = 8 \end{cases} \quad \begin{cases} ax + (a-1)y = a+2 \\ (a+1)x - ay = 5a+3 \end{cases}$$

$$\begin{cases} ax + y + z = 1 \\ x + ay + z = 1 \\ x + y + az = 1 \end{cases} \quad \begin{cases} x + ay + 2z = 3 \\ x + 2ay + 2z = 4 \\ x + 2y + az = 2 \end{cases} \quad \begin{cases} x + y + z = a \\ x - y \quad b \\ x \quad + z + c = \end{cases}$$

1.3. Resolver los siguientes sistemas (en función de a, sólo cuando sea necesario):

$$\begin{cases} x + y = 0 \\ x - y = 2a \\ x - 2y = 1 \end{cases} \quad \begin{cases} x - y = 2a \\ x - 2y = 1 \end{cases} \quad \begin{cases} x + y = 0 \\ x - 2y = 1 \end{cases} \quad \begin{cases} x + y = 0 \\ x - y = 2a \end{cases}$$

1.4. Realizar todos los productos posibles de dos matrices entre las siguientes:

$$A = \begin{pmatrix} 4 & 6 & 3 & 0 \\ 7 & 1 & 0 & 6 \\ 2 & 1 & 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 4 & 0 \\ 3 & 6 \\ 2 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 0 & 1 \end{pmatrix}$$

$$D = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \qquad Y = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

1.5. Sean $A = \begin{pmatrix} 2 & 1 \\ 4 & 7 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Calcular A^2, B^2, $(A+B)^2$, AB y BA.

Dar una explicación intuitiva de porqué $(A+B)^2 \neq A^2 + 2AB + B^2$.

1.6. Determinar si las siguientes matrices son invertibles o no.

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

1.7. Calcular, si existen, las inversas de las siguientes matrices (utilizando el método del testigo):

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix} \qquad C = \begin{pmatrix} 2 & 0 & 4 \\ 6 & 1 & 7 \\ 5 & 3 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 5 & 9 \\ 1 & 2 & 4 \end{pmatrix}$$

Dar el rango de cada matriz.

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

a) Calcular A^3.

b) Utilizando el punto 1.8.*a* deducir si A es inversible o no (y si lo es calcular su inversa) sin utilizar el determinante ni el método del testigo.

c) Calcular lo mismo que en el punto 1.8.*b* con el determinante y el método del testigo.

1.9. Sea $A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$. Calcular $A^3 - 2A^2$ y deducir A^{-1} en función de A.

1.10. Sean $A = \begin{pmatrix} 1 & m & 2 \\ 1 & 2m & 2 \\ 1 & 2 & m \end{pmatrix}$, con $m \in \mathbb{R}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ y $B = \begin{pmatrix} 3 \\ 4 \\ 3 \end{pmatrix}$.

a) Resolver el sistema $AX = B$ en función de m.

b) Determinar para qué valores de m la matriz A es invertible.

c) Calcular el rango de A en función de m.

1.11. Sea el sistema lineal $AX = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

a) Aprovechar la estructura particular de A para resolver el sistema directamente. Deducir de la solución obtenida la expresión de la inversa de A.

b) Calcular A^{-1} con el método de la matriz testigo.

1.12. Considerar el siguiente sistema:

$$\begin{cases} x + y + z = a \\ x - y \quad\; = b \\ \quad\; y + z = c \end{cases}, \quad (a, b, c) \in \mathbb{R}^3$$

a) Escribir el sistema en la forma matricial $AX = B$.

b) Resolver utilizando el método de Gauss (en función de a, b, y c).

c) Determinar la inversa de A.

1.13. Considerar el siguiente sistema lineal:

$$\begin{cases} x + \;\; y + \;\; z = 4 \\ x + 2y + 2z = 5 \\ x + \;\; y \quad\;\; = 6 \end{cases}$$

a) Resolver con el método de Gauss.

b) Escribir el sistema en la forma matricial $AX = B$.

c) Calcular la inversa de A.

d) Calcular nuevamente el resultado, con ayuda de la inversa.

Capítulo 2

Aritmética entera y modular

2.1. Aritmética entera

2.1.1. Divisores

El conjunto de números enteros es el conjunto $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Los números naturales ($\mathbb{N}$) son un subconjunto de los enteros (son los *enteros positivos*).

Definición 2.1.1. Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b *divide* a a (notación $b \mid a$) si existe $n \in \mathbb{Z}$ tal que $a = bn$.
Alternativamente podemos decir que b *es divisor de* a o que a *es múltiplo de* b.

Propiedades. Para cualquier $a, b \in \mathbb{Z}$,

1. $1 \mid a$ y $a \mid 0$.
2. $[(a \mid b) \wedge (b \mid a)] \implies a = \pm b$
3. $[(a \mid b) \wedge (b \mid c)] \implies a \mid c$
4. $a \mid b \implies a \mid bx$ para todo $x \in \mathbb{Z}$
5. Si $x = y + z$, con $x, y, z \in \mathbb{Z}$ y a divide a dos de los enteros x, y y z, entonces a divide al entero restante.
6. $[(a \mid b) \wedge (a \mid c)] \implies a \mid (bx + cy)$ para todos $x, y \in \mathbb{Z}$.
   (La expresión $bx + cy$ se denomina *combinación lineal de* b *y* c).
7. Para $1 \leq i \leq n$, sea $c_i \in \mathbb{Z}$. Si a divide a cada c_i, entonces, $a \mid (c_1x_1 + \cdots + c_nx_n)$ con $x_i \in \mathbb{Z}$ para $i = 1, \dots, n$.

Demostración.

1. $a = 1a$, por lo tanto $1 \mid a$ para cualquier a. $0 = a0$, por lo tanto $a \mid 0$ para cualquier a.
2. Si $a \mid b$ y $b \mid a$, entonces existen $n_1, n_2 \in \mathbb{Z}$ tales que $b = an_1$ y $a = bn_2$. Por lo tanto, $b = an_1 = (bn_2)n_1$, lo que significa que $n_2n_1 = 1$, y como ambos son enteros, $n_1 = n_2 = 1$ o $n_1 = n_2 = -1$. Es decir, $a = \pm b$.

3. Si $a \mid b$ y $b \mid c$, entonces existen $n_1, n_2 \in \mathbb{Z}$ tales que $b = an_1$ y $c = bn_2$. Es decir, $c = (an_1)n_2 = a(n_1n_2)$. Por lo tanto, $a \mid c$.

4. Si $a \mid b$, entonces $b = an$, lo que implica que $bx = (an)x = a(nx)$, por lo tanto $a \mid bx$.

5. Veamos todos los casos:

   - $a \mid x$ y $a \mid y$, es decir, $x = an_1$ e $y = an_2$. Entonces $an_1 = an_2 + z \implies z = an_1 - an_2 \implies z = a(n_1 - n_2)$. Por lo tanto $a \mid z$.
   - $a \mid y$ y $a \mid z$, es decir, $y = an_1$ y $z = an_2$. Entonces $x = an_1 + an_2 = a(n_1 + n_2)$, por lo tanto $a \mid x$.
   - $a \mid x$ y $a \mid z$, es decir $x = an_1$ y $z = an_2$. Entonces $an_1 = y + an_2 \implies y = an_1 - an_2 \implies y = a(n_1 - n_2)$, por lo tanto $a \mid y$.

6. Si $a \mid b$ y $a \mid c$, entonces $b = an_1$ y $c = an_2$. Entonces, $bx + cy = an_1x + an_2y \implies bx + cy = a(n_1x + n_2y)$, por lo tanto $a \mid bx + cy$.

7. Si $a \mid c_i$ para $i = 1, \ldots, n$, entonces, $c_i = an_i$. Entonces $c_1x_1 + \cdots + c_nx_n = an_1x_1 + \cdots + an_nx_n \implies c_1x_1 + \cdots + c_nx_n = a(n_1x_1 + \cdots + n_nx_n)$, por lo tanto $a \mid (c_1x_1 + \cdots + c_nx_n)$. □

Ejemplo 21. ¿Existen enteros x, y y z tales que $6x + 9y + 15z = 107$?
Supongamos que existen dichos enteros. Como $3 \mid 6$, $3 \mid 9$ y $3 \mid 15$, la propiedad 7. dice que $3 \mid 107$, lo cual es falso, por lo tanto no existen tales enteros.

2.1.2. Números primos

Para todo $n \in \mathbb{Z}$, $n > 1$, el entero n tiene al menos dos divisores positivos: 1 y n.

Definición 2.1.2. Los números positivos con exactamente 2 divisores (por ejemplo 2, 3, 5, 7, 11) se llaman *primos*. Todos los demás enteros positivos mayores que 1 y que no son primos se llaman compuestos.
Es decir: p es primo $\iff p \in \mathbb{Z}^{>1}$ y para todo $n \in \mathbb{Z}^{>0}$ se cumple

$$n \mid p \implies (n = 1) \vee (n = p)$$

Teorema 2.1.1. Si $n \in \mathbb{Z}^{>1}$ y n es compuesto, entonces existe un primo p tal que $p \mid n$.

Teorema 2.1.2 (Teorema de Euclides[1])**.** Existe una infinidad de números primos.

2.1.3. Algoritmo de la división

Teorema 2.1.3. Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Ejemplo 22.

1. Sean $a = 170$ y $b = 11$, entonces $q = 15$ y $r = 5$.

2. Sean $a = 98$ y $b = 7$, entonces $q = 14$ y $r = 0$.

3. Sean $a = -45$ y $b = 8$, entonces $q = -6$ y $r = 3$

[1]Del siglo IV a.C.

El algoritmo

$a, b, q, r \in \mathbb{Z}$;
read(a, b);
if $a = 0$
then $q = 0, r = 0$;
else{
  $q = 0, r = |a|$;
  while $(r \geq b)$ do $r = r - b, q = q + 1$;
  if $a < 0$ then $r = r - b, q = q + 1, r = -r, q = -q$
}

Ejemplo 23. Sean $a = 37$, $b = 8$.

Bloque while:

r	q
37	0
29	1
21	2
13	3
5	4

Es decir, que 37 dividido 8 es 4 con resto 5:

$$37 = 4 \times 8 + 5$$

Ejemplo 24. Sean $a = -37$, $b = 8$.

Bloque while:

r	q
37	0
29	1
21	2
13	3
5	4

Bloque if $a < 0$:

r	q
-3	5
3	-5

Es decir, que -37 dividido 8 es -5 con resto 3:

$$-37 = (-5) \times 8 + 3$$

2.2. Aritmética modular

2.2.1. Definiciones y propiedades

Definición 2.2.1. Sea $n \in \mathbb{Z}^+$, $n \geq 1$. Para $a, b \in \mathbb{Z}$, decimos que a es congruente con b modulo n, y lo escribimos $a \equiv_n b$ (o $a \equiv b (\mathsf{mod}\ n)$), si $n \mid (a - b)$.

Ejemplo 25.

1. $17 \equiv_5 2$ porque $5 \mid (17 - 2)$.

2. $-7 \equiv_6 -49$ porque $6 \mid (-49+7)$.

Observación.

$$a = bn + r \quad \iff \quad a \equiv_b r \qquad \text{ya que } b \mid (a-r)$$

Teorema 2.2.1. La congruencia módulo n es una relación de equivalencia

Demostración.

Simétrica $a \equiv_n b \iff b \equiv_n a$, ya que

$$a \equiv_n b \iff n \mid (a-b) \iff n \mid (b-a) \iff b \equiv_n a$$

Reflexiva $a \equiv_n a$ ya que $n \mid (a-a)$.

Transitiva Si $a \equiv_n b$ y $b \equiv_n c$, entonces $a \equiv_n c$, ya que

$$\begin{aligned}
\left\{ \begin{array}{l} n \mid (a-b) \\ n \mid (b-c) \end{array} \right\} &\implies \left\{ \begin{array}{l} nk = a-b \\ np = b-c \end{array} \right\} \\
&\implies nk + np = a - b + b - c \\
&\implies n(k+p) = a - c \\
&\implies n \mid (a-c) \\
&\implies a \equiv_n c
\end{aligned}$$

□

Definición 2.2.2. Como una relación de equivalencia sobre un conjunto genera una partición, para $n \geq 2$, la congruencia módulo n divide a $\mathbb{Z}$ en n clases de equivalencia:

$$\begin{aligned}
[0] &= \{\dots, -2n, -n, 0, n, 2n, \dots\} = \{0 + nx \mid x \in \mathbb{Z}\} \\
[1] &= \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\} = \{1 + nx \mid x \in \mathbb{Z}\} \\
[2] &= \{\dots, -2n+2, -n+2, 2, n+2, 2n+2, \dots\} = \{2 + nx \mid x \in \mathbb{Z}\} \\
&\vdots \\
[n-1] &= \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\} = \{(n-1) + nx \mid x \in \mathbb{Z}\}
\end{aligned}$$

Llamamos *conjunto de restos módulo n* (notación $\mathbb{Z}_n$) al conjunto $\{[0], [1], [2], \dots, [n-1]\}$.

Ejemplo 26. En $\mathbb{Z}_7$, $9, 16, 23 \in [2]$, y $-6, 1, 8 \in [1]$.

Propiedades. Sean $n \in \mathbb{Z}^+$ y $a, b, c, d \in \mathbb{Z}$ tales que

$$a \equiv_n b \qquad c \equiv_n d$$

entonces

1. $a + c \equiv_n b + d$
2. $ac \equiv_n bd$

Es decir, la suma y el producto son cerrados en $\mathbb{Z}_n$. Definimos:

$$[a] + [b] = [a+b] \qquad \text{y} \qquad [a][b] = [ab]$$

2.2.2. Ecuaciones de congruencias lineales

Definición 2.2.3 (Máximo común divisor)**.** El máximo común divisor entre los enteros a y b es el entero c si y sólo sí $c \mid a$, $c \mid b$ y para todo divisor d de a y b, $d \mid c$.
Notación $c = \mathsf{mcd}(a, b)$.

Para encontrar el máximo común divisor entre dos números, buscamos sus factores primos y luego comparamos. El producto de los factores en común será el mcd.

Ejemplo 27.

2100	2
1050	2
525	3
175	5
35	5
7	7
1	

125	5
25	5
5	5
1	

Por lo tanto,

$$2100 = 2^2 \times 3 \times 5^2 \times 7 \qquad \text{y} \qquad 125 = 5^3$$

Coinciden en $5^2 = 25$, por lo tanto, $\mathsf{mcd}(2100, 125) = 25$.

Teorema 2.2.2. La ecuación $ax \equiv_n b$ tiene solución si y sólo si $\mathsf{mcd}(a, n) \mid b$. En ese caso, las soluciones son

$$x = x_0 + \frac{nt}{\mathsf{mcd}(a, n)}, \qquad t \in \mathbb{Z}$$

donde x_0 es una solución particular de la ecuación diofántica $ax_0 + ny = b$ (ecuación con soluciones enteras).

Ejemplo 28.

$$5x \equiv_8 2$$

Notar que $\mathsf{mcd}(5, 8) = 1$ y $1 \mid 2$, por lo que la ecuación tiene solución.
Sea x_0 solución a la ecuación $5x_0 + 8y = 2$.
Entonces $x_0 = 2$ y $y = -1$, y tenemos $x = 2 + 8t$, para cualquier t.
Por ejemplo, si $t = 3$, $x = 2 + 8 \times 3 = 26$ y $5 \times 26 = 130 \equiv_8 2$ ya que $8 \mid (130 - 2)$.

2.3. Ejercicios del capítulo

Aritmética entera

2.1. Demostrar el teorema de las propiedades de los divisores.

2.2. Sean $a, b, c, d \in \mathbb{Z}^+$. Demuestre las siguientes propiedades:

a) $[(a \mid b) \wedge (c \mid d)] \Rightarrow ac \mid bd$.

b) $a \mid b \Rightarrow ac \mid bc$.

c) $ac \mid bc \Rightarrow a \mid b$.

2.3. Si p, q son primos, demuestre que $p \mid q$ si y sólo si $p = q$.

2.4. Si $a, b, c \in \mathbb{Z}^+$ y $a \mid bc$, ¿implica esto que $a \mid b$ o $a \mid c$?

2.5. Para cualesquiera enteros a, b y c, demuestre que si $a \nmid bc$, entonces $a \nmid b$ y $a \nmid c$.

2.6. Sean $n \in \mathbb{Z}^+$, donde $n \geq 2$. Demuestre que si $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{Z}^+$ y $a_i \mid b_i$ para todo $1 \leq i \leq n$, entonces $(a_1 a_2 \ldots a_n) \mid (b_1 b_2 \ldots b_n)$.

2.7. Encuentre tres enteros positivos a, b, c tales que $31 \mid (5a + 7b + 11c)$.

2.8. Si $a, b, c \in \mathbb{Z}$ y $31 \mid (5a + 7b + 11c)$, demuestre que:

a) $31 \mid (21a + 17b + 9c)$.

b) $31 \mid (6a + 27b + 7c)$.

2.9. Sean $a, b \in \mathbb{Z}^+$. Si $b \mid a$ y $b \mid (a + 2)$, demuestre que $b = 1$ o $b = 2$.

2.10. Si $n \in \mathbb{Z}^+$ y n es impar, demuestre que $8 \mid (n^2 - 1)$.

2.11. Si $a, b \in \mathbb{Z}^+$ y ambos son impares, demuestre que $2 \mid (a^2 + b^2)$, pero $4 \nmid (a^2 + b^2)$.

2.12. Determine el cociente q y el resto r para cada caso utilizando el algoritmo de la división:

a) $a = 23$, $b = 7$.

b) $a = -115$, $b = 12$.

c) $a = 0$, $b = 42$.

d) $a = 37$, $b = 1$.

e) $a = 434$, $b = 31$.

f) $a = -644$, $b = 85$.

2.13. Si $n \in \mathbb{Z}^+$, demuestre que $3 \mid (7^n - 4^n)$.

2.14. Para $n \in \mathbb{Z}^+$, escriba un programa (o desarrolle un algoritmo) que imprima todos los divisores positivos de n.

2.15. Sea $n \in \mathbb{Z}^+$ con $n = r_k 10^k + \cdots + r_2 10^2 + r_1 10 + r_0$. Demuestre que

a) $2 \mid n$ si y sólo si $2 \mid r_0$

b) $4 \mid n$ si y sólo si $4 \mid r_1 10 + r_0$

c) $8 \mid n$ si y sólo si $8 \mid r_2 10^2 + r_1 10 + r_0$

Establezca un teorema general sugerido por estos resultados.

Aritmética modular

2.16. Enumerar cuatro elementos de cada una de las siguientes clases de equivalencia:

a) $[1]$ en $\mathbb{Z}_7$

b) $[2]$ en $\mathbb{Z}_{11}$

c) $[10]$ en $\mathbb{Z}_{17}$

2.17. Demuestre que si $a, b, c, n \in \mathbb{Z}$ con $a, n > 0$ y $b \equiv_n c$, entonces $ab \equiv_{an} ac$.

2.18. Sean $a, b, m, n \in \mathbb{Z}$ con $m, n > 0$. Demuestre que si $a \equiv_n b$ y $m \mid n$, entonces $a \equiv_m b$.

2.19. Demuestre que para todo entero n, exactamente uno de los enteros n, $2n - 1$ y $2n + 1$ es divisible entre 3.

2.20. ¿Si la aguja de las horas de un reloj marca las 12, qué hora marcará 103 horas después?

2.21. Para cada una de las siguientes ecuaciones de congruencias lineales, determinar si tiene solución, y encontrar un conjunto de soluciones en caso de que la tenga.

a) $81x \equiv_9 2$
b) $81x \equiv_9 27$
c) $81x \equiv_9 0$
d) $2x \equiv_3 2$
e) $3x \equiv_6 18$
f) $3x \equiv_{18} 6$
g) $x \equiv_4 1$
h) $5x \equiv_{12} 103$
i) $5x \equiv_{103} 12$
j) $2x \equiv_2 3$
k) $100x \equiv_2 102$
l) $102x \equiv_{100} 2$

Capítulo 3

Estructuras algebraicas

3.1. Algunas estructuras abstractas

3.1.1. Operación binaria interna

Definición 3.1.1 (Operación binaria interna)**.** Una operación binaria interna en un conjunto es una regla que asigna a cada par ordenado de elementos de un conjunto, algún elemento del conjunto.
Es decir, $\odot$ es una operación binaria interna en A si para todo $a, b \in A$ se tiene $a \odot b \in A$

Definición 3.1.2 (Propiedades)**.** Sea $\odot$ una operación binaria interna en un conjunto A. La siguiente es una lista de propiedades que puede o no tener dicha operación:

- Conmutatividad: Si $\forall a, b \in A$, $a \odot b = b \odot a$
- Asociatividad: Si $\forall a, b, c \in A$, $(a \odot b) \odot c = a \odot (b \odot c)$
- Existencia de elemento neutro: Si $\exists e \in A$ tal que $\forall a \in A$, $a \odot e = e \odot a = a$.
- Existencia de elemento inverso: Si $\forall a \in A, \exists b \in A$ tal que $a \odot b = b \odot a = e$.
- Existencia de elemento absorbente: Si $\exists z \in A$ tal que $\forall a \in A$, $a \odot z = z \odot a = z$.

Ejemplo 29.

1. Definimos la operación $\odot$ sobre el conjunto $\mathbb{N}$ como

$$a \odot b = \begin{cases} a & \text{Si } a > b \\ b & \text{Si } b \geq a \end{cases}$$

   Notar que $\odot$ es la operación máx. La operación es una operación binaria interna ya que toma dos números naturales y devuelve un natural. Es conmutativa, asociativa, tiene elemento neutro (1), pero no tiene inverso, ni absorbente.

2. Definimos la operación $\oplus$ sobre el conjunto $\mathbb{N}$ como

$$a \oplus b = \begin{cases} a & \text{Si } a < b \\ b & \text{Si } b \leq a \end{cases}$$

Notar que $\oplus$ es la operación mín. La operación es una operación binaria interna ya que toma dos números naturales y devuelve un natural. Es conmutativa, asociativa, no tiene elemento neutro, y por lo tanto, tampoco tiene inverso, pero tiene elemento absorbente (1).

3. Definimos la operación $\otimes$ sobre un conjunto A cualquiera como $a \otimes b = a$. Es decir, $\otimes$ es la función first. Esta operación no es conmutativa ($a \otimes b = a$ y $b \otimes a = b$), es asociativa ($a \otimes (b \otimes c) = a$ y $(a \otimes b) \otimes c = a \otimes b = a$). No tiene elemento neutro, y por tanto no tiene inverso, ni tiene elemento absorbente.

4. La suma sobre $\mathbb{N}_0$ es conmutativa, asociativa, tiene neutro (0), no tiene inverso, y no tiene elemento absorbente.

5. El producto sobre $\mathbb{Z}$ es conmutativo, asociativo, tiene neutro (1), no tiene inverso (ya que para 0 no existe inverso) y tiene elemento absorbente (0).

6. El producto sobre $\mathbb{Z} \setminus \{0\}$ es conmutativo, asociativo, tiene neutro (1), tiene inverso, pero no tiene elemento absorbente.

3.1.2. Magma, semigrupos, monoides y grupos

Definición 3.1.3 (Magma)**.** Un magma es una estructura algebraica que consiste en un conjunto y una operación binaria interna.

Ejemplo 30. Todos los ítemes del ejemplo 29 son ejemplos de magmas:

- $(\mathbb{N}, \odot)$
- $(\mathbb{N}, \oplus)$
- $(A, \otimes)$
- $(\mathbb{N}_0, +)$
- $(\mathbb{Z}, \times)$
- $(\mathbb{Z} \setminus \{0\}, \times)$

Definición 3.1.4 (Semigrupo)**.** Un semigrupo es un magma donde su operación es asociativa.

Ejemplo 31.

- Todos los ítemes del ejemplo 29 son operaciones asociativas, y por lo tanto, forman semigrupo con sus respectivos conjuntos.
- La resta no es ya que $10 - (2 - 3) \neq (10 - 2) - 3$, y por lo tanto $(\mathbb{Z}, -)$ es un magma pero no un semigrupo.

Definición 3.1.5 (Monoide)**.** Un monoide es un semigrupo con elemento neutro.

Ejemplo 32.

- Los ejemplos 29.1., 29.4., 29.5. y 29.6. son monoides, en cambio los ejemplos 29.2. y 29.3. no lo son.
- El conjunto de listas, que incluye la lista vacía, y la operación concat es un monoide, ya que la lista vacía es el neutro de la operación concat, y dicha operación es asociativa.

- $(\mathbb{M}_2, .)$, donde . es el producto matricial, es un monoide, ya que el producto es asociativo y existe el elemento neutro (I).

Definición 3.1.6 (Grupo)**.** Un grupo es un monoide con elemento inverso.

Ejemplo 33.

- En el ejemplo 29, no hay ningún grupo.
- $(\mathbb{Z}, +)$ es un grupo.
- $(\mathbb{M}_2, .)$, no es un grupo, ya que no toda matriz cuadrada tiene inversa.

Definición 3.1.7 (Grupo abeliano)**.** Un grupo abeliano es un grupo donde la operación es conmutativa.

Ejemplo 34.

- $(Z, +)$ es un grupo abeliano.
- El conjunto de matrices invertibles con el producto de matrices es un grupo, pero no es abeliano, ya que el producto matricial no es conmutativo.

3.1.3. Homomorfismos de grupos

Un homomorfismo de grupos es una función entre grupos que preserva la operación binaria.

Definición 3.1.8 (Homomorfismo de grupos)**.** Dados dos grupos $(G, \odot)$ y $(H, \oplus)$, la aplicación $\varphi : G \to H$ es un homomorfismo de grupos si se verifica que para todos los pares de elementos $a, b \in G$,

$$\varphi(a \odot b) = \varphi(a) \oplus \varphi(b)$$

Definición 3.1.9 (Imagen de un homomorfismo)**.** Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. El conjunto de todos los elementos de H que son la imagen de algún elemento de G se denota $\mathsf{Im}(\varphi)$. Es decir:

$$\mathsf{Im}(\varphi) = \{h \in H \mid h = \varphi(g), \text{para algún } g \in G\}$$

Teorema 3.1.1. Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces, $\mathsf{Im}(\varphi)$ es un subgrupo de H (es decir, $\mathsf{Im}(\varphi) \subseteq H$ y $(\mathsf{Im}(\varphi), \oplus)$ es un grupo).

Demostración. Ejercicio □

Definición 3.1.10 (Núcleo o kernel)**.** Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. El conjunto de todos los elementos de G cuya imagen a través de φ es el elemento neutro H, se llama núcleo o kernel de φ. Es decir:

$$\mathsf{ker}(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$$

Teorema 3.1.2. Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces, $\mathsf{ker}(\varphi)$ es un subgrupo de G (es decir, $\mathsf{ker}(\varphi) \subseteq G$ y $(\mathsf{ker}(\varphi), \odot)$ es un grupo).

Demostración. Ejercicio □

Propiedades. Dado un homomorfismo de grupos $\varphi : (G, \odot) \to (H, \oplus)$, se verifican las siguientes propiedades:

1. La imagen del elemento neutro de G es el elemento neutro de H: $\varphi(e_G) = e_H$,
2. El kernel de φ es un subconjunto no vacío: $\mathsf{ker}(\varphi) \neq \emptyset$.
3. La imagen de un inverso es el inverso de la imagen: $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Demostración.

1. Sea $a \in G$. Entonces,

$$\varphi(a) = \varphi(e_G \odot a) = \varphi(e_G) \oplus \varphi(a)$$
$$\varphi(a) = \varphi(a \odot e_G) = \varphi(a) \oplus \varphi(e_G)$$

   Es decir, $\varphi(e_G)$ es el elemento neutro en $(H, \oplus)$. O, dicho de otro modo, $\varphi(e_G) = e_H$.

2. Dado que $\varphi(e_G) = e_H$, $\varphi(e_G) \in \mathsf{ker}(\varphi)$, y entonces $\mathsf{ker}(\varphi) \neq \emptyset$.

3. Sea $a \in G$. Entonces,

$$\varphi(a^{-1}) \oplus \varphi(a) = \varphi(a^{-1} \odot a) = \varphi(e_G) = e_H$$
$$\varphi(a) \oplus \varphi(a^{-1}) = \varphi(a \odot a^{-1}) = \varphi(e_G) = e_H$$

   Por lo tanto, $\varphi(a^{-1})$ es la inversa de $\varphi(a)$. Es decir, $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Teorema 3.1.3. $\forall a \in G, \forall k \in \mathsf{ker}(\varphi), \varphi(a \odot k) = \varphi(a)$.

Demostración. $\varphi(a \odot k) = \varphi(a) \oplus \varphi(k) = \varphi(a) \oplus e_H = \varphi(a)$. □

Ejemplo 35.

- $f : (\mathbb{R}, +) \to (\mathbb{R}^*, .)$, con $f(x) = e^x$ es un homomorfismo de grupos.

  Demostración.

  - $(\mathbb{R}, +)$ es un grupo: $+$ es una operación binaria interna en $\mathbb{R}$, es asociativa, tiene elemento neutro (0) y todo elemento $a \in \mathbb{R}$ tiene inverso, $-a$.
  - $(\mathbb{R}^*, .)$ es un grupo: $.$ es una operación binaria interna en $\mathbb{R}^*$, es asociativa, tiene elemento neutro (1) y todo elemento $a \in \mathbb{R}^*$ tiene elemento inverso, $1/a$.
  - Y tenemos que $f(a + b) = e^{a+b} = e^a e^b = f(a).f(b)$. □

  $\mathsf{Im}(f) = \mathbb{R}^+$, $\mathsf{ker}(f) = \{0\}$.

- Sea $\mathbb{M}_n$ el conjunto de matrices cuadradas invertibles de tamaño n con coeficientes en $\mathbb{R}$, y sea $|\cdot|$ la operación determinante. Entonces, $|\cdot| : (\mathbb{M}_n, .) \to (\mathbb{R}^*, .)$ es un homomorfismo de grupos.

Demostración.

- $(\mathbb{M}_n, .)$ es un grupo: El producto de matrices cuadradas invertibles es una operación binaria interna, para ver eso sólo hace falta mostrar que el producto da una matriz cuadrada de dimensión n, invertible y a coeficientes no nulos. Es trivial que la matriz tiene la misma dimensión n y que sus coeficientes serán no nulos. Demostramos que tienen inversa: Sean $A, B \in \mathbb{M}_n$, entonces, tenemos que mostrar que AB tiene inversa. $AB(B^{-1}A^{-1}) = AIA^{-1} = AA^{-1} = I$. $(B^{-1}A^{-1})AB = B^{-1}IB = B^{-1}B = I$, por lo tanto $B^{-1}A^{-1}$ es la inversa de AB.
- $(\mathbb{R}^*, .)$ es un grupo (ver ejemplo anterior).
- Y tenemos que para todo $A, B \in \mathbb{M}_n$, $|AB| = |A||B|$. □

$Im(|\cdot|) = \mathbb{R}$, $\mathsf{ker}(|\cdot|) = \{A \in \mathbb{M}_n \mid |A| = 1\}$

Definición 3.1.11 (Monomorfismo)**.** Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces φ es un monomorfismo de grupos si es inyectivo. Es decir, si no existen dos elementos de G con la misma imagen:

$$\forall a, b \in G,\ \varphi(a) = \varphi(b) \iff a = b$$

Teorema 3.1.4. Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos y $\varphi : G \to H$ un homomorfismo de grupos. Entonces, φ es un monomorfismo de grupos sí y sólo sí $\mathsf{ker}(\varphi) = \{e_G\}$.

Demostración.

⇒) Consideremos que φ es un monomorfismo. Sabemos que $\varphi(e_G) = e_H$, por lo tanto $e_G \in \mathsf{ker}(\varphi)$. Dado que φ es inyectiva, no puede haber ningún otro elemento a de G tal que $\varphi(a) = e_H$, y por lo tanto, no hay más elementos que e_G en $\mathsf{ker}(\varphi)$.

⇐) Consideremos que $\mathsf{ker}(\varphi) = \{e_G\}$. Sean $a, b \in G$ tales que $\varphi(a) = \varphi(b)$. Sabemos que $\varphi(a^{-1})$ es la inversa de $\varphi(a)$ en H, y como que $\varphi(a) = \varphi(b)$, $\varphi(a^{-1})$ también es la inversa de $\varphi(b)$. Entonces,

$$\varphi(b \odot a^{-1}) = \varphi(b) \oplus \varphi(a^{-1}) = e_H$$
$$\varphi(a^{-1} \odot b) = \varphi(a^{-1}) \oplus \varphi(b) = e_H$$

Por lo tanto, $b \odot a^{-1} \in \mathsf{ker}(\varphi)$ y $a^{-1} \odot b \in \mathsf{ker}(\varphi)$, es decir, $b \odot a^{-1} = a^{-1} \odot b = e_G$, y por lo tanto a^{-1} es la inversa de b, lo que implica que $a = b$. □

Definición 3.1.12 (Epimorfismo)**.** Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces φ es un epimorfismo si es sobreyectivo. Es decir, si todo elemento de H es imagen de algún elemento de G:

$$\forall h \in H, h = \varphi(g) \text{ para algún } g \in G$$

Dicho de otro modo, $\mathsf{Im}(\varphi) = H$.

Definición 3.1.13 (Isomorfismo)**.** Sean $(G, \odot)$ y $(H, \oplus)$ dos grupos, y sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces φ es un isomorfismo si es simultáneamente inyectivo y sobreyectivo, o lo que es lo mismo, biyectivo. Cuando esto ocurre, ambos grupos tienen la misma estructura algebraica (son *isomorfos*), y sólo se diferencian por los símbolos utilizados para denotar al conjunto, los elementos y la operación.

Ejemplo 36. Sea $\mathbb{Z}^p = \{n \in \mathbb{Z} \mid n \text{ es par}\}$. Mostraremos que $(\mathbb{Z}, +)$ y $(\mathbb{Z}^p, +)$ son isomorfos, es decir, que existe un isomorfismo $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}^p, +)$.
Primero tenemos que mostrar que $(\mathbb{Z}, +)$ y $(\mathbb{Z}^p, +)$ son grupos:

$(\mathbb{Z}, +)$**:** $+$ es binaria interna en $\mathbb{Z}$, es asociativa, tiene elemento neutro (0), y todo elemento $n \in \mathbb{Z}$ tiene inverso, $-n$.

$(\mathbb{Z}, +)$**:** $+$ es binaria interna en $\mathbb{Z}^p$ (notar que la suma de dos números pares es un número par), es asociativa, tiene elemento neutro (0), y todo elemento $p \in \mathbb{Z}^p$ tiene inverso, $-p$ (notar que si p es par, $-p$ también lo es).

Definimos $\varphi(n) = 2n$. Dado que esta función es biyectiva, φ es un isomorfismo de grupos, y por lo tanto, $(\mathbb{Z}, +)$ y $(\mathbb{Z}^p, +)$ son isomorfos.

3.2. Espacios vectoriales

3.2.1. El espacio vectorial $\mathbb{K}^n$

Definición 3.2.1 (Cuerpo)**.** Un cuerpo es una estructura algebraica que consiste en un conjunto y dos operaciones binarias internas (a las que se les llama aditiva y multiplicativa) con las siguientes propiedades:

- Ambas son asociativas.
- Ambas son conmutativas.
- La multiplicativa distribuye respecto a la aditiva.
- Ambas tienen elementos inversos para todos los elementos del conjunto.
- Ambas tienen elemento neutro.

Es decir, $(\mathbb{K}, \oplus, \otimes)$ es un cuerpo sí y sólo sí

- $(\mathbb{K}, \oplus)$ es un grupo abeliano.
- $(\mathbb{K} \setminus \{e_\oplus\}, \otimes)$ es un grupo abeliano, donde $e_\oplus$ es el neutro del grupo $(\mathbb{K}, \oplus)$.
- $\otimes$ distribuye con respecto a $\oplus$: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Ejemplo 37.

- $(\mathbb{R}, +, \times)$ es un cuerpo, ya que $(\mathbb{R}, +)$ es un grupo abeliano, $(\mathbb{R}^*, \times)$ es un grupo abeliano, y $\times$ distribuye con respecto a $+$.
- $(\{\mathsf{T}, \mathsf{F}\}, \mathsf{xor}, \mathsf{and})$ es un cuerpo: *Ejercicio.*

Definición 3.2.2 (El espacio vectorial $\mathbb{K}^n$)**.** Dado un número natural n fijo y un cuerpo $\mathbb{K}$ a cuyos elementos llamaremos escalares, se llaman vectores de n componentes del cuerpo $\mathbb{K}$ a las sucesiones o sistemas ordenados de n escalares de $\mathbb{K}$, es decir a los elementos de $\mathbb{K}^n$. Estos vectores son, pues, los objetos

$$\vec{v} = (v_1, v_2, \ldots, v_n)$$

donde $v_1, v_2, \ldots, v_n \in \mathbb{K}$. A v_i se le llama componente i-ésima del vector $\vec{v}$.

Definición 3.2.3 (Suma entre vectores y producto por un escalar)**.** Sea $(\mathbb{K}, \oplus, \otimes)$ un cuerpo. En el espacio vectorial $\mathbb{K}^n$ definimos las siguientes operaciones:

- Suma de vectores: haciendo abuso de notación, utilizamos el símbolo $+$ para la suma de vectores.

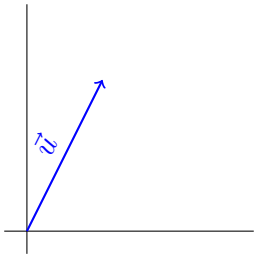
$$\vec{u} + \vec{v} = (u_1 \oplus v_1, u_2 \oplus v_2, \ldots, u_n \oplus v_n)$$

- Producto por un escalar: Sea $\lambda \in \mathbb{K}$. Entonces,

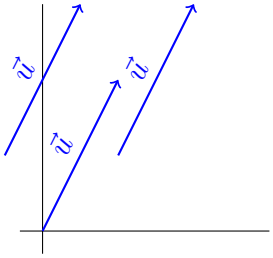
$$\lambda\vec{v} = (\lambda \otimes v_1, \lambda \otimes v_2, \ldots, \lambda \otimes v_n)$$

Observación. Son las mismas operaciones que definimos entre matrices. De hecho, los vectores son matrices de una sola fila, donde las componentes son elementos de $\mathbb{K}$.

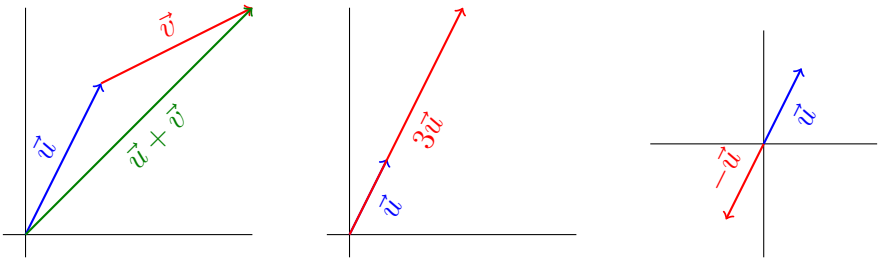
Interpretación gráfica (para los espacios vectoriales $\mathbb{R}^2$ y $\mathbb{R}^3$). A un vector (a, b) de $\mathbb{R}^2$ lo representamos en el plano como una flecha con origen en $(0, 0)$ y fin en (a, b).



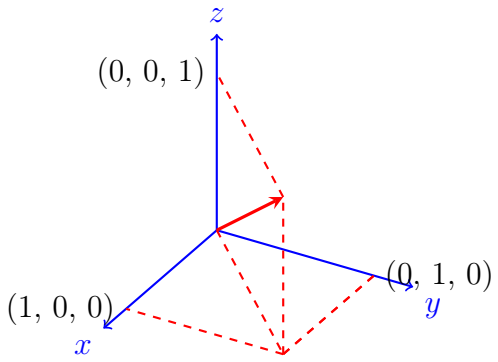
Sin embargo, lo único importante es la dirección (la pendiente que forma con el eje), el sentido (para que lado apunta la flecha) y el módulo (el tamaño de la flecha), así que es perfectamente válido dibujar el vector en cualquier otro lugar del plano, siempre y cuando esos tres parámetros se mantengan:



Las operaciones entre vectores se pueden ver gráficamente de la siguiente manera:



En $\mathbb{R}^3$ es análogo. Por ejemplo, el vector $(1, 1, 1)$ se gráfica de la siguiente manera:



Observación. Decimos que $\lambda\vec{v}$ es proporcional a $\vec{v}$.

Propiedades. Sean $\vec{u}, \vec{v}, \vec{w} \in \mathbb{K}^n$, $\lambda, \mu \in \mathbb{K}$.

1. La suma es asociativa: $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$.
2. La suma es conmutativa: $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.
3. Existe elemento neutro respecto a la suma, llamado vector nulo $\vec{v} + \vec{0} = \vec{v}$, donde $\vec{0} = (e_\oplus, e_\oplus, \ldots, e_\oplus)$.
4. Para cada $\vec{v}$ existe un vector $-\vec{v}$ tal que $\vec{v} + (-\vec{v}) = \vec{0}$. Si $\vec{v} = (v_1, v_2, \ldots, v_n)$, entonces $-\vec{v} = (-v_1, -v_2, \ldots, -v_n)$, donde $-v_i$ es el inverso de v_i con respecto a $\oplus$. A $-\vec{v}$ se le llama opuesto de $\vec{v}$.
5. $\lambda(\vec{u} + \vec{v}) = \lambda\vec{u} + \lambda\vec{v}$.
6. $(\lambda \oplus \mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$.
7. $\lambda(\mu\vec{v}) = (\lambda \otimes \mu)\vec{v}$.
8. $e_\otimes\vec{v} = \vec{v}$.

Demostración. Ejercicio □

Observación. A partir de ahora, para ayudar a la intuición, escribimos 0 para $e_\oplus$ y 1 para $e_\otimes$.

Consecuencias.

1. $0\vec{u} = \vec{0}$
2. $\lambda\vec{0} = \vec{0}$
3. $\lambda\vec{u} = \vec{0} \Rightarrow [\lambda = 0 \text{ o } \vec{u} = \vec{0}]$.
4. $(-\lambda)\vec{u} = \lambda(-\vec{u}) = -(\lambda\vec{u})$

Demostración. Ejercicio □

Definición 3.2.4 (Combinación lineal o dependencia lineal)**.** Se dice que un vector $\vec{v}$ es una combinación lineal de los vectores $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_h$ o que $\vec{v}$ depende linealmente de ellos si existen escalares $\lambda_1, \lambda_2, \ldots, \lambda_h$ tales que

$$\vec{v} = \lambda_1\vec{u}_1 + \lambda_2\vec{u}_2 + \cdots + \lambda_h\vec{u}_h$$

Observación. La dependencia lineal es transitiva: si $\vec{v}$ depende linealmente de unos vectores y cada uno de estos dependen linealmente de otros, $\vec{v}$ depende linealmente de éstos últimos.

Definición 3.2.5 (Conjunto linealmente dependiente)**.** Se dice que un sistema de vectores (o conjunto de vectores) $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ es un conjunto linealmente dependiente (o LD) si se verifican las siguientes propiedades (que son equivalentes entre sí):

1. Alguno de los vectores de S depende linealmente de los demás.
2. Para algunos escalares $\lambda_1, \lambda_2, \ldots, \lambda_p$, que no son todos nulos, se verifica

$$\lambda_1\vec{v}_1 + \lambda_2\vec{v}_2 + \cdots + \lambda_p\vec{v}_p = \vec{0}$$

Ejemplo 38.

1. El vector nulo $\vec{0}$ es combinación lineal de cualesquiera vectores $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_h$, ya que

$$\vec{0} = 0\vec{v}_1 + 0\vec{v}_2 + \cdots + 0\vec{v}_h$$

   Por lo tanto, si $\vec{0} \in S$, S es linealmente dependiente.

2. Sean

$$\vec{u}_1 = (2, -1, 5, 1) \quad \vec{u}_2 = (-1, 3, -2, 0) \quad \vec{u}_3 = (3, 1, 8, 2) \quad \vec{v} = (1, -8, 1, -1)$$

El vector $\vec{v}$ depende linealmente de los vectores $\vec{u}_1$, $\vec{u}_2$ y $\vec{u}_3$, ya que

$$\vec{v} = \vec{u}_1 - 2\vec{u}_2 - \vec{u}_3$$

Hay otras maneras de expresarlo, por ejemplo

$$\vec{v} = -\vec{u}_1 - 3\vec{u}_2 + 0\vec{u}_3$$

O sea que $\vec{v}$ es también combinación lineal solamente de $\vec{u}_1$ y $\vec{u}_2$.

Teorema 3.2.1. Si $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_p$ son p vectores de $\mathbb{K}^n$, con $p > n$, entonces $S = \{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_p\}$ es LD.

Demostración. La prueba está en la página 28 del libro

J. de Burgos, Álgebra lineal, 3ra ed., Mc Graw Hill, 2006

Se recomienda leerla. □

Definición 3.2.6 (Conjunto linealmente independiente)**.** Se dice que un sistema o conjunto de vectores $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ es un sistema linealmente independiente (LI) si se verifica una de las siguientes propiedades (que son equivalentes entre sí):

1. El sistema S no es linealmente dependiente (es decir, ninguno de sus vectores depende linealmente de los demás).

2. La única combinación lineal de vectores de S que es nula es la que tiene todos sus coeficientes nulos. Es decir:

$$\lambda_1\vec{v}_1 + \lambda_2\vec{v}_2 + \cdots + \lambda_p\vec{v}_p = \vec{0} \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_p = 0$$

Ejemplo 39. Sean $\vec{a} = (3, 1, 7, -5, 4)$, $\vec{b} = (0, 2, 4, -3, -2)$, $\vec{c} = (0, 0, -6, 5, 1)$.

$$\alpha\vec{a} + \beta\vec{b} + \gamma\vec{c} = \vec{0}$$

es un sistema de ecuaciones con solución única $\alpha = \beta = \gamma = 0$. Por lo tanto, $\{\vec{a}, \vec{b}, \vec{c}\}$ es LI.
Veamos:

$$\alpha(3, 1, 7, -5, 4) + \beta(0, 2, 4, -3, -2) + \gamma(0, 0, -6, 5, 1) = (0, 0, 0, 0, 0)$$

implica que

$$\begin{cases} 3\alpha & & & & & = & 0 \\ \alpha & + & 2\beta & & & = & 0 \\ 7\alpha & + & 4\beta & - & 6\gamma & = & 0 \\ -5\alpha & - & 3\beta & + & 5\gamma & = & 0 \\ 4\alpha & - & 2\beta & + & \gamma & = & 0 \end{cases}$$

y la única solución a este sistema es $\alpha = \beta = \gamma = 0$.

Teorema 3.2.2 (de existencia del rango)**.** Para cualquier sistema $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ de p vectores, no todos nulos, se verifica que:

1. Hay algún sistema $S_0 \subseteq S$ tal que

   a) S_0 es LI

   b) Todos los demás vectores de S dependen linealmente de los de S_0

2. Todos los sistemas S_0 de vectores de S que satisfacen $1.a$ y $1.b$ tienen el mismo número de vectores.

Corolario 3.2.3. Para cada sistema $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ de vectores no nulos, existe un número r tal que

1. Hay un sistema formado por r vectores de S que es LI.
2. Todo sistema formado por más de r vectores de S es LD.

Este número r es entonces el mayor número de vectores LI que hay en S y se le llama rango de S.

Teorema 3.2.4 (del Rango)**.** Sea $S = \{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_m\} \subseteq \mathbb{K}^n$ con $\vec{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$. Consideremos la matriz

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

Entonces, rango S = rango A.

Observación. Si tomamos la matriz A^T donde las columnas son los vectores de S en lugar de las filas, el rango es el mismo.

3.2.2. Espacios, subespacios y combinaciones lineales

Hasta ahora no definimos lo que era un espacio vectorial. Sólo definimos los elementos (vectores) del espacio vectorial $\mathbb{K}^n$, con n fijo y $\mathbb{K}$ un cuerpo. También definimos las operaciones suma y producto por escalar. Las propiedades que tiene este modelo concreto, que coinciden con las de otros muchos ejemplos, se tomarán como punto de partida para definir los espacios vectoriales. Vamos a definir, justamente, un espacio vectorial como un conjunto con dos operaciones que cumpla con ciertas propiedades, como una estructura algebraica más.

Concepto de espacio vectorial

Definición 3.2.7 (Espacio vectorial)**.** Sea V un conjunto dado, a cuyos elementos llamaremos vectores. Se considera también un cuerpo $\mathbb{K}$, a cuyos elementos llamaremos escalares. Se dice que V es un espacio vectorial sobre $\mathbb{K}$ si dispone de las siguientes operaciones "suma" y "producto por escalar", y se satisfacen las siguientes propiedades:

1. Una operación + interna en V (suma de vectores) tal que se cumplen los siguientes axiomas:
   - *a)* (Asociatividad) $\forall \vec{u}, \vec{v}, \vec{w} \in V$ se cumple $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$.
   - *b)* (Conmutatividad) $\forall \vec{u}, \vec{v}$ se cumple $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.
   - *c)* (Existencia de elemento neutro) $\exists \vec{0} \in V$ tal que $\forall \vec{u} \in V$ se cumple $\vec{u} + \vec{0} = \vec{u}$.
   - *d)* (Existencia de inversos) para cada $\vec{u} \in V$, existe $-\vec{u} \in V$ tal que $\vec{u} + (-\vec{u}) = \vec{0}$.
2. Una operación externa (producto por escalar) que a cada pareja $\lambda \in \mathbb{K}$, $\vec{u} \in V$ asocia un vector $\lambda\vec{u}$, tal que se cumplen los siguientes axiomas:
   - *a)* $\forall \vec{u}, \vec{v} \in V, \lambda \in \mathbb{K}$ se cumple $\lambda(\vec{u} + \vec{v}) = \lambda\vec{u} + \lambda\vec{v}$.

b) $\forall \vec{u} \in V, \lambda, \mu \in \mathbb{K}$ se cumple $(\lambda + \mu)\vec{u} = \lambda\vec{u} + \mu\vec{u}$.

c) $\forall \vec{u} \in V, \lambda, \mu \in \mathbb{K}$ se cumple $\lambda(\mu\vec{u}) = (\lambda\mu)\vec{v}$.

d) $\forall \vec{u} \in V$ se cumple $1\vec{u} = \vec{u}$, donde 1 es el elemento neutro de la operación multiplicativa en el cuerpo $\mathbb{K}$.

Observaciones.

- Los cuatro axiomas que afectan a la suma se pueden resumir diciendo que $(V, +)$ es un grupo abeliano.
- Por ser $(V, +)$ un grupo:
  - El vector nulo $\vec{0}$ es único.
  - Cada vector $\vec{u}$ tiene un solo opuesto $-\vec{u}$.
  - Si $\vec{u} + \vec{v} = \vec{u} + \vec{w}$ entonces $\vec{v} = \vec{w}$.
- Como en todo grupo, escribimos $\vec{u} - \vec{v}$ para $\vec{u} + (-\vec{v})$.

Ejemplo 40.

1. $\mathbb{K}^n$ es un espacio vectorial sobre el cuerpo $\mathbb{K}$, como vimos en la sección precedente.

2. Sea $V = \mathcal{F}(C, \mathbb{K})$ el conjunto de las funciones definidas en un conjunto C y con valores en el cuerpo $\mathbb{K}$. Entonces, V es un espacio vectorial sobre $\mathbb{K}$ con las siguientes operaciones:

$$\forall f, g \in V,\ f + g \text{ es tal que } \forall x \in C,\ (f + g)(x) = f(x) + g(x)$$
$$\forall f \in V, \lambda \in \mathbb{K},\ \lambda f \text{ es tal que } \forall x \in C,\ (\lambda f)(x) = \lambda f(x)$$

3. El conjunto $V = \mathbb{K}[x]$ de los polinomios con coeficientes en $\mathbb{K}$ y con variable x, es un espacio vectorial sobre $\mathbb{K}$ respecto de las operaciones usuales de suma de polinomios y producto de un escalar por un polinomio.

4. El conjunto $V = \mathbb{M}_{n\times m}$ de matrices de dimensión $n \times m$ cuyos elementos pertenecen al cuerpo $\mathbb{K}$, es un espacio vectorial respecto de la suma de matrices y el producto de un escalar por una matriz.

Consecuencias (de los axiomas de espacios vectoriales)**.** En un espacio vectorial V sobre un cuerpo $\mathbb{K}$, para cualesquiera que sean $\vec{u}, \vec{v} \in V$ y $\lambda, \mu \in V$ se verifica que:

1. $\lambda\vec{0} = \vec{0}$
2. $0\vec{u} = \vec{0}$
3. $\lambda\vec{u} = \vec{0} \implies [\lambda = 0 \text{ ó } \vec{u} = \vec{0}]$
4. $[\lambda\vec{u} = \mu\vec{u} \text{ y } \vec{u} \neq \vec{0}] \implies \lambda = \mu$
5. $[\lambda\vec{u} = \lambda\vec{v} \text{ y } \lambda \neq 0] \implies \vec{u} = \vec{v}$
6. $(-\lambda)\vec{u} = \lambda(-\vec{u}) = -\lambda\vec{u}$

Demostración. Ejercicio (y si no sale, verla en la página 118 del libro de Burgos). □

Subespacio vectorial

Se llaman subespacios de un espacio vectorial V a aquellos subconjuntos de V que forman un espacio vectorial con las mismas operaciones que V.

Definición 3.2.8 (Subespacio vectorial)**.** Sea V un espacio vectorial sobre el cuerpo $\mathbb{K}$ y sea $U \subseteq V$. Se dice que U es un subespacio vectorial de V si las operaciones de V son, también, operaciones para U, y con ellas U es un espacio vectorial sobre $\mathbb{K}$.

Teorema 3.2.5 (Caracterización de espacios vectoriales)**.** Sea V un espacio vectorial sobre el cuerpo $\mathbb{K}$ y sea $U \subseteq V$. U es un subespacio vectorial de V si, siendo $U \neq \emptyset$ se cumplen las siguientes condiciones:

1. Si $\vec{u}, \vec{v} \in U$, entonces $\vec{u} + \vec{v} \in U$.
2. Si $\lambda \in \mathbb{K}, \vec{u} \in U$, entonces $\lambda\vec{u} \in U$.

Ambas condiciones se pueden sustituir por la siguiente condición:

3. Si $\vec{u}, \vec{v} \in U$ y $\lambda, \mu \in \mathbb{K}$, entonces $\lambda\vec{u} + \mu\vec{v} \in U$.

Es decir: "toda combinación lineal de vectores de U está en U".

Observaciones.

- El vector nulo pertenece a todos los subespacios de un espacio vectorial.
- Para todo espacio vectorial, $O = \{\vec{0}\}$ es un subespacio vectorial del mismo. A este subespacio se le llama subespacio nulo.
- Todo espacio vectorial es subespacio vectorial de sí mismo.
- A los subespacios vectoriales de un espacio V diferentes de V y O se les llaman subespacios propios.

Ejemplo 41.

1. El conjunto $U = \{(x, y, z) \in \mathbb{R}^3 \mid 3x - 2y + 4z = 0\}$ es un subespacio vectorial del espacio $\mathbb{R}^3$.
2. El conjunto de las matrices reales simétricas de tamaño 7×7 es un subespacio del espacio vectorial de las matrices reales de tamaño 7×7.

Teorema 3.2.6. Sean U y W dos subespacios vectoriales del espacio vectorial V. Entonces $U \cap W$ es también un subespacio vectorial de V.

Ejemplo 42. Sea V el espacio vectorial real de las funciones de $\mathbb{R}$ en $\mathbb{R}$. Sea U_1 el subespacio de V que forman las funciones acotadas y sea U_2 el subespacio de V que forman las funciones polinómicas. La intersección $U_1 \cap U_2$ es un subespacio que está formado por las funciones constantes.

Subespacio engendrado por un sistema de vectores

Teorema 3.2.7. Sea S un sistema de vectores de un espacio vectorial V sobre el cuerpo $\mathbb{K}$. El conjunto de todas las combinaciones lineales de los vectores de S es un subespacio vectorial que se llama subespacio engendrado por S y se denota poniendo $\langle S\rangle$ o

$$\langle \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\rangle = \{\lambda_1\vec{u}_1 + \lambda_2\vec{u}_2 + \cdots + \lambda_p\vec{u}_p \mid \lambda_i \in \mathbb{K} \text{ para } i = 1, 2, \ldots, p\}$$

También se dice que S es un sistema generador de $\langle S\rangle$. Este subespacio, $\langle S\rangle$, es el menor de todos los subespacios que contienen a S.

Ejemplo 43.

1. En el espacio vectorial $\mathbb{R}^4$, los vectores $\vec{u} = (1, 2, 0, 0), \vec{v} = (0, 3, -1, 0)$ y $\vec{w} = (0, 0, 5, 4)$ engendran el subespacio:

$$\langle \vec{u}, \vec{v}, \vec{w}\rangle = \{(\lambda, 2\lambda + 3\mu, -\mu + 5\nu, 4\nu) \mid \lambda, \mu, \nu \in \mathbb{R}\}$$

2. En el espacio vectorial $\mathbb{R}[x]$ de polinomios reales con variable x, consideramos los siguientes polinomios:

$$p(x) = 1 - x \qquad q(x) = 1 - x^2 \qquad r(x) = 2x + x^2$$

   El subespacio vectorial engendrado por $p(x)$, $q(x)$ y $r(x)$ está formado por todos los polinomios siguientes (al variar $\alpha, \beta, \gamma \in \mathbb{R}$):

$$\alpha p(x) + \beta q(x) + \gamma r(x) = (\alpha + \beta) + (-\alpha + 2\gamma)x + (\beta + \gamma)x^2 \tag{3.1}$$

   Notar que este subespacio no es otro que el de los polinomios de grado menor o igual que 2, ya que cualquier polinomio $a + bx + cx^2$ puede expresarse en la forma (3.1), sin más que tomar $\alpha = 2a + b - 2c$, $\beta = -a - b + 2c$ y $\gamma = a + b - c$.

Definición 3.2.9 (Sistemas equivalentes de vectores)**.** Sean $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ y $T = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q\}$ dos sistemas de vectores de un espacio vectorial V. Se dice que S y T son sistemas equivalentes si engendran el mismo subespacio, es decir $\langle S\rangle = \langle T\rangle$, esto es, si todo vector de uno cualquiera de los sistemas S o T depende linealmente de los vectores del otro.
Esta relación entre sistemas de vectores de V es una equivalencia, es decir, es reflexiva, simétrica y transitiva.

Ejemplo 44. Consideramos los siguientes vectores de $\mathbb{R}^3$:

$$\vec{a} = (1, 0, 1) \quad \vec{b} = (0, 1, 1) \quad \vec{c} = (1, 1, 2) \quad \vec{u} = (2, 1, 3) \quad \vec{v} = (1, 2, 3)$$

Es fácil comprobar que $\langle \vec{a}, \vec{b}, \vec{c}\rangle = \langle \vec{u}, \vec{v}\rangle$, ya que ambos están formados por vectores $(x, y, z) \in \mathbb{R}^3$ tales que $x + y = z$. Por lo tanto, los sistemas $\{\vec{a}, \vec{b}, \vec{c}\}$ y $\{\vec{u}, \vec{v}\}$ son equivalentes.

Propiedades (de la dependencia e independencia lineal)**.** Se consideran aquí vectores de un espacio vectorial V sobre un cuerpo $\mathbb{K}$.

1. Un sistema de vectores $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ es linealmente dependiente si y sólo si alguno de sus vectores depende linealmente de los demás.

2. Dos sistemas de vectores $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ y $T = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_q\}$ son equivalentes, o sea, $\langle S\rangle = \langle T\rangle$ si y sólo si todo vector de uno de los sistemas depende linealmente de los vectores del otro, y recíprocamente.

3. Si S es un sistema linealmente independiente de vectores y $\vec{v}$ es un vector que no depende de los vectores de S, entonces el sistema $S \cup \{\vec{v}\}$ es linealmente independiente.

Teorema 3.2.8 (Fundamental de la independencia lineal)**.** Sea $V = \langle G\rangle$ donde $G = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$. Si $I = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_h\} \subseteq V$ y I es LI, entonces $h \leq p$.

3.2.3. Bases y coordenadas

Espacios de dimensión finita

Definición 3.2.10 (Dimensión finita)**.** Un espacio vectorial V se dice que es de dimensión finita si está generado por un número finito de vectores, es decir, si en V existe algún sistema de vectores S tal que $V = \langle S\rangle$.

Definición 3.2.11 (Base)**.** Si V es un espacio vectorial de dimensión finita, se dice que un sistema de vectores B es una base de V si verifica cualquiera de las condiciones siguientes (que son equivalentes entre sí):

1. $\langle B\rangle = V$ y B es LI.

2. Todo vector de V se puede expresar de una única manera como combinación lineal de los vectores de B.

Ejemplo 45.

1. En el espacio vectorial $\mathbb{K}^n$, donde $\mathbb{K}$ es un cuerpo, los n vectores

$$\vec{e}_1 = (1, 0, \ldots, 0),\ \vec{e}_2 = (0, 1, \ldots, 0),\ \ldots,\ \vec{e}_n = (0, 0, \ldots, 1)$$

   forman una base, llamada base canónica de $\mathbb{K}^n$. Así ocurre, en efecto, ya que $B = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ es:

   - Generador, puesto que cualquier vector $(x_1, x_2, \ldots, x_n)$ de $\mathbb{K}^n$ es combinación lineal de los vectores de B, ya que

$$(x_1, x_2, \ldots, x_n) = x_1\vec{e}_1 + x_2\vec{e}_2 + \cdots + x_n\vec{e}_n$$

   - LI, ya que la relación $\lambda_1\vec{e}_1 + \lambda_2\vec{e}_2 + \cdots + \lambda_n\vec{e}_n = \vec{0}$ equivalen a $(\lambda_1, \lambda_2, \ldots, \lambda_n) = (0, 0, \ldots, 0)$. Es decir, $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

2. En el espacio vectorial $\mathbb{M}_{n\times m}$ de las matrices reales de tamaño $n \times m$, las $n \cdot m$ siguientes matrices E_{ij}, para $i = 1, \ldots, n$ y $j = 1, \ldots, m$ forman una base, siendo E_{ij} la matriz que tiene todas sus componentes en 0 excepto en la posición ij que vale 1.

   En efecto, $B = \{E_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, m\}$ es generador e independiente, pues:

   - Cualquier matriz $A = (a_{ij}) \in \mathbb{M}_{n\times m}$ es combinación lineal de las matrices de B, ya que
   $$A = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}E_{ij}$$
   - La única combinación lineal nula de las matrices E_{ij} es la que tiene todos los coeficientes nulos, ya que
   $$\sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}E_{ij} = O \implies (\lambda_{ij}) = O \implies \forall i, j,\ \lambda_{ij} = 0$$

Teorema 3.2.9 (Existencia de bases)**.** Cualquier sistema generador de un espacio vectorial de dimensión finita, $V \neq O$, incluye a una base de V. En consecuencia, todo espacio vectorial $V \neq O$ de dimensión finita tiene alguna base.

Teorema 3.2.10 (de la dimensión)**.** Todas las bases de un espacio vectorial $V \neq O$ de dimensión finita tienen igual número de vectores. A este número se le llama dimensión del espacio V y se lo representa con $\dim V$.
Por convención, $\dim O = 0$.

Propiedades (de las bases y la dimensión)**.** Si $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ es un sistema de vectores de un espacio vectorial V de dimensión finita, entonces se verifica que

1. Si $\langle S\rangle = V$ entonces $p \geq \dim V$.

2. Si S es LI, entonces $p \leq \dim V$.

3. Si $\langle S\rangle = V$ y S es LI, entonces $p = \dim V$ y S es base de V.

4. Si S es LI y $\dim V = p$, entonces S es base de V.

Observaciones.

1. La dimensión de un espacio vectorial V es el número máximo de vectores de V linealmente independientes.

2. La dimensión de un espacio vectorial V es el número mínimo de vectores de un sistema generador de V.

Teorema 3.2.11 (de la base incompleta)**.** En un espacio vectorial V de dimensión finita, todo sistema LI de vectores puede completarse hasta obtener una base.
Dicho de otro modo:
Si V es un espacio tal que $\dim V = n$ y si $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{v}_p\}$ es un sistema LI de p vectores de V, con $p \leq n$, entonces es posible encontrar (mejor dicho, existe) algún sistema S' de $n - p$ vectores de V tal que $S \cup S'$ sea una base de V.
Más aún, los vectores de S' se pueden tomar de entre los de una base cualquiera de B.

Ejemplo 46. En el espacio vectorial $\mathbb{R}^3$, los vectores $\vec{a} = (1, -1, 2)$ y $\vec{b} = (0, 1, -2)$ son LI y, por ello, es seguro que hay algún vector $\vec{c} \in \mathbb{R}^3$ tal que $\{\vec{a}, \vec{b}, \vec{c}\}$ es una base de $\mathbb{R}^3$. Es más, el vector $\vec{c}$ que se puede elegir de muchas maneras,puede ser,en particular, uno de los tres vectores de la base canónica (o también de cualquier otra base), que son los vectores $\vec{e}_1 = (1, 0, 0)$, $\vec{e}_2 = (0, 1, 0)$ y $\vec{e}_3 = (0, 0, 1)$. Nótese que $\vec{c}$ no puede ser $\vec{e}_1$, ya que $\vec{e}_1 = \vec{a} + \vec{b}$. Sin embargo, sí puede tomarse $\vec{c} = \vec{e}_2$, ya que $\vec{e}_2$ es linealmente independiente de $\vec{a}$ y $\vec{b}$.

Teorema 3.2.12. Si U es un subespacio del espacio vectorial V, entonces $\dim U \leq \dim V$, donde la igualdad es válida sólo si $U = V$.

Rango de un sistema de vectores

Vamos a generalizar la noción de rango que dimos para $\mathbb{K}^n$ a cualquier espacio vectorial.

Definición 3.2.12 (Rango)**.** Se llama rango de un sistema S de un número finito de vectores de un cierto espacio, a la dimensión del subespacio que engendra S. Es decir:

$$\text{rang } S = \dim(\langle S \rangle)$$

El rango de S es, entonces, el mayor número de vectores linealmente independientes que hay en S.

Observaciones.

1. Un sistema de vectores S es LI si y sólo si su rango es igual al número de vectores que lo conforman.

2. En un espacio vectorial de dimensión finita, un sistema de vectores es generador si y sólo si su rango es igual a la dimensión del espacio.

Definición 3.2.13. Sea V un espacio vectorial de dimensión finita sobre un cuerpo $\mathbb{K}$. Dada una base $B = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ de V, se sabe que para cada vector $\vec{v} \in V$ existen unos únicos escalares $v_1, v_2, \ldots, v_n \in \mathbb{K}$ tales que

$$\vec{v} = v_1\vec{e}_1 + v_2\vec{e}_2 + \cdots + v_n\vec{e}_n$$

Entonces, si dice que la n-upla $(v_1, v_2, \ldots, v_n)$ es el sistema de coordenadas del vector $\vec{v}$ en la base B.

Teorema 3.2.13 (Cálculo del rango)**.** Sea V un espacio vectorial sobre un cuerpo $\mathbb{K}$, que tiene dimensión n y sea B una base de V. Dado un sistema finito $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ de vectores de V, si $S^* = \{\vec{u}_1^*, \vec{u}_2^*, \ldots, \vec{u}_p^*\}$ es el correspondiente sistema de sus n-uplas de coordenadas (es decir, vectores de $\mathbb{K}^n$), se verifica que:

1. $\lambda_1\vec{u}_1 + \lambda_2\vec{u}_2 + \cdots + \lambda_p\vec{u}_p = \vec{0} \iff \lambda_1\vec{u}_1^* + \lambda_2\vec{u}_2^* + \cdots + \lambda_p\vec{u}_p^* = \vec{0}$
2. rang S = rang S^*

Ejemplo 47. En el espacio vectorial $\mathbb{M}_{2\times3}$ de matrices reales de tamaño 2×3, consideremos el sistema $S = \{M_1, M_2, M_3, M_4\}$, formado por las cuatro matrices:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & -1 \end{pmatrix} \quad M_2 = \begin{pmatrix} 2 & -1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \quad M_3 \begin{pmatrix} 3 & 1 & 2 \\ 4 & 2 & 0 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & 3 & 2 \\ 0 & 3 & -3 \end{pmatrix}$$

Usando la base canónica de $\mathbb{M}_{2\times3}$, los vectores de coordenadas de las matrices dadas son, respectivamente:

$$\vec{v}_1 = (1,0,0,2,1,-1) \quad \vec{v}_2 = (2,-1,0,3,0,1) \quad \vec{v}_3 = (3,1,2,4,2,0) \quad \vec{v}_4 = (0,3,2,0,3,-3)$$

El rango del sistema dado S es igual al rango del sistema $S^* = \{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4\}$. Al rango de este sistema de vectores de $\mathbb{R}^6$ lo calculamos con el método de Gauss, y obtenemos que rang S = rang $S^* = 3$.

3.3. Ejercicios del capítulo

3.1. Demostrar que una operación binaria definida en un conjunto de un sólo elemento es asociativa y conmutativa.

3.2. Muestre las propiedades que posee la siguiente operación sobre $A = \{a, b, c\}$:

*	a	b	c
a	c	b	a
b	b	c	b
c	a	b	c

3.3. Escribir la tabla de las operaciones lógicas AND, OR y XOR, y muestre qué propiedades cumplen estas operaciones.

3.4. Sea S un conjunto con exactamente un elemento. ¿Cuántas operaciones binarias diferentes pueden definirse en S? Reponda la pregunta para el caso de S con 2 elementos; con 3 elementos; y con n elementos.

3.5. Sea S el conjunto de todas las funciones que van de todos los reales a todos los reales, y f y g dos elementos de S, demuestre para cada caso si $*$ define una operación binaria interna:

a) $(f * g)(x) = f(x) + g(x)$

b) $(f * g)(x) = f(g(x))$

c) $(f * g)(x) = f(x)/g(x)$

3.6. Dados $a, b, c, d \in S$, demuestre que si $*$ es una operación conmutativa y asociativa en S, entonces $(a * b) * (c * d) = ((d * c) * a) * b$

3.7. Demostrar que si para una operación en un conjunto cualquiera A existe un elemento neutro, éste es único.

3.8. Responda los siguientes items (justifique sus respuestas):

a) ¿La mezcla de colores sobre el conjunto de colores primarios forma un magma? ¿Por qué?

b) Dar un ejemplo de magma sobre $\mathbb{Z}$ que no sea un semigrupo.

c) ¿La operación de mínimo sobre el conjunto N, qué estructura algebraica forma?

d) Forme un magma utilizando una operación relacional.

e) Forme dos monoides utilizando operaciones sobre conjuntos.

f) ¿Qué estructura algebraica forma la suma de clases de equivalencia de la relación módulo n? ¿Y la multiplicación?

g) ¿Cursó Estructuras de Datos? Dados `z` (neutro de un monoide) y la operación `<+>` (operacion binaria de un monoide), describa algunas operaciones que generaliza la siguiente función:

```
g [] = z
g (x:xs) = x <+> g xs
```

h) Dado el tipo `Persona`, un registro con edad y nombre, ¿puede formarse algún monoide?

i) ¿Qué estructura algebraica forman las funciones y la composición de funciones?

3.9. Demuestre que $< \mathbb{N}, + >$ no es un grupo

3.10. Demuestre que $\mathbb{Q}^+$ con la multiplicación en $\mathbb{Q}^+$ forman un grupo abeliano

3.11. Demostrar que para cualquier grupo $< G, * >$ con neutro e, $a \in G$, y $n \in \mathbb{N}$, se cumple $a^n * a^{-n} = e$

3.12. Con la siguiente tabla, resuelva la ecuación $a * b * x = b * b$

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

3.13. Forme un grupo con la suma entre matrices y otro con la multiplicación entre matrices.

3.14. Si $*$ es una operación binaria en un conjunto S, un elemento x de S es idempotente para $*$ si $x*x = x$. Probar que un grupo tiene exactamente un elemento idempotente.

3.15. Un grupo $< G, * >$ es cíclico si existe un $a \in G$ que operado con sí mismo permite generar G. Encuentre dos ejemplos de grupos cíclicos: uno donde G sea un conjunto infinito, y otro donde G sea un conjunto finito.

3.16. Sean los grupos $< \mathbb{R} \setminus \{0\}, . >$ y $< \mathbb{R}_*^+, \times >$, mostrar que la función $f(x) = |x|$ es un morfismo de grupos.

3.17. Plantear dos isomorfismos entre una estructura formada con una operación del Álgebra de Bool y otra con una operación entre las clases de equivalencia módulo 2. *Consejo*: utilice las tablas de las operaciones. ¿Ambos isomorfismos son de grupos?

3.18. Sean los monoides $< \{V, F\}, \wedge >$ y $< \{V, F\}, \vee >$, mostrar que la función $f(p) = \neg p$ es un isomorfismo de monoides. ¿Lo mismo ocurre de manera similar con $< \wp(A), \cup >$ y $< \wp(A), \cap >$ con $f(S) = S^{\complement}$?

3.19. Discutir por qué $\mathbb{Z}$ bajo la suma no es isomorfo a $\mathbb{R}$ bajo la suma

3.20. **Desafío**: resolver alguno de los siguientes items

a) Un automorfismo es un isomorfismo de una estructura algebraica consigo misma. Encontrar un ejemplo de automorfismo.

b) Mostrar un isomorfismo entre $\mathbb{R}$ bajo la suma y $\mathbb{R}^*$ bajo la multiplicación.

3.21. Si ninguno de los vectores $\vec{u}_1, \vec{u}_2, \ldots \vec{u}_p$ depende linealmente de $S = \{\vec{v}_1, \vec{v}_2, \ldots \vec{v}_h\}$, ¿puede ocurrir que alguna combinación lineal de aquellos dependa linealmente de S?

3.22. Estudiar si los siguientes sistemas de vectores de $\mathbb{R}^3$ son linealmente dependientes o independientes:

a) $\{(5, 3, 1), (1, 3, 2), (1, 1, 1)\}$ *b*) $\{(3, 2, 1), (1, -3, 2), (-1, -2, 3)\}$

3.23. Sean $\vec{u} = (-1, 2)$, $\vec{v} = (0, 1)$ y $\lambda = 2$. Resolver gráficamente:

a) $\vec{u} + \vec{v}$. *b*) $\lambda\vec{u}$. *c*) $-\lambda\vec{v}$. *d*) $\vec{v} - \vec{u}$.

3.24. Si $\vec{u}$ y $\vec{v}$ son dos vectores distintos, analizar si algunos de los vectores

$$(2 + \lambda)\vec{u} + (3 - \lambda)\vec{v}$$

con λ escalar, pueden ser iguales.

3.25. Sean $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ y $T = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_q\}$ dos sistemas de vectores. Si tanto S como T son LI y todos los vectores de T son independientes de S, ¿el sistema $S \cup T$ es forzosamente LI?

3.26. Sea $S = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ un sistema de vectores de $\mathbb{R}^n$. Si es $p > n$, comprobar que el sistema S es LD.

3.27. Sean $\vec{u} = (2, 3, 5)$, $\vec{v} = (1, 2, 3)$ y $\vec{w} = (2, 1, 3)$. Analizar si existen escalares a_i, b_i y c_i tales que los vectores

$$\begin{aligned} \vec{x} &= a_1\vec{u} + b_1\vec{v} + c_1\vec{w} \\ \vec{y} &= a_2\vec{u} + b_2\vec{v} + c_2\vec{w} \\ \vec{z} &= a_3\vec{u} + b_3\vec{v} + c_3\vec{w} \end{aligned}$$

sean LI.

3.28. Sean $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n$ los siguientes vectores de $\mathbb{R}^n$: el vector $\vec{u}_i$ (para $i = 1, 2, \ldots, n$) tiene todas sus componentes valiendo 1 excepto la i que vale h. Hallar el rango de $\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ en función de h.

3.29. Hallar el rango del sistema $S = \{\vec{u}_1, \vec{u}_2, \vec{u}_3, \vec{u}_4, \vec{u}_5, \vec{u}_6\}$ siendo:

$$\begin{aligned} \vec{u}_1 &= (2, 6, -1, 0, -1) & \vec{u}_2 &= (2, -2, 1, -3, 2) & \vec{u}_3 &= (3, 4, 1, -1, 2) \\ \vec{u}_4 &= (1, -2, 2, -1, 2) & \vec{u}_5 &= (-1, -1, 1, 2, 1) & \vec{u}_6 &= (1, 8, -3, 1, -4) \end{aligned}$$

3.30. Sean $R = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_p\}$ y $S = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_p\}$ dos sistemas de igual número de vectores cuyos rangos respectivos son r y s. Considerar el sistema $T = \{\vec{w}_i = \vec{u}_i + \vec{v}_i \mid i = 1, 2, \ldots, p\}$. Probar que $\mathsf{rang}\ T \leq r + s$.

3.31. Sean V_1 y V_2 dos espacios vectoriales (con el mismo cuerpo de escalares) y considérese el producto cartesiano $V_1 \times V_2$, en el que se definen la suma y el producto por un escalar mediante:

$$\begin{gathered} (\vec{v}_1, \vec{v}_2) + (\vec{u}_1, \vec{u}_2) = (\vec{v}_1 + \vec{u}_1, \vec{v}_2 + \vec{u}_2) \\ \lambda(\vec{v}_1, \vec{v}_2) = (\lambda\vec{v}_1, \lambda\vec{v}_2) \end{gathered}$$

Probar que con esas operaciones el conjunto $V_1 \times V_2$ es un espacio vectorial. Si V_1 y V_2 tienen dimensión finita, probar que

$$\dim(V_1 \times V_2) = \dim V_1 + \dim V_2$$

3.32. Probar que el conjunto $\mathscr{C}(\mathbb{R}, \mathbb{R})$, de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$, es un espacio vectorial real respecto de las operaciones usuales.

3.33. Considerar el espacio vectorial $V = \mathscr{M}_2$, de las matrices cuadradas de tamaño 2×2, y sea $S = (M_1, M_2, M_3, M_4)$ el sistema formado por las matrices:

$$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad M_4 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

a) Comprobar que S es una base de V.

b) Hallar las coordenadas x_1, x_2, x_3, x_4 en la base S de una matriz genérica M de V:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

3.34. Hallar los valores que hay que asignar al parámetro α para que las siguientes matrices no formen base del espacio vectorial $\mathscr{M}_2$, de las matrices cuadradas de tamaño 2×2:

$$\begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 6 & 5 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & \alpha \end{pmatrix}$$

3.35. En el espacio vectorial de las matrices reales y simétricas de tamaño 3×3, se consideran las matrices:

$$M_1 = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & 4 \\ -1 & 4 & -2 \end{pmatrix} \quad M_2 = \begin{pmatrix} 2 & 4 & -2 \\ 4 & 6 & 8 \\ -2 & 8 & -4 \end{pmatrix} \quad M_3 = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 6 \\ 2 & 6 & 0 \end{pmatrix}$$

$$M_4 = \begin{pmatrix} 1 & 4 & 5 \\ 4 & 1 & 8 \\ 5 & 8 & 2 \end{pmatrix} \quad M_5 = \begin{pmatrix} 2 & 7 & 3 \\ 7 & 3 & 9 \\ 3 & 9 & 1 \end{pmatrix}$$

Hallar la dimensión y una base del subespacio que engendran estas 5 matrices. Obtener las coordenadas de todas ellas en la base elegida.

3.36. En el espacio vectorial $V = \mathscr{F}(\mathbb{R}, \mathbb{R})$, de las funciones de $\mathbb{R}$ en $\mathbb{R}$, se considera el sistema de funciones:

$$S = \{1, \sin x, \cos x, \sin 2x, \cos 2x\}$$

a) Comprobar que S es LI.

b) Hallar una base B del subespacio que engendran las funciones:

$$\begin{aligned} f_1(x) &= 1 - 2\sin x + 3\cos x - \sin 2x \\ f_2(x) &= \sin x + \cos x - 2\sin 2x - \cos 2x \\ f_3(x) &= 2 - \cos x + \sin 2x + 3\cos 2x \\ f_4(x) &= 1 + 4\sin x - 2\cos x - 2\sin 2x + \cos 2x \\ f_5(x) &= 4 + \sin x - \cos x + 5\cos 2x \end{aligned}$$

c) Completar la base B hasta obtener una base del subespacio engendrado por S.

3.37. En el espacio vectorial $V = \mathscr{M}_2$, de las matrices reales de tamaño 2×2, se consideran los sistemas $S = (M_1, M_2, M_3, M_4)$ y $T = (N_1, N_2, N_3, N_4, N_5)$, donde:

$$M_1 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \quad M_3 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & -1 \\ 3 & -2 \end{pmatrix}$$

$$N_1 = \begin{pmatrix} -2 & 1 \\ 3 & -2 \end{pmatrix} \; N_2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \; N_3 = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix} \; N_4 = \begin{pmatrix} 0 & 4 \\ 2 & 1 \end{pmatrix} \; N_5 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

Comprobar si S y T son sistemas equivalentes. Hallar bases de los subespacios que engendran S y T.

3.38. Sea A una matriz cuadrada de tamaño $n \times n$; sean $C_1, C_2, \ldots, C_p$ matrices columna de tamaño $n \times 1$. Probar que:

a) Si los vectores columna $AC_1, AC_2, \ldots, AC_p$ son LI, entonces $C_1, C_2, \ldots, C_p$ también son LI.

b) Si A tiene inversa y $C_1, C_2, \ldots, C_p$ son LI, entonces $AC_1, AC_2, \ldots, AC_p$ también son LI.

3.39. En el espacio vectorial $\mathscr{F}(\mathbb{R}, \mathbb{R})$, de las funciones de $\mathbb{R}$ en $\mathbb{R}$, se consideran las funciones

$$f_1(x) = e^{a_1 x}, f_2(x) = e^{a_2 x}, \ldots, f_n(x) = e^{a_n x}$$

Comprobar que si estas n funciones son linealmente independientes, entonces los números reales $a_1, \ldots, a_n$ son todos distintos.