

# Álgebra I

## Parcial VI



**Los Del DGIIM**, [losdeldgiim.github.io](https://losdeldgiim.github.io)

Doble Grado en Ingeniería Informática y Matemáticas  
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

# Álgebra I

# Parcial VI

Los Del DGIIM, [losdeldgiim.github.io](https://losdeldgiim.github.io)

José Juan Urrutia Milán

Granada, 2023-2024

**Asignatura** Álgebra I.

**Curso Académico** 2024-25.

**Grado** Grado en Matemáticas.

**Grupo** Único.

**Profesor** María del Pilar Carrasco Carrasco.

**Descripción** Parcial I

**Fecha** 14 de noviembre de 2024.

Los puntos de los ejercicios se reparten de forma equitativa entre los apartados.

**Ejercicio 1** (3 puntos).

- (a) Sean  $P, Q, R$  propiedades referidas a los elementos de un conjunto  $X$ . Supongamos que  $P \implies \neg R$ . Demostrar la siguiente equivalencia:

$$(P \vee Q) \wedge \neg R \iff P \vee (Q \wedge \neg R)$$

- (b) Sean  $f : X \rightarrow Y$  y  $g : Y \rightarrow Z$  aplicaciones componibles. Demosotrar que si  $f$  y  $g$  son biyectivas entonces  $g \circ f : X \rightarrow Z$  es biyectiva. Demostrar que, en tal caso,  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

- (c) Sea  $X = \{0, 2, 4\}$ . En el conjunto  $X \times X$  definimos la relación binaria  $\sim$ :

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Demostrar que  $\sim$  es una relación de equivalencia y calcular (describiendo todas las clases de equivalencia) el conjunto cociente  $X \times X / \sim$ .

- (a) Sean  $X_P, X_Q$  y  $X_R$  los subconjuntos de  $X$  conformados por los elementos que verifican la propiedad  $P, Q$  y  $R$  respectivamente. Puesto que  $P \implies \neg R$ , se tiene que  $X_P \subseteq X_{\neg R} = c(X_R)$ . Se trata de demostrar que:

$$(X_P \cup X_Q) \cap c(X_R) = X_P \cup (X_Q \cap c(X_R))$$

aplicando la propiedad distributiva de la intersección:

$$(X_P \cup X_Q) \cap c(X_R) = (X_P \cap c(X_R)) \cup (X_Q \cap c(X_R)) \stackrel{(*)}{=} X_P \cup (X_Q \cap c(X_R))$$

Donde en  $(*)$  aplicamos que  $X_P \subseteq c(X_R)$ .

- (b) Partimos de que  $f : X \rightarrow Y$  y  $g : Y \rightarrow Z$  son biyectivas. Entonces:

$$\begin{aligned} \exists f^{-1} : Y \rightarrow X \text{ única tal que } f \circ f^{-1} = id_Y \wedge f^{-1} \circ f = id_X \\ \exists g^{-1} : Z \rightarrow Y \text{ única tal que } g \circ g^{-1} = id_Z \wedge g^{-1} \circ g = id_Y \end{aligned}$$

Se trata de probar que  $g \circ f : X \rightarrow Z$  es biyectiva. Para ello, consideramos la composición  $f^{-1} \circ g^{-1} : Z \rightarrow X$ . Se tiene entonces que:

$$\begin{aligned} (g \circ f) \circ (f^{-1} \circ g^{-1}) &\stackrel{(*)}{=} g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ (id_Y \circ g^{-1}) = g \circ g^{-1} = id_Z \\ (f^{-1} \circ g^{-1}) \circ (g \circ f) &\stackrel{(*)}{=} f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ (id_Y \circ f) = f^{-1} \circ f = id_X \end{aligned}$$

Donde en  $(*)$  hemos aplicado la propiedad asociativa de la composición. Por tanto,  $g \circ f : X \rightarrow Z$  tiene inversa y por consiguiente es biyectiva.

Además, como la inversa de una aplicación biyectiva es única, será

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

(c) Tenemos que:

$$X = \{0, 2, 4\} \quad X \times X = \{(a, b) \mid a, b \in X\}$$

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Para ver que  $\sim$  es una relación de equivalencia, hemos de ver:

**Propiedad reflexiva.**

Puesto que  $a + b = b + a$ , entonces:

$$(a, b) \sim (a, b) \quad \forall (a, b) \in X \times X$$

**Propiedad simétrica.**

Sean  $(a, b), (c, d) \in X \times X$ . Entonces:

$$(a, b) \sim (c, d) \iff a + d = b + c \iff d + a = c + b \iff (c, d) \sim (a, b)$$

**Propiedad transitiva.**

Supongamos que  $(a, b), (c, d), (e, f) \in X \times X$  de forma que  $(a, b) \sim (c, d)$  y  $(c, d) \sim (e, f)$ . Entonces:

$$\begin{aligned} & \left. \begin{array}{l} (a, b) \sim (c, d) \\ \wedge \\ (c, d) \sim (e, f) \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} a + d = b + c \\ \wedge \\ c + f = d + e \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} a + d + f = b + c + f \\ \wedge \\ c + f + b = d + e + b \end{array} \right. \\ & \Rightarrow a + d + f = d + e + b \Rightarrow a + f = e + b \Rightarrow (a, b) \sim (e, f) \end{aligned}$$

Demostrado que  $\sim$  es una relación de equivalencia, calculamos  $X \times X / \sim$ :

$$X \times X = \{(0, 0), (0, 2), (0, 4), (2, 0), (2, 2), (2, 4), (4, 0), (4, 2), (4, 4)\}$$

$$X \times X / \sim = \{[(a, b)] \mid (a, b) \in X \times X\}$$

Calculamos las diferentes clases:

$$\begin{aligned} [(0, 0)] &= \{(a, b) \in X \times X \mid (a, b) \sim (0, 0)\} = \{(a, b) \in X \times X \mid a = b\} \\ &= \{(0, 0), (2, 2), (4, 4)\} = [(2, 2)] = [(4, 4)] \\ [(0, 2)] &= \{(a, b) \in X \times X \mid (a, b) \sim (0, 2)\} = \{(a, b) \in X \times X \mid a + 2 = b\} \\ &= \{(0, 2), (2, 4)\} = [(0, 2)] = [(2, 4)] \\ [(0, 4)] &= \{(a, b) \in X \times X \mid (a, b) \sim (0, 4)\} = \{(a, b) \in X \times X \mid a + 4 = b\} \\ &= \{(0, 4)\} \\ [(2, 0)] &= \{(a, b) \in X \times X \mid (a, b) \sim (2, 0)\} = \{(a, b) \in X \times X \mid a = b + 2\} \\ &= \{(2, 0), (4, 2)\} = [(4, 2)] \\ [(4, 0)] &= \{(a, b) \in X \times X \mid (a, b) \sim (4, 0)\} = \{(a, b) \in X \times X \mid a = b + 4\} \\ &= \{(4, 0)\} \end{aligned}$$

Con lo que:

$$X \times X / \sim = \{[(0, 0)], [(0, 2)], [(0, 4)], [(2, 0)], [(4, 0)]\}$$

**Ejercicio 2** (4 puntos). Efectuar los siguientes cálculos:

- El resto de dividir  $18 \cdot 15 - 561 \cdot 15^2$  entre 13.
- $[2 \cdot (3^5 - 5^2)]^{-1}$  en  $\mathbb{Z}_7$ .
- $(2x^3 - 3x + 5)(3x - 2)$  en  $\mathbb{Z}_6[x]$ .
- $(7 - 4\sqrt{3})^{-1}$  en  $\mathbb{Z}[\sqrt{3}]$ .
- $(\frac{2}{3} - \frac{1}{9}\sqrt{-3})^{-1}$  en  $\mathbb{Q}[\sqrt{-3}]$ .

- Puesto que la aplicación

$$\begin{aligned} R : \mathbb{Z} &\longrightarrow \mathbb{Z}_{13} \\ a &\longmapsto R(a) := Res(a; 13) \end{aligned}$$

Es un homomorfismo de anillos, será:

$$\begin{aligned} Res(18 \cdot 15 - 561 \cdot 15^2; 13) &= Res(18; 13) \cdot Res(15; 13) - Res(561; 13) \cdot Res(15; 13)^2 \\ &\stackrel{(*)}{=} 5 \cdot 2 - 2 \cdot 2^2 = 10 - 8 = 2 \end{aligned}$$

Donde en (\*) hemos aplicado que  $561 = 13 \cdot 43 + 2$

- Para ello, primero calcularemos  $2 \cdot (3^5 - 5^2)$  en  $\mathbb{Z}_7$ :

- $3^5 = 5$  en  $\mathbb{Z}_7$  pues  $3^5 = 243 = 7 \cdot 34 + 5$
- $5^2 = 5$  en  $\mathbb{Z}_7$  pues  $5^2 = 25 = 7 \cdot 3 + 4$

Entonces:

$$2(3^5 - 5^2) = 2(5 - 4) = 2$$

Y solo queda calcular el inverso de 2 en  $\mathbb{Z}_7$ :

$$[2 \cdot (3^5 - 5^2)]^{-1} = 2^{-1} = 4$$

Ya que  $2 \cdot 4 = 8 = 1$  en  $\mathbb{Z}_7$ .

- $(2x^3 - 3x + 5)(3x - 2) = 6x^4 - 4x^3 - 9x^2 + 6x + 15x - 10 = 2x^3 + 3x^2 + 3x + 2$

- Puesto que

$$N(7 - 4\sqrt{3}) = (7 - 4\sqrt{3})(7 + 4\sqrt{3}) = 49 - 3 \cdot 16 = 49 - 48 = 1$$

Entonces tenemos que  $7 - 4\sqrt{3} \in U(\mathbb{Z}[\sqrt{3}])$  y:

$$(7 - 4\sqrt{3})^{-1} = 7 + 4\sqrt{3}$$

- (e) Sabemos que si  $0 \neq \alpha \in \mathbb{Q}[\sqrt{-3}]$  entonces tenemos que  $N(\alpha) \neq 0$  y  $\alpha^{-1} = \frac{1}{N(\alpha)}\bar{\alpha}$ .

Para  $\alpha = \frac{2}{3} - \frac{1}{9}\sqrt{-3}$ , será:

$$N(\alpha) = \frac{4}{9} + \frac{3}{81} = \frac{13}{27}$$

y entonces:

$$\left(\frac{2}{3} - \frac{1}{9}\sqrt{-3}\right)^{-1} = \frac{27}{13} \left(\frac{2}{3} + \frac{1}{9}\sqrt{-3}\right) = \frac{18}{13} + \frac{3}{13}\sqrt{-3}$$

**Ejercicio 3** (3 puntos). Sea  $f : A \rightarrow B$  un homomorfismo de anillos. Demostrar:

- (a)  $Img(f)$  es un subanillo de  $B$ .
- (b)  $f(n \cdot a) = n \cdot f(a)$ , para todo  $n \in \mathbb{Z}$  y todo  $a \in A$ .
- (c)  $f(u^n) = f(u)^n$ , para todo  $n \in \mathbb{Z}$  y todo  $u \in U(A)$ .

- (a) Sabemos que  $Img(f) = \{f(a) \mid a \in A\} \subseteq B$ .

Para demostrar que es un subanillo de  $B$  hemos de ver que es cerrado para sumas, productos, opuestos y que contiene al 1 de  $B$ .

Sean  $b_1, b_2 \in Img(f)$ , entonces  $\exists a_1, a_2 \in A$  tales que:

$$b_1 = f(a_1) \quad b_2 = f(a_2)$$

Entonces:

$$\begin{aligned} b_1 + b_2 &= f(a_1) + f(a_2) = f(a_1 + a_2) \in Img(f) \\ b_1 \cdot b_2 &= f(a_1)f(a_2) = f(a_1 \cdot a_2) \in Img(f) \end{aligned}$$

por lo que  $Img(f)$  es cerrado para sumas y productos. Para ver que es cerrado para opuestos, utilizamos que todo homomorfismo verifica que  $f(-a) = -f(a) \forall a \in A$ . Entonces:

$$\text{Si } b \in Img(f) \implies \exists a \in A \mid f(a) = b \implies -b = -f(a) = f(-a) \in Img(f)$$

Finalmente, como  $f(1) = 1 \in Img(f)$ , tenemos que  $Img(f)$  es un subanillo de  $B$ .

- (b) Distinguimos casos:

- Para  $n \geq 1$  y  $a \in A$ :  $n \cdot a = \overbrace{a + \dots + a}^{n \text{ veces}}$ , con lo que:

$$f(n \cdot a) = f(\overbrace{a + \dots + a}^{n \text{ veces}}) = \overbrace{f(a) + \dots + f(a)}^{n \text{ veces}} = n \cdot f(a)$$

- Para  $n = 0$  y  $a \in A$ , tenemos que  $0 \cdot a = 0$ , con lo que:

$$f(0 \cdot a) = f(0) = 0 = 0 \cdot f(a)$$

- Para  $n < 0$  y  $a \in A$ , tenemos que  $n \cdot a = (-n)(-a)$ , con lo que:

$$f(n \cdot a) = f((-n)(-a)) \stackrel{(*)}{=} (-n)f(-a) = (-n)(-f(a)) = n \cdot f(a)$$

Donde en (\*) usamos que  $-n > 0$ , con lo que podemos aplicar el primer apartado.

(c) Distinguimos casos:

- Para  $n \geq 1$  y  $a \in A$ :  $a^n = \overbrace{a \cdot \dots \cdot a}^{n \text{ veces}}$ , con lo que:

$$f(u^n) = f(\underbrace{u \cdot \dots \cdot u}_{n \text{ veces}}) = \overbrace{f(u) \cdot \dots \cdot f(u)}^{n \text{ veces}} = [f(u)]^n$$

- Para  $n = 0$  y  $a \in A$ ,  $a^0 = 1$ , con lo que:

$$f(u^0) = f(1) = 1 = [f(u)]^0$$

- Para  $n < 0$  y  $u \in U(A)$ ,  $u^n = (u^{-1})^{-n}$ .

Además, si  $u \in U(A) \implies \exists u^{-1} \in A \mid uu^{-1} = 1$ . Entonces:

$$1 = f(1) = f(uu^{-1}) = f(u)f(u^{-1})$$

y por tanto  $f(u) \in U(B)$  y  $f(u)^{-1} = f(u^{-1})$ . Entonces:

$$f(u^n) = f((u^{-1})^{-n}) \stackrel{(*)}{=} [f(u^{-1})]^{-n} = [f(u)^{-1}]^{-n} = f(u)^n$$

Donde en (\*) hemos usado que  $-n > 0$  y el primer apartado.