Capítulo II.1

Preliminares

1. Sea p un numero primo. Demostrar que $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo con las operaciones definidas como
$$[a] + [b] := [a + b], \quad [a] \cdot [b] := [ab].$$

Solución. *En primer lugar, comprobemos que las operaciones $+$ y $\cdot$ están bien definidas, es decir, no dependen del representante de la clase elegida. Para ello, veamos que si $[a] = [c]$ y $[b] = [d]$, entonces $[a + b] = [c + d]$ en $\mathbb{Z}_p$. En efecto, dado que $a - c = mp$ y $b - d = np$ para ciertos enteros m, n, se tiene que*

$$a + b - (c + d) = (a - c) + (b - d) = mp + np = (m + n)p,$$

de donde se concluye que $[a + b] = [c + d]$ en $\mathbb{Z}_p$. Por otro lado, veamos que $[ab] = [cd]$. Se tiene que

$$ab - cd = (c + mp)b - c(b - np) = cb + mpb - cb + cnp = (mb + cn)p,$$

de donde se deduce que $[ab] = [cd]$ en $\mathbb{Z}_p$.

En segundo lugar, comprobamos si ocurre que $(\mathbb{Z}_p, +, \cdot)$ sea un anillo conmutativo unitario para el que todos sus elementos salvo la clase nula son invertibles, o no. Para ello,

1. *Veamos que $(\mathbb{Z}_p, +)$ es un grupo abeliano, para lo que se utilizará que $(\mathbb{Z}, +)$ es un grupo abeliano:*
   a) *Dados $[a], [b], [c]$ en $\mathbb{Z}_p$ se tiene que*
   $$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c]$$
   $$= [a] + ([b] + [c]).$$
   b) *Existe un elemento neutro que es $[0]$ puesto que para cada $[a] \in \mathbb{Z}_p$*
   $$[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a],$$

c) Dado $[a] \in \mathbb{Z}_p$*, el elemento* $[-a] \in \mathbb{Z}_p$ *es elemento inverso de* $[a]$ *ya que*

$$[a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a].$$

Hasta aquí tenemos que $(\mathbb{Z}_p, +)$ *es un grupo.*

d) Dados $[a], [b] \in \mathbb{Z}_p$ *se tiene que* $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

Por tanto, $(\mathbb{Z}_p, +)$ *es también abeliano.*

2. $(\mathbb{Z}_p, \cdot)$ *es un semigrupo. En efecto, dados* $[a], [b], [c] \in \mathbb{Z}_p$ *se tiene que*

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c]).$$

3. *Para todos* $[a], [b], [c]$ *en* $\mathbb{Z}_p$ *se cumple que*

$$[a]\cdot([b]+[c]) = [a]\cdot[b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a]\cdot[b]+[a]\cdot[c],$$

y también

$$([b]+[c])\cdot[a] = [b+c]\cdot[a] = [(b+c)a] = [ba+ca] = [ba]+[ca] = [b]\cdot[a]+[c]\cdot[a].$$

Veamos a continuación que $(\mathbb{Z}_p, +, \cdot)$ *es unitario. Para ello, consideramos* $[1] \in \mathbb{Z}_p$*. Se tiene que para cualquier* $[a] \in \mathbb{Z}_p$

$$[1] \cdot [a] = [1\, a] = [a] = [a\, 1] = [a] \cdot [1], \text{ siendo además } [1a] = [a].$$

Se hace notar que hasta el momento no se ha necesitado que p *sea un número primo. Por último, comprobemos que todos sus elementos salvo la clase nula son invertibles. Para ello, haremos uso del resultado clásico conocido como el Teorema de Bézout que afirma*

Teorema de Bézout. Sean $a, b \in \mathbb{Z}$*. Existen* $u, v \in \mathbb{Z}$ *tal que* $ua + vb = \mathrm{mcd}(a, b)$.

En el caso que nos concierne, tomamos $b = p$*. Al ser* p *primo y considerando* $0 < a < p$ *se tiene que existen* $u, v \in \mathbb{Z}$ *tal que*

$$au + vp = \mathrm{mcd}(a, p) = 1,$$

con lo que

$$[au + vp] = [1] \Rightarrow [a] \cdot [u] + [v] \cdot [p] = [a] \cdot [u] + [v] \cdot [0] = [a] \cdot [u] = [1],$$

de donde se deduce que $[a]^{-1} = [u]$.

Observación. Para obtener $[u]$ *se puede aplicar el algoritmo de Euclides reiteradamente de la siguiente forma:*

$$\begin{aligned} p &= a \cdot q_1 + r_1 \\ a &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ &\vdots \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1} \cdot q_n + 1. \end{aligned}$$

El último valor 1 se obtiene como consecuencia de que $\mathrm{mcd}(a,p)=1$. *Despejando* r_i

$$\begin{aligned} p-a\cdot q_1 &= r_1\\ a-r_1\cdot q_2 &= r_2\\ r_1-r_2\cdot q_3 &= r_3\\ &\vdots\\ r_{n-3}-r_{n-2}\cdot q_{n-1} &= r_{n-1}\\ r_{n-2}-r_{n-1}\cdot q_n &= 1. \end{aligned}$$

Ahora, sustituyendo de forma regresiva en las igualdades anteriores se llega al valor de $[u]$ *obteniendo* $ua+vp=1$.

Observación. Alternativamente se puede utilizar el Teorema pequeño de Fermat (véase, por ejemplo, [15, 17]) •

2. Determinar $[305]^{-1}$ en $\mathbb{Z}_{307}$.

   Solución. *Teniendo en cuenta el ejercicio anterior,* $\mathbb{Z}_{307}$ *es un cuerpo pues* $p=307$ *es primo. Por tanto existe* $[305]^{-1}$ *en* $\mathbb{Z}_{307}$. *Seguimos el algoritmo de Euclides extendido, con* $a=305$. *Se tiene que*

$$\begin{aligned} 307 &= 305\cdot 1+2\\ 305 &= 2\cdot 152+1 \end{aligned}$$

de donde

$$\begin{aligned} 307-305\cdot 1 &= 2\\ 305-2\cdot 152 &= 1 \end{aligned}$$

con lo que

$$153\cdot a-152\cdot p=1$$

de donde se concluye que $[a]^{-1}=[153]$ *en* $\mathbb{Z}_{307}$. •

3. Dar un ejemplo de dos conjuntos no vacíos A, B para los que $A\times B\neq B\times A$.

   Solución. *Consideremos los conjuntos* $A=\{1\}$ *y* $B=\{2\}$. *El producto cartesiano* $A\times B=\{(1,2)\}$, *mientras que* $B\times A=\{(2,1)\}$, *por lo que* $A\times B\neq B\times A$. •

4. Demostrar que el conjunto $\mathbb{K}=\{a+b\mathrm{i}\,|\,a,b\in\mathbb{Z}\}$, con la suma y multiplicación de los números complejos, tiene estructura de anillo conmutativo unitario. ¿Es un cuerpo?
   A este anillo se le llama anillo de los enteros gaussianos y se representa por $\mathbb{Z}[\mathrm{i}]$ (véase Subsección I.1.1.2).

Solución. *En primer lugar, comprobamos que la suma y el producto de dos enteros gaussianos es de nuevo un número gaussiano. Para ello, consideremos* $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *en* $\mathbb{K}$. *Teniendo en cuenta que la suma y multiplicación de números enteros es un número entero, resulta que*

$$(a_1 + b_1\mathrm{i}) + (a_2 + b_2\mathrm{i}) = a_1 + a_2 + (b_1 + b_2)\mathrm{i} \in \mathbb{K},$$

$$(a_1 + b_1\mathrm{i}) \cdot (a_2 + b_2\mathrm{i}) = (a_1a_2 - b_1b_2) + (a_2b_1 + a_1b_2)\mathrm{i} \in \mathbb{K}.$$

Por otro lado, es claro que $(\mathbb{K}, +)$ *es un grupo abeliano. En efecto*

a) Dados $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *y* $a_3 + b_3\mathrm{i}$ *en* $\mathbb{K}$, *se tiene que*

$$\begin{aligned}((a_1 + b_1\mathrm{i}) + (a_2 + b_2\mathrm{i})) + (a_3 + b_3\mathrm{i}) &= ((a_1 + a_2) + (b_1 + b_2)\mathrm{i}) + (a_3 + b_3\mathrm{i})\\ = ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)\mathrm{i} &= (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))\mathrm{i}\\ &= (a_1 + b_1\mathrm{i}) + ((a_2 + b_2\mathrm{i}) + (a_3 + b_3\mathrm{i})).\end{aligned}$$

b) El elemento $0 = 0 + 0\mathrm{i}$, *que pertenece a* $\mathbb{K}$, *es elemento neutro, pues para todo* $a + b\mathrm{i} \in \mathbb{K}$

$$(a+b\mathrm{i})+(0+0\mathrm{i}) = (a+0)+(b+0)\mathrm{i} = a+b\mathrm{i} = (0+a)+(0+b)\mathrm{i} = (0+0\mathrm{i})+(a+b\mathrm{i}).$$

c) Dado $a + b\mathrm{i} \in \mathbb{K}$, *se tiene que* $(-a) + (-b)\mathrm{i} \in \mathbb{K}$ *es elemento inverso, ya que*

$$\begin{aligned}(a + b\mathrm{i}) + ((-a) + (-b)\mathrm{i}) &= (a + (-a)) + (b + (-b))\mathrm{i} = 0 + 0\mathrm{i} = 0\\ &= ((-a) + a) + ((-b) + b)\mathrm{i} = ((-a) + (-b)\mathrm{i}) + (a + b\mathrm{i}).\end{aligned}$$

d) Dados $a_1 + b_1\mathrm{i}$ *y* $a_2 + b_2\mathrm{i}$ *en* $\mathbb{K}$, *se tiene que*

$$(a_1+b_1\mathrm{i})+(a_2+b_2\mathrm{i}) = a_1+a_2+(b_1+b_2)\mathrm{i} = a_2+a_1+(b_2+b_1)\mathrm{i} = (a_2+b_2\mathrm{i})+(a_1+b_1\mathrm{i}).$$

La propiedad d) permite deducir que $\mathbb{K}$ *es un grupo abeliano. En segundo lugar, comprobamos que* $(\mathbb{K}, \cdot)$ *es un semigrupo. Para ello, se comprueba que dados* $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *y* $a_3 + b_3\mathrm{i}$ *en* $\mathbb{K}$, *entonces*

$$\begin{aligned}&((a_1 + b_1\mathrm{i}) \cdot (a_2 + b_2\mathrm{i})) \cdot (a_3 + b_3\mathrm{i}) = ((a_1a_2 - b_1b_2) + (a_2b_1 + a_1b_2)\mathrm{i}) \cdot (a_3 + b_3\mathrm{i})\\ &= ((a_1a_2 - b_1b_2)a_3 - (a_2b_1 + a_1b_2)b_3) + ((a_1a_2 - b_1b_2)b_3 + (a_2b_1 + a_1b_2)a_3)\mathrm{i}.\end{aligned}$$

Por otro lado,

$$\begin{aligned}&(a_1 + b_1\mathrm{i}) \cdot ((a_2 + b_2\mathrm{i}) \cdot (a_3 + b_3\mathrm{i})) = (a_1 + b_1\mathrm{i}) \cdot ((a_2a_3 - b_2b_3) + (a_3b_2 + a_2b_3)\mathrm{i})\\ &= (a_1(a_2a_3 - b_2b_3) - b_1(a_3b_2 + a_2b_3)) + (a_1(a_3b_2 + a_2b_3) + b_1(a_2a_3 - b_2b_3))\mathrm{i}.\end{aligned}$$

Basta tener en cuenta las propiedades sobre los números enteros para concluir que

$$(a_1a_2 - b_1b_2)a_3 - (a_2b_1 + a_1b_2)b_3 = a_1(a_2a_3 - b_2b_3) - b_1(a_3b_2 + a_2b_3),$$

$$(a_1a_2 - b_1b_2)b_3 + (a_2b_1 + a_1b_2)a_3 = a_1(a_3b_2 + a_2b_3) + b_1(a_2a_3 - b_2b_3),$$

por lo que se deduce que

$$((a_1 + b_1\mathrm{i}) \cdot (a_2 + b_2\mathrm{i})) \cdot (a_3 + b_3\mathrm{i}) = (a_1 + b_1\mathrm{i}) \cdot ((a_2 + b_2\mathrm{i}) \cdot (a_3 + b_3\mathrm{i})).$$

Así mismo, comprobamos que para $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *y* $a_3 + b_3\mathrm{i}$ *en* $\mathbb{K}$,

$$\begin{aligned}(a_1 + b_1\mathrm{i}) \cdot ((a_2 + b_2\mathrm{i}) + (a_3 + b_3\mathrm{i})) &= (a_1 + b_1\mathrm{i}) \cdot ((a_2 + a_3) + (b_2 + b_3)\mathrm{i}) \\ &= (a_1(a_2 + a_3) - b_1(b_2 + b_3)) + (a_1(b_2 + b_3) + b_1(a_2 + a_3))\mathrm{i}\end{aligned}$$

que coincide con

$$\begin{aligned}&((a_1 + b_1\mathrm{i}) \cdot (a_2 + b_2\mathrm{i})) + ((a_1 + b_1\mathrm{i}) \cdot (a_3 + b_3\mathrm{i})) \\ &\quad = ((a_1a_2 - b_1b_2) + (b_1a_2 + a_1b_2)\mathrm{i}) + ((a_1a_3 - b_1b_3) + (b_1a_3 + a_1b_3)\mathrm{i}) \\ &\quad\quad = ((a_1a_2 - b_1b_2) + (a_1a_3 - b_1b_3)) + ((b_1a_2 + a_1b_2) + (b_1a_3 + a_1b_3))\mathrm{i}\end{aligned}$$

sin más que igualar parte real e imaginaria, ya que

$$a_1(a_2 + a_3) - b_1(b_2 + b_3) = (a_1a_2 - b_1b_2) + (a_1a_3 - b_1b_3),$$

$$a_1(b_2 + b_3) + b_1(a_2 + a_3) = (b_1a_2 + a_1b_2) + (b_1a_3 + a_1b_3).$$

Similarmente, se comprueba que para $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *y* $a_3 + b_3\mathrm{i}$ *en* $\mathbb{K}$, *se cumple que*

$$((a_1 + b_1\mathrm{i}) + (a_2 + b_2\mathrm{i})) \cdot (a_3 + b_3\mathrm{i}) = (a_1 + b_1\mathrm{i}) \cdot (a_3 + b_3\mathrm{i}) + (a_2 + b_2\mathrm{i}) \cdot (a_3 + b_3\mathrm{i}).$$

Además, para $a_1 + b_1\mathrm{i}$, $a_2 + b_2\mathrm{i}$ *en* $\mathbb{K}$, *se verifica que*

$$(a_1 + b_1\mathrm{i}) \cdot (a_2 + b_2\mathrm{i}) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)\mathrm{i} = (a_2 + b_2\mathrm{i})(a_1 + b_1\mathrm{i}).$$

Por tanto, $(\mathbb{K}, +, \cdot)$ *es un anillo conmutativo. Por otra parte,* $1 = 1 + 0\mathrm{i} \in \mathbb{K}$ *y para todo* $a + b\mathrm{i} \in \mathbb{K}$ *se cumple que*

$$(a + b\mathrm{i}) \cdot 1 = a + b\mathrm{i} = 1 \cdot (a + b\mathrm{i}).$$

De todo ello se concluye que $(\mathbb{K}, +, \cdot)$ *es un anillo conmutativo unitario.*

Finalmente, es claro que $(\mathbb{K}, +, \cdot)$ *no es un cuerpo ya que, por ejemplo, el elemento* $0 + 2\mathrm{i} \in \mathbb{K}$ *no admite elemento inverso respecto* $a \cdot$ *en* $\mathbb{K}$. *De lo contrario, existen* $a, b \in \mathbb{Z}$ *con*

$$(0 + 2\mathrm{i}) \cdot (a + b\mathrm{i}) = 1 + 0\mathrm{i},$$

de donde se deduce que $-2b + 2a\mathrm{i} = 1 + 0\mathrm{i}$. *Igualando parte real e imaginaria, debería ser* $-2b = 1$ *lo que no es posible para ningún* $b \in \mathbb{Z}$. *Por tanto, el elemento* $0 + 2\mathrm{i}$ *no es invertible respecto* $a \cdot$ *en* $\mathbb{K}$, *y* $\mathbb{K}$ *no es un cuerpo.* •

5. Demostrar que el conjunto $\mathbb{K} = \{a + b\mathrm{i} \,|\, a, b \in \mathbb{Q}\}$, con la suma y multiplicación de los números complejos, tiene estructura de cuerpo.
A este cuerpo se le llama cuerpo de los racionales gaussianos y se representa por $\mathbb{Q}[\mathrm{i}]$ (véase Subsección I.1.1.2).

   Solución. *La demostración de que* $(\mathbb{K}, +, \cdot)$ *es un anillo conmutativo unitario es análoga a la del ejercicio anterior, utilizando en este caso las propiedades de anillo conmutativo unitario de* $(\mathbb{Q}, +, \cdot)$. *Por tanto, solo falta comprobar que todo elemento no nulo de* $\mathbb{K}$ *es invertible respecto a la multiplicación. Sea* $a + b\mathrm{i} \in \mathbb{K} \setminus \{0\}$. *Entonces, a y b no pueden ser ambos nulos, lo que es equivalente a que* $a^2 + b^2 \neq 0$. *Consideremos el elemento*

$$\lambda := \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\mathrm{i},$$

   que es un elemento de $\mathbb{K}$, *según la consideración previa. Ahora bien,*

$$(a + b\mathrm{i}) \cdot \lambda = \left(a\frac{a}{a^2 + b^2} - b\frac{-b}{a^2 + b^2}\right) + \left(a\frac{-b}{a^2 + b^2} + b\frac{a}{a^2 + b^2}\right)\mathrm{i} = 1 + 0\mathrm{i} = 1.$$

   De la misma forma,

$$\lambda \cdot (a + b\mathrm{i}) = 1,$$

   con lo que se deduce que λ *es elemento inverso de* $a + b\mathrm{i}$ *respecto a la multiplicación. De aquí se concluye que* $(\mathbb{K}, +, \cdot)$ *es un cuerpo.* •

6. ¿Es $[10] = [3]$ en $\mathbb{Z}_7$?

   Solución. *Como* $10 - 3 = 7 = 0 \, mod \, 7$, *aplicando la Proposición I.1.1.2 (3) y Ejemplo I.1.1.4, se deduce que* $[10] = [3]$ *en* $\mathbb{Z}_7$. •

7. Construir las tablas de sumar y multiplicar de $\mathbb{Z}_3$.

   Solución. *Las propiedades de suma y producto en* $\mathbb{Z}_3$ *permiten deducir que*

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

   •

8. En $\mathbb{Z}_5$ determinar $([1] + [3]^3)/[2]$.

   Solución. *Se tiene que*

$$[3]^3 = ([3] \cdot [3]) \cdot [3] = [9] \cdot [3] = [4] \cdot [3] = [12] = [2]$$

en $\mathbb{Z}_5$. *Por otro lado, se tiene que* $[2]\cdot[3]=[3]\cdot[2]=[6]=[1]$ *en* $\mathbb{Z}_5$, *por lo que* $[2]^{-1}=[3]$. *Se concluye que*

$$([1]+[3]^3)/[2]=([1]+[2])/[2]=[3]\cdot[2]^{-1}=[3]\cdot[3]=[4].$$

•

9. Obtener $[99]^{-1}$ en $\mathbb{Z}_{101}$.

   Solución. *Aplicamos el algoritmo para obtener la identidad de Bézout (véase la solución del Ejercicio 1 de este capítulo)*

$$\left.\begin{array}{l}\overbrace{101}^{p}=\overbrace{99}^{a}\cdot 1+\overbrace{2}^{r_1}\\ \underbrace{99}_{a}=\underbrace{2}_{r_1}\cdot 49+\underbrace{1}_{r_2}\end{array}\right\}\Rightarrow\left.\begin{array}{r}r_1=p-a\cdot 1\\ r_2=a-r_1\cdot 49\end{array}\right\}\Rightarrow 1=r_2=a-(p-a)\,49=50\,a-49\,p$$

   de donde $[99]^{-1}=[50]$ *en* $\mathbb{Z}_{101}$. •

10. Obtener $[9]^{-1}$ en $\mathbb{Z}_{11}$.

    Solución. *Aplicamos el algoritmo para obtener la identidad de Bézout (véase la solución del Ejercicio 1 de este capítulo)*

$$\left.\begin{array}{l}\overbrace{11}^{p}=\overbrace{9}^{a}\cdot 1+\overbrace{2}^{r_1}\\ \underbrace{9}_{a}=\underbrace{2}_{r_1}\cdot 4+\underbrace{1}_{r_2}\end{array}\right\}\Rightarrow\left.\begin{array}{r}r_1=p-a\cdot 1\\ r_2=a-r_1\cdot 4\end{array}\right\}\Rightarrow 1=r_2=a-(p-a)\,4=5\,a-4\,p$$

    de donde $[9]^{-1}=[5]$ *en* $\mathbb{Z}_{11}$. •

11. Obtener $[8]^{-1}$ en $\mathbb{Z}_{13}$.

    Solución. *Aplicamos el algoritmo para obtener la identidad de Bézout (véase la solución del Ejercicio 1 de este capítulo)*

$$\left.\begin{array}{l}\overbrace{13}^{p}=\overbrace{8}^{a}\cdot 1+\overbrace{5}^{r_1}\\ \underbrace{8}_{a}=\underbrace{5}_{r_1}\cdot 1+\underbrace{3}_{r_2}\\ \underbrace{5}_{r_1}=\underbrace{3}_{r_2}\cdot 1+\underbrace{2}_{r_3}\\ \underbrace{3}_{r_2}=\underbrace{2}_{r_3}\cdot 1+\underbrace{1}_{r_4}\end{array}\right\}\Rightarrow\left.\begin{array}{r}r_1=p-a\\ r_2=a-r_1\\ r_3=r_1-r_2\\ r_4=r_2-r_3\end{array}\right\}\Rightarrow$$

$$\Rightarrow\left.\begin{array}{r}r_2=2a-p\\ r_3=p-a-r_2\\ r_4=r_2-r_3\end{array}\right\}\Rightarrow\left.\begin{array}{r}r_3=2p-3a\\ r_4=2a-p-r_3\end{array}\right\}\Rightarrow 1=r_4=5a-3p$$

    de donde $[8]^{-1}=[5]$ *en* $\mathbb{Z}_{13}$. •

12. Sean A y B dos matrices cuadradas de orden n sobre un cuerpo $\mathbb{K}$. Demostrar o refutar las siguientes afirmaciones

(i) $(A+B)^2 = A^2 + B^2 + 2AB$

(ii) $(A+B)^2 = A^2 + B^2 + AB + BA$

(iii) $(A+B)(A-B) = A^2 - B^2$

(iv) $(A+B)(A-B) = A^2 - B^2 + BA - AB$

(v) $(A+B)(A-B) = A^2 - B^2 - BA + AB$

(vi) $AB = BA$

(vii) Si $AB = \mathbf{0}$ entonces $A = \mathbf{0}$ o $B = \mathbf{0}$.

(viii) $\det(A+B) = \det(A) + \det(B)$.

(ix) AA^T es simétrica.

Solución.

(i) Se tiene que $(A+B)^2 = (A+B)(A+B) = A(A+B) + B(A+B) = A^2 + AB + BA + B^2$*, que no siempre coincide con* $A^2 + B^2 + 2AB$*. Basta considerar* A, B *con* $AB \neq BA$*, por ejemplo,*

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \tag{II.1.1}$$

siendo

$$(A+B)^2 = \begin{pmatrix} 6 & 4 \\ 2 & 2 \end{pmatrix} \neq \begin{pmatrix} 5 & 4 \\ 3 & 3 \end{pmatrix} = A^2 + B^2 + 2AB.$$

Por tanto, la afirmación no es cierta.

(ii) Como consecuencia del razonamiento del apartado anterior se deduce que la afirmación es cierta.

(iii) Se tiene que

$$(A+B)(A-B) = A(A-B) + B(A-B) = A^2 - AB + BA - B^2,$$

que no coincide con $A^2 - B^2$ *salvo que* A *y* B *conmuten. Tomando* A *y* B *como en* (II.1.1) *se tiene que*

$$(A+B)(A-B) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = A^2 - B^2.$$

Por tanto, la afirmación no es cierta.

(iv) Como consecuencia del razonamiento del apartado anterior se deduce que la afirmación es cierta.

(v) *El enunciado es cierto siempre que* $A^2-B^2+BA-AB = A^2-B^2-BA+AB$, *es decir,* $AB = BA$. *Tomando* A, B *como en* (II.1.1), *se tiene que*

$$(A+B)(A-B) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix} = A^2 - B^2 - BA + AB.$$

Por tanto, la afirmación no es cierta.

(vi) *La afirmación no es cierta; elíjanse las matrices* A *y* B *como en* (II.1.1).

(vii) *La afirmación no es cierta. Basta considerar*

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

(viii) *Las matrices* A *y* B *del apartado anterior permiten deducir que la afirmación es falsa, puesto que*

$$\det(A+B) = \det(\mathrm{I}) = 1 \neq 0 = 0+0 = \det(A) + \det(B).$$

(ix) *Obsérvese que (véase Proposición I.1.2.2)*

$$(AA^T)^T = (A^T)^T A^T = AA^T,$$

por lo que AA^T *es una matriz simétrica y, por tanto, la afirmación es correcta.*

•

13. Sea A una matriz invertible. Determinar el valor de $\det(A)$ en función del valor de $\det(A^{-1})$.

Solución. *Obsérvese, de las propiedades de los determinantes, que*

$$1 = \det(\mathrm{I}) = \det(AA^{-1}) = \det(A)\det(A^{-1}),$$

de donde $\det(A^{-1}) = (\det(A))^{-1}$. •

14. Sea A una matriz ortogonal. Demostrar que $\det(A) = \pm 1$.

Solución. *Como* $A \cdot A^T = \mathrm{I}$, *aplicando la Proposición I.1.2.4 (1), (2), se deduce que* $\det(A)^2 = \det(\mathrm{I}) = 1$ *y, por tanto,* $\det(A) = \pm 1$. •

15. Demostrar que la matriz

$$\begin{pmatrix} \cos(t) & -\operatorname{sen}(t) \\ \operatorname{sen}(t) & \cos(t) \end{pmatrix}$$

es ortogonal.

Solución.

$$AA^T = \begin{pmatrix} \cos(t) & -\operatorname{sen}(t) \\ \operatorname{sen}(t) & \cos(t) \end{pmatrix} \begin{pmatrix} \cos(t) & \operatorname{sen}(t) \\ -\operatorname{sen}(t) & \cos(t) \end{pmatrix}$$
$$= \begin{pmatrix} \cos^2(t) + \operatorname{sen}^2(t) & 0 \\ 0 & \cos^2(t) + \operatorname{sen}^2(t) \end{pmatrix} = \mathrm{I},$$

para todo $t \in \mathbb{R}$. *Similarmente* $A^T A = \mathrm{I}$. •

16. Dos matrices A, B cuadradas $n \times n$, con coeficientes en un cuerpo, se llaman semejantes si existe una matriz invertible P, de orden $n \times n$, tal que $A = P^{-1}BP$. Demostrar que si A y B son semejantes, entonces $\det(A) = \det(B)$.

    Solución. *Sean* A *y* B *semejantes, con* P *invertible cumpliendo* $A = P^{-1}BP$. *Entonces, de las propiedades del determinante*

$$\begin{aligned} \det(A) &= \det(P^{-1}BP) = \det(P^{-1})\det(B)\det(P) \\ &= \det(P)^{-1}\det(B)\det(P) = \det(P)^{-1}\det(P)\det(B) \\ &= \det(B). \end{aligned}$$

•

17. Dos matrices A, B cuadradas $n \times n$, con coeficientes en un cuerpo, se llaman congruentes si existe una matriz invertible P, de orden $n \times n$, tal que $A = P^T BP$. Demostrar que si A y B son congruentes, entonces $\det(A) = \det(P)^2\det(B)$.

    Solución. *Sean* A *y* B *congruentes, con* P *invertible cumpliendo* $A = P^T BP$. *Entonces*

$$\begin{aligned} \det(A) &= \det(P^T BP) = \det(P^T)\det(B)\det(P) \\ &= \det(P)\det(B)\det(P) = \det(P)^2\det(B). \end{aligned}$$

•

18. Calcular el determinante de las siguientes matrices

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ 0 & 0 & a_{3,3} & a_{3,4} \\ 0 & 0 & a_{4,3} & a_{4,4} \end{pmatrix}, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & 0 & 0 \\ a_{2,1} & a_{2,2} & 0 & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 & a_{1,3} & a_{1,4} \\ 0 & 0 & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{pmatrix}, \quad \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & 0 & 0 \\ a_{4,1} & a_{4,2} & 0 & 0 \end{pmatrix}$$

Solución. *Sean*

$$A_{11} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \quad A_{21} = \begin{pmatrix} a_{3,1} & a_{3,2} \\ a_{4,1} & a_{4,2} \end{pmatrix},$$
$$A_{12} = \begin{pmatrix} a_{1,3} & a_{1,4} \\ a_{2,3} & a_{2,4} \end{pmatrix}, \quad A_{22} = \begin{pmatrix} a_{3,3} & a_{3,4} \\ a_{4,3} & a_{4,4} \end{pmatrix}.$$

Las propiedades de los determinantes permiten deducir que el determinante de la primera matriz del enunciado coincide con

$$\begin{aligned} \det(A_{11})\det(A_{22}) - \det(\mathbf{0})\det(A_{12}) &= \det(A_{11})\det(A_{22}) \\ &= (a_{1,1}a_{2,2} - a_{2,1}a_{1,2})(a_{3,3}a_{4,4} - a_{4,3}a_{3,4}), \end{aligned}$$

mientras que el determinante de la segunda matriz es

$$\begin{aligned} \det(A_{11})\det(A_{22}) - \det(\mathbf{0})\det(A_{21}) &= \det(A_{11})\det(A_{22}) \\ &= (a_{1,1}a_{2,2} - a_{2,1}a_{1,2})(a_{3,3}a_{4,4} - a_{4,3}a_{3,4}). \end{aligned}$$

El determinante de la tercera matriz viene dado por

$$\begin{aligned} \det(\mathbf{0})\det(A_{22}) - \det(A_{21})\det(A_{12}) &= -\det(A_{21})\det(A_{12}) \\ &= -(a_{1,3}a_{2,4} - a_{2,3}a_{1,4})(a_{3,1}a_{4,2} - a_{4,1}a_{3,2}), \end{aligned}$$

mientras que el de la cuarta coincide con el valor del anterior determinante. •

19. Calcular el determinante de las siguientes matrices

a)
$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1+\alpha_1 & 1 & \cdots & 1 \\ 1 & 1 & 1+\alpha_2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1+\alpha_{n-1} \end{pmatrix}$$

b)
$$\begin{pmatrix} 1 & n & n & n & \cdots & n \\ n & 2 & n & n & \cdots & n \\ n & n & 3 & n & \cdots & n \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n & n & n & n & \cdots & n \end{pmatrix}$$

c)

$$\begin{pmatrix} 1-t & 1 & \cdots & 1 \\ 1 & 1-t & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1-t \end{pmatrix}$$

Solución. *Respecto al determinante de la primera matriz del enunciado, se tiene que éste no varía si se considera la columna j-ésima y se sustituye por dicha columna menos la primera, para cada $j \neq 1$, teniendo en cuenta las propiedades de los determinantes. Por ello, dicho determinante coincide con el de la matriz*

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_1 & 0 & \cdots & 0 \\ 1 & 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & \alpha_{n-1} \end{pmatrix}$$

cuyo determinante es $\alpha_1\alpha_2\cdots\alpha_{n-1}$.

En cuanto a la segunda matriz, se tiene que, al sustituir la columna j-ésima por ésta menos la columna n-ésima, para $j \neq n$, queda la matriz

$$\begin{pmatrix} 1-n & 0 & 0 & 0 & \cdots & n \\ 0 & 2-n & 0 & 0 & \cdots & n \\ 0 & 0 & 3-n & 0 & \cdots & n \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & n \end{pmatrix}$$

cuyo determinante coincide con el de la matriz del enunciado y viene dado por

$$n(n-1-n)(n-2-n)\cdots(3-n)(2-n)(1-n) = n!(-1)^{n-1}.$$

En cuanto a la tercera matriz, se observa que la suma de todas las columnas es $n-t$, por lo que podemos sustituir la primera columna por la suma de todas las columnas sin modificar el valor del determinante. Así, el determinante de la matriz coincide con el de

$$\begin{pmatrix} n-t & 1 & \cdots & 1 \\ n-t & 1-t & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ n-t & 1 & \cdots & 1-t \end{pmatrix},$$