Álgebra I

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra I

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán
Arturo OlivaresMartos

Granada, 2023-2024

Índice

1. Cuestionarios

1.1. Cuestionario I

Ejercicio 1. Si A es un conjunto finito arbitrario, la afirmación "$|P(A)| > |A|$" es:

- Siempre verdadera.
- Verdadera o falsa, depende de A.
- Siempre falsa.

Ejercicio 2. Si A, B, C son conjuntos cualesquira con B y C disjuntos, selecciona la afirmación verdadera:

- $(A \cup B) \cap C = A$.
- $(A \cup B) \cap (A \cup C) = A$.
- $(A \cap B) \cup (A \cap C) = A$.

Ejercicio 3. Si A y B son subconjuntos de un conjunto, la afirmación "$c(A) \cap c(B) = c(A \cap B)$" es:

- Siempre cierta.
- Siempre falsa.
- A veces verdadera y a veces falsa, depende de A y B.

Ejercicio 4. Sean P y Q las propiedades referidas a los elementos de un conjunto. Las proposiciones $P \Rightarrow \neg Q$ y $Q \Rightarrow \neg P$ son:

- Siempre equivalentes.
- Nunca equivalentes.
- A veces equivalentes y a veces no, depende de P y de Q.

Ejercicio 5. Sean P, Q y R propiedades referidas a los elementos de un conjunto tal que $P \Rightarrow Q \vee R$, entonces (seleccionar la afirmación correcta):

- $P \Rightarrow Q$ y $P \Rightarrow R$.
- $P \Rightarrow Q$ o $P \Rightarrow R$.
- $P \Rightarrow Q$ siempre que $R \Rightarrow Q$.

Ejercicio 1. Si A es un conjunto finito arbitrario, la afirmación "$|P(A)| > |A|$" es:

- Siempre verdadera.
- Verdadera o falsa, depende de A.
- Siempre falsa.

Justificación: Si $A = \emptyset$, entonces $P(A) = \{\emptyset\}$ y $|P(A)| = 1 > 0 = |A|$.
Si $A \neq \emptyset$, entonces $P(A)$ contiene a todos los subconjuntos unitarios $\{a\}$, con $a \in A$ (luego, el cardinal de $P(A)$ es, como mínimo, igual al de $|A|$) y, además, contiene el subconjunto vacío, luego tiene al menos tantos elementos como A más uno.

Otra alternativa es usar la fórmula vista para el cardinal del conjunto potencia de un conjunto finito vista en teoría:
Sea A un conjunto finito arbitrario con $|A| = n \in \mathbb{N}$, entonces $|\mathcal{P}(A)| = 2^n$.
Notemos que $2^n > n \quad \forall n \in \mathbb{N}$.

Ejercicio 2. Si A, B, C son conjuntos cualesquira con B y C disjuntos, selecciona la afirmación verdadera:

- $(A \cup B) \cap C = A$.
- $(A \cup B) \cap (A \cup C) = A$.
- $(A \cap B) \cup (A \cap C) = A$.

Justificación:

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C) = A \cup \emptyset = A$$

Ejercicio 3. Si A y B son subconjuntos de un conjunto, la afirmación "$c(A) \cap c(B) = c(A \cap B)$" es:

- Siempre cierta.
- Siempre falsa.
- A veces verdadera y a veces falsa, depende de A y B.

Justificación: Por las Leyes de Morgan: $c(A \cap B) = c(A) \cup c(B)$, por lo que podemos intuir que la afirmación no siempre es cierta. Podemos dar un contraejemplo para ilustrarlo:
Sea $X = \{1, 2, 3, 4, 5\}$, sean $A = \{1, 2, 3\}$, $B = \{4, 5\} \subseteq X$:

$$c(A) = B \qquad c(B) = Ac(A \cap B) = c(\emptyset) = X \neq c(A) \cap c(B) = \emptyset$$

Además, como no impone nada sobre los conjuntos, podemos ver que si $A = B$, es cierta la afirmación. Supongamos que $A = B$:

$$c(A \cap B) = c(A \cap A) = c(A) = c(A) \cup c(A) = c(A) \cup c(B)$$

Ejercicio 4. Sean P y Q las propiedades referidas a los elementos de un conjunto. Las proposiciones $P \Rightarrow \neg Q$ y $Q \Rightarrow \neg P$ son:

- <u>Siempre equivalentes.</u>
- Nunca equivalentes.
- A veces equivalentes y a veces no, depende de P y de Q.

Justificación: $Q \Rightarrow \neg P$ es el contrarrecíproco de $P \Rightarrow \neg Q$.
Demostremos que $(Q \Rightarrow \neg P) \Leftrightarrow (P \Rightarrow \neg Q)$:
O, equivalentemente, que $X_Q \subseteq c(X_P) \Leftrightarrow X_P \subseteq c(X_Q)$.

$\Rightarrow)$ Sea $x \in X_P \Rightarrow x \notin c(X_P) \Rightarrow x \notin X_Q \Rightarrow x \in c(X_Q)$
Para todo $x \in X_P$, luego $X_P \subseteq c(X_Q)$.

$\Leftarrow)$ Sea $x \in X_Q \Rightarrow x \notin c(X_Q) \Rightarrow x \notin X_P \Rightarrow x \in c(X_P)$
Para todo $x \in X_Q$, luego $X_Q \subseteq c(X_P)$.

Ejercicio 5. Sean P, Q y R propiedades referidas a los elementos de un conjunto tal que $P \Rightarrow Q \vee R$, entonces (seleccionar la afirmación correcta):

- $P \Rightarrow Q$ y $P \Rightarrow R$.
- $P \Rightarrow Q$ o $P \Rightarrow R$.
- <u>$P \Rightarrow Q$ siempre que $R \Rightarrow Q$.</u>

Justificación: Por hipótesis, $X_P \subseteq X_Q \cup X_R$.
Si $X_R \subseteq X_Q \Rightarrow X_P \subseteq X_Q = X_Q \cup X_R$.

1.2. Cuestionario II

Ejercicio 1. Sean X e Y dos conjuntos finitos con $|X| = |Y|$ y $f : X \to Y$ una aplicación. La afirmación "Si f es inyectiva o sobreyectiva, entonces f es biyectiva" es:

- Verdadera o falsa, depende de f.
- Siempre verdadera.
- Siempre falsa.

Ejercicio 2. Sea $f : X \to Y$ una aplicación inyectiva y sean $A, B \subseteq X$. Selecciona la afirmación verdadera:

- $f_*(A) - f_*(B)$ es un subconjunto propio de $f_*(A - B)$.
- $f_*(A - B)$ es un subconjunto propio de $f_*(A) - f_*(B)$.
- $f_*(A - B) = f_*(A) - f_*(B)$.

Ejercicio 3. Sea $f : X \to X$ una aplicación tal que $f_*(c(A)) = c(f_*(A))$, para todo $A \in \mathcal{P}(X)$. Entonces:

- f es inyectiva, pero no necesariamente sobreyectiva.
- f es sobreyectiva, pero no necesariamente inyectiva.
- f es biyectiva.

Ejercicio 4. Sea X un conjunto con $|X| \geqslant 2$. La afirmación "Todo subconjunto de $X \times X$ es de la forma $A \times B$ para ciertos subconjuntos $A, B \subseteq X$" es:

- Verdadera o falsa, depende de X.
- Siempre verdadera.
- Siempre falsa.

Ejercicio 5. Sea R una relación simétrica y transitiva en un conjunto $X \neq \emptyset$ ¿Prueba el siguiente razonamiento que R es reflexiva?:
"Por simetría, aRb implica bRa y entonces, por transitividad, concluimos que aRa".

- Sí.
- No.

Ejercicio 1. Sean X e Y dos conjuntos finitos con $|X| = |Y|$ y $f : X \to Y$ una aplicación. La afirmación "Si f es inyectiva o sobreyectiva, entonces f es biyectiva" es:

- Verdadera o falsa, depende de f.
- <u>Siempre verdadera.</u>
- Siempre falsa.

Justificación: Si f es inyectiva, entonces $|X| = |Img(f)|$, luego $|Img(f)| = |Y|$ y por tanto, $Img(f) = Y$ y f es sobreyectiva luego biyectiva.
Si f es sobreyectiva, entonces $|Y| = |Img(f)|$, luego $|Img(f)| = |X|$ y por tanto, f es necesariamente inyectiva luego biyectiva.

Ejercicio 2. Sea $f : X \to Y$ una aplicación inyectiva y sean $A, B \subseteq X$. Selecciona la afirmación verdadera:

- $f_*(A) - f_*(B)$ es un subconjunto propio de $f_*(A - B)$.
- $f_*(A - B)$ es un subconjunto propio de $f_*(A) - f_*(B)$.
- <u>$f_*(A - B) = f_*(A) - f_*(B)$.</u>

Justificación: Empezamos recordando la definición de $f_*(A)$ para $A \subseteq X$:

$$f_*(A) = \{y \in X \mid \exists x \in X \text{ con } f(x) = y\}$$

$\subseteq$) Sea $y \in f_*(A - B) \Rightarrow \exists x \in A - B \mid y = f(x)$.
Esto es, $\exists x \in A \wedge x \notin B \mid y = f(x)$.
Como $x \in A \Rightarrow y = f(x) \in f_*(A)$. Además, por ser f inyectiva, se tiene que $y \notin f_*(B)$, ya que si suponemos que $y \in f_*(B)$:

$y \in f_*(B) \Rightarrow \exists b \in B \mid y = f(b) \Rightarrow f(x) = f(b)$ con lo que $x = b \in B$, en contradicción con que $x \notin B$.

Así, $y \in f_*(A) - f_*(B)$ para todo $y \in f_*(A - B)$. Luego:

$$f_*(A - B) \subseteq f_*(A) - f_*(B)$$

$\supseteq$) Sea $y \in f_*(A) - f_*(B) \Rightarrow y \in f_*(A) \wedge y \notin f_*(B)$.
Como $y \in f_*(A) \Rightarrow \exists x \in A \mid y = f(x)$.
Como $y \notin f_*(B) \Rightarrow x \notin B$.
Luego $x \in A - B \Rightarrow y = f(x) \in f_*(A - B)$ para todo $y \in f_*(A) - f_*(B)$. Luego:

$$f_*(A) - f_*(B) \subseteq f_*(A - B)$$

Ejercicio 3. Sea $f : X \to X$ una aplicación tal que $f_*(c(A)) = c(f_*(A))$, para todo $A \in \mathcal{P}(X)$. Entonces:

- f es inyectiva, pero no necesariamente sobreyectiva.

- f es sobreyectiva, pero no necesariamente inyectiva.
- f es biyectiva.

Justificación: Procedemos a demostrar la inyectividad y sobreyectividad de la aplicación.
Para la sobreyectividad, consideramos $\emptyset \in \mathcal{P}(X)$:

$$f_*(c(\emptyset)) = f_*(X) = Img(f) = c(f_*(\emptyset)) = c(\emptyset) = X$$

Para la inyectividad, podemos suponer sin perder generalidad que $|X| \geqslant 2$ (si no lo fuera, la aplicación sería automáticamente inyectiva).
Sean $x, x' \in X \mid x \neq x'$. Entonces, $x' \in c(\{x\})$ luego:

$$f(x') \in f_*(c(\{x\})) = c(\{f(x)\})$$

Luego $f(x') \neq f(x)$.

Ejercicio 4. Sea X un conjunto con $|X| \geqslant 2$. La afirmación "Todo subconjunto de $X \times X$ es de la forma $A \times B$ para ciertos subconjuntos $A, B \subseteq X$" es:

- Verdadera o falsa, depende de X.
- Siempre verdadera.
- Siempre falsa.

Justificación: Supongamos que sí y consideremos el siguiente conjunto:
Sea $D = \{(x, x) \mid x \in X\} \subseteq X \times X$.
Si $D = A \times B$ para ciertos $A, B \subseteq X$, entonces para todo $x \in X$, $(x, x) \in A \times B$ y, por tanto, $x \in A$ y $x \in B$.
Así que $A = X = B$ y, necesariamente, $D = X \times X$. Pero $|X| \geqslant 2$, luego existen $a, b \in X$ con $a \neq b$, esto es, $(a, b) \notin D$ y $D \neq X \times X$.
Lo que nos lleva a contradicción.

Ejercicio 5. Sea R una relación simétrica y transitiva en un conjunto $X \neq \emptyset$ ¿Prueba el siguiente razonamiento que R es reflexiva?:
"Por simetría, aRb implica bRa y entonces, por transitividad, concluimos que aRa".

- Sí.
- No.

Justificación: Dado un $a \in X$, no tiene por qué existir a priori un elemento $b \in X$ tal que aRb. Por tanto, buscamos un contraejemplo para desmentir la afirmación:

Dado $X = \{a, b, c\} \neq \emptyset$ y la relación $R = \{(a, b), (b, a), (b, b), (a, a)\} \subseteq X \times X$.
Observemos que R es simétrica y transitiva pero no reflexiva:
Es simétrica ya que para todos $\alpha, \beta \in X \mid \alpha R \beta \Rightarrow \beta R \alpha$:

Ya que aRb, ¿se cumple que bRa?. Sí.
Ya que bRa, ¿se cumple que aRb?. Sí.
Ya que bRb, ¿se cumple que bRb?. Sí.
Ya que aRa, ¿se cumple que aRa?. Sí.

Es transitiva ya que para todos $\alpha, \beta, \gamma \in X \mid \alpha R\beta \wedge \beta R\gamma \Rightarrow \alpha R\gamma$:

Ya que aRb y bRa, ¿se cumple que aRa?. Sí.
Ya que bRa y aRb, ¿se cumple que bRb?. Sí.
Ya que bRb y bRb, ¿se cumple que bRb?. Sí.
Ya que aRa y aRa, ¿se cumple que aRa?. Sí.

No es reflexiva, ya que $\exists c \in X \mid c \not R c$.

1.3. Cuestionario III

Ejercicio 1. Sea X un conjunto no vacío. Definimos en $\mathcal{P}(X)$ operaciones de suma y producto por $A + B = A \cup B$ y $A \cdot B = A \cap B$. Entonces (selecciona la respuesta correcta).

- $\mathcal{P}(X)$ es un anillo conmutativo.
- $\mathcal{P}(X)$ no es un anillo conmutativo, falla un axioma.
- $\mathcal{P}(X)$ no es un anillo conmutativo, fallan dos axiomas.

Ejercicio 2. Para enteros m y n tales que $2 \leqslant m < n$, la afirmación "$\mathbb{Z}_m$ es un subanillo de $\mathbb{Z}_n$" es:

- Verdadera o falsa, dependiendo de m y de n.
- Siempre verdadera.
- Siempre falsa.

Ejercicio 3. En el anillo $\mathbb{Z}_8$ (seleccion la afirmación verdadera).

- 3 es una unidad y $4 \cdot 3^{-1} = 4$.
- 3 es una unidad, pero $4 \cdot 3^{-1} \neq 4$.
- 3 no es una unidad.

Ejercicio 4. En el anillo $\mathbb{Z}[\sqrt{3}]$, la afirmación "$(7 + 4\sqrt{3})^n$ es una unidad para todo natural $n \geqslant 1$" es:

- Verdadera o falsa, dependiendo de n.
- Siempre verdadera.
- Siempre falsa.

Ejercicio 5. Sea $A \subseteq \mathbb{R}$ un subanillo. La afirmación "Z es un subanillo de A" es:

- Siempre verdadera.
- Siempre falsa.
- Verdadera o falsa, dependiendo de A.

Ejercicio 1. Sea X un conjunto no vacío. Definimos en $\mathcal{P}(X)$ operaciones de suma y producto por $A + B = A \cup B$ y $A \cdot B = A \cap B$. Entonces (selecciona la respuesta correcta).

- $\mathcal{P}(X)$ es un anillo conmutativo.
- $\mathcal{P}(X)$ no es un anillo conmutativo, falla un axioma.
- $\mathcal{P}(X)$ no es un anillo conmutativo, fallan dos axiomas.

Justificación: En este caso, $0 = \emptyset$, ya que:

$$\emptyset + A = \emptyset \cup A = A \quad \forall A \in \mathcal{P}(X)$$

Y no hay opuestos, sea $A \neq \emptyset \in \mathcal{P}(X)$:

$$A + B = A \cup B \supseteq A \neq \emptyset \quad \forall B \in \mathcal{P}(X)$$

Podemos ver que el resto de axiomas se cumplen:

- Conmutativa de la suma:
$$A + B = A \cup B = B \cup A = B + A \quad \forall A, B \in \mathcal{P}(X)$$
- Asociativa de la suma:
$$A + (B + C) = A \cup (B \cup C) = (A \cup B) \cup C = (A + B) + C \quad \forall A, B, C \in \mathcal{P}(X)$$
- Elemento neutro de la suma (ya demostrado).
- Existencia de opuestos (ya se ha visto que no se cumple).
- Conmutativa del producto:
$$A \cdot B = A \cap B = B \cap A = B \cdot A \quad \forall A, B \in \mathcal{P}(X)$$
- Asociativa del producto:
$$A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C \quad \forall A, B, C \in \mathcal{P}(X)$$
- Elemento neutro del producto:
$$A \cdot X = A \quad \forall A \in \mathcal{P}(X)$$
- Distributiva del producto respecto de la suma:
$$A \cdot (B + C) = A \cap (B \cup C) = (A \cap B) \cup (A \cap C) = (A \cdot B) + (A \cdot C) \quad \forall A, B, C \in \mathcal{P}(X)$$

Ejercicio 2. Para enteros m y n tales que $2 \leqslant m < n$, la afirmación "$\mathbb{Z}_m$ es un subanillo de $\mathbb{Z}_n$" es:

- Verdadera o falsa, dependiendo de m y de n.
- Siempre verdadera.
- Siempre falsa.

Justificación: En $\mathbb{Z}_m$, se tiene que $m = 0$.
Sin embargo, por ser $2 \leqslant m < n$, tenemos que $m \neq 0$ en $\mathbb{Z}_n$.

Ejercicio 3. En el anillo $\mathbb{Z}_8$ (seleccion la afirmación verdadera).

- 3 es una unidad y $4 \cdot 3^{-1} = 4$.
- 3 es una unidad, pero $4 \cdot 3^{-1} \neq 4$.
- 3 no es una unidad.

Justificación: 3 es una unidad ya que $3 \cdot 3 = 9 = 1$, luego $3^{-1} = 3$.
Entonces, $4 \cdot 3^{-1} = 4 \cdot 3 = 12 = 4$.

Ejercicio 4. En el anillo $\mathbb{Z}[\sqrt{3}]$, la afirmación "$(7 + 4\sqrt{3})^n$ es una unidad para todo natural $n \geqslant 1$" es:

- Verdadera o falsa, dependiendo de n.
- Siempre falsa.
- Siempre verdadera.

Justificación: Tenemos que $7 + 4\sqrt{3}$ es invertible, puesto que:

$$N(7 + 4\sqrt{3}) = 7^2 - 3 \cdot 16 = 49 - 48 = 1$$

Como el producto de unidades es una unidad, cualquier potencia de una unidad también lo es.

Ejercicio 5. Sea $A \subseteq \mathbb{R}$ un subanillo. La afirmación "Z es un subanillo de A" es:

- Siempre verdadera.
- Siempre falsa.
- Verdadera o falsa, dependiendo de A.

Justificación: Por inducción, veamos primero que $\mathbb{N} = \mathbb{Z}^+ \subseteq A$.
Esto es, que $n \in A \quad \forall n \in \mathbb{N}$.

$n = 0$: Por ser A subanillo de $\mathbb{R}$, se tiene que $0 \in A$.

$n = 1$: Por ser A subanillo de $\mathbb{R}$, se tiene que $1 \in A$.

$n > 1$: Como hipótesis de inducción, supongamos que $n \in A$ y veamos que $n+1 \in A$. Por ser A cerrado para la suma, tenemos que $1 \in A$ y que $n \in A$ por hipótesis de inducción, luego $n + 1 \in A$.

Por tanto, $\mathbb{N} = \mathbb{Z}^+ \subseteq A$.
Ahora, para $n \in \mathbb{Z}$ con $n \geqslant 0$, A es cerrado para opuestos, luego $-n \in A$.
Por tanto, $\mathbb{Z} \subseteq A$.

Por ser $\mathbb{Z}$ cerrado para la suma, producto, opuestos y contiene al 0 y al 1, $\mathbb{Z}$ es subanillo de A. Por tanto, $\mathbb{Z}$ es el menor subanillo de $\mathbb{R}$.

1.4. Cuestionario IV

Ejercicio 1. En el anillo $\mathbb{Z}_{10}$, la afirmación "$3^{4k+3} = -3$, para cualquier $k \in \mathbb{Z}$" es:

- Siempre falsa.
- Siempre cierta.
- A veces cierta y a veces falsa, depende de k.

Ejercicio 2. En el anillo $\mathbb{Z}_n[x]$, la afirmación "la suma reiterada n veces de cualquier polinomio es 0", es:

- Verdera o falsa, depende de n.
- Siempre falsa.
- Siempre verdadera.

Ejercicio 3. Un subanillo A de un anillo B se dice propio si $A \subsetneq B$. Seleccion el enunciado correcto:

- En anillo $\mathbb{Z}$ no tiene subanillos propios.
- El conjunto $A = \{5k \mid k \in \mathbb{Z}\}$ es un subanillo propio de $\mathbb{Z}$.
- El cuerpo $\mathbb{Q}$ no tiene subanillos propios.

Ejercicio 4. Homomorifismos $\phi : \mathbb{Z}_2 \to \mathbb{Z}$,

- Hay exactamente uno.
- Hay al menos dos.
- No hay ninguno.

Ejercicio 5. Sea A un anillo comutativo, la afirmación "Para cualesquiera indeterminadas x e y, los anillos de polinomios $A[x]$ y $A[y]$ son isomorifos". Es:

- Verdadera o falsa, depende de A.
- Siempre verdadera.
- Siempre falsa.

Ejercicio 1. En el anillo $\mathbb{Z}_{10}$, la afirmación "$3^{4k+3} = -3$, para cualquier $k \in \mathbb{Z}$" es:

- Siempre falsa.
- Siempre cierta.
- A veces cierta y a veces falsa, depende de k.

Justificación:

$$3^{4k+3} = \left(3^4\right)^k \cdot 3^3 = (9 \cdot 9)^k \cdot 9 \cdot 3 = 1^k \cdot 7 = 7 \quad \forall k \in \mathbb{Z}$$

Ejercicio 2. En el anillo $\mathbb{Z}_n[x]$, la afirmación "la suma reiterada n veces de cualquier polinomio es 0", es:

- Verdera o falsa, depende de n.
- Siempre falsa.
- Siempre verdadera.

Justificación: Sea $R_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ el homomorfismo de reducción módulo n. Para cualquier $f \in \mathbb{Z}_n[x]$:

$$nf = nR_n(f) = R_n(nf) = R_n(n)R_n(f) = 0 \cdot f = 0$$

Ejercicio 3. Un subanillo A de un anillo B se dice propio si $A \subsetneq B$. Seleccion el enunciado correcto:

- En anillo $\mathbb{Z}$ no tiene subanillos propios.
- El conjunto $A = \{5k \mid k \in \mathbb{Z}\}$ es un subanillo propio de $\mathbb{Z}$.
- El cuerpo $\mathbb{Q}$ no tiene subanillos propios.

Justificación: Si A es un subanillo de $\mathbb{Z}$, entonces $1 \in A$ con lo que para todo $n \geqslant 0$, $\overbrace{1 + \cdots + 1}^{n \text{ veces}} = n \in A$ y, como A contiene a sus opuestos, entonces $\mathbb{Z} \subseteq A$. Por lo que $A = \mathbb{Z}$.

Ejercicio 4. Homomorifismos $\phi : \mathbb{Z}_2 \to \mathbb{Z}$,

- Hay exactamente uno.
- Hay al menos dos.
- No hay ninguno.

Justificación: Si $\phi : \mathbb{Z}_2 \to \mathbb{Z}$ fuese un homomorfismo, tendríamos que:

$$\phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$$

Pero en $\mathbb{Z}_2$, $1 + 1 = 0$ y por tanto, $\phi(1 + 1) = \phi(0) = 0$, así que sería $0 = 2$ en $\mathbb{Z}$, lo que es una contradicción.

Ejercicio 5. Sea A un anillo comutativo, la afirmación "Para cualesquiera indeterminadas x e y, los anillos de polinomios $A[x]$ y $A[y]$ son isomorifos". Es:

- Verdadera o falsa, depende de A.
- <u>Siempre verdadera.</u>
- Siempre falsa.

Justificación: El automorfismo identidad $id_A : A \cong A$ extiende a un único homomorfismo $\phi : A[x] \to A[y]$ tal que $\phi(x) = y$. Explícitamente:

$$\phi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i y^i$$

Claramente ϕ es biyectiva.

1.5. Cuestionario V

Ejercicio 1. En relación con los anillos $\mathbb{Z}_6$ y $\mathbb{Z}\times\mathbb{Z}$, selecciona la afirmación correcta:

- Ambos son DI.
- Uno de ellos es DI, pero el otro no.
- Ninguno es DI.

Ejercicio 2. En relación a las siguientes proposiciones, referidas a los elementos de un Dominio de Integridad:

(a) $a \mid b \wedge a \nmid c \Rightarrow b \nmid b + c$.

(b) $a \mid b \wedge a \nmid c \Rightarrow a \nmid b + c$.

Selecciona la afirmación correcta:

- Ambas son verdad.
- Una es verdad y la otra es falsa.
- Ambas son falsas.

Ejercicio 3. Polinomios de grado uno que son unidades en el anillo de polinomios $\mathbb{Z}_4[x]$:

- No hay.
- Hay dos.
- Hay infinitos.

Ejercicio 4. En el anillo $\mathbb{Z}[i]$:

- 3 es unidad.
- 3 es irreducible.
- 3 no es irreducible.

Ejercicio 5. En el anillo $\mathbb{Z}[i]$:

- 2 es unidad.
- 2 es irreducible.
- 2 no es irreducible.

Ejercicio 1. En relación con los anillos $\mathbb{Z}_6$ y $\mathbb{Z}\times\mathbb{Z}$, selecciona la afirmación correcta:

- Ambos son DI.
- Uno de ellos es DI, pero el otro no.
- Ninguno es DI.

Justificación:

- En $\mathbb{Z}_6$, $2 \cdot 3 = 0$.
- En $\mathbb{Z} \times \mathbb{Z}$, $(1, 0) \cdot (0, 1) = (0, 0)$.

Ejercicio 2. En relación a las siguientes proposiciones, referidas a los elementos de un Dominio de Integridad:

(a) $a \mid b \wedge a \nmid c \Rightarrow b \nmid b + c$.

(b) $a \mid b \wedge a \nmid c \Rightarrow a \nmid b + c$.

Selecciona la afirmación correcta:

- Ambas son verdad.
- Una es verdad y la otra es falsa.
- Ambas son falsas.

Justificación:

- La primera es cierta: si $b = ax$ y fuese $b+c = ay$, tendríamos que $c = ay-ax = a(x - y)$, así que $a \mid c$, lo que es contradictorio.
- La segunda es falsa: por ejemplo, en $\mathbb{Z}$, $2 \nmid 1$ y $2 \nmid 3$, pero $2 \mid 1 + 3 = 4$.

Ejercicio 3. Polinomios de grado uno que son unidades en el anillo de polinomios $\mathbb{Z}_4[x]$:

- No hay.
- Hay dos.
- Hay infinitos.

Justificación: La tabla de multiplicar en $\mathbb{Z}_4$ es:

$(\mathbb{Z}_4, \cdot)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Buscamos estudiar el cardinal del conjunto:

$$\{p \in U(\mathbb{Z}_4[x]) \mid \deg(p) = 1\}$$

Sea $ax + b \in U(\mathbb{Z}_4[x])$ con $a \neq 0$:

$$\begin{aligned}(ax+b)(ax+b) = 1 \Longrightarrow (ax+b)^2 = 1 &\Longrightarrow a^2x + 2abx + b^2 = 1 \\ &\Longrightarrow a^2 = 0 \quad \wedge \quad 2ab = 0 \quad \wedge \quad b^2 = 1\end{aligned}$$

$$\begin{cases} a^2 = 0 & \Longrightarrow \quad a = 2 \\ 2ab = 0 & \Longrightarrow \quad 4b = 0 \Longrightarrow 0b = 0 \Longrightarrow 0 = 0 \\ b^2 = 1 & \Longrightarrow \quad b = 1 \quad \vee \quad b = 3 \end{cases}$$

Luego:

$$\begin{aligned} 2x + 1 \in U(\mathbb{Z}_4[x]) \\ 2x + 3 \in U(\mathbb{Z}_4[x]) \end{aligned}$$

Tenemos dos polinomios que verifican la segunda opción. Además, la última no puede ser por ser $\mathbb{Z}_4[x]$ finito.

Ejercicio 4. En el anillo $\mathbb{Z}[i]$:

- 3 es unidad.
- <u>3 es irreducible.</u>
- 3 no es irreducible.

Justificación:

$$N(3) = 9 \neq \pm 1 \Longrightarrow 3 \notin U(\mathbb{Z}[i])$$

Para probar que 3 es irreducible, supongamos una factorización $3 = \alpha \cdot \beta$ con $\alpha, \beta \in \mathbb{Z}[i] \setminus U(\mathbb{Z}[i])$. Entonces:

$$N(3) = N(\alpha)N(\beta) \Longrightarrow 9 = N(\alpha)N(\beta) \quad N(\alpha), N(\beta) \in \mathbb{Z}$$

Como $\alpha, \beta \notin U(\mathbb{Z}[i]) \Longrightarrow N(\alpha), N(\beta) \neq \pm 1$ Como $\alpha, \beta \in \mathbb{Z}[i]$, se tiene que:

$$\begin{aligned} N(\alpha) = a^2 + b^2 \geqslant 1 \\ N(\beta) = (a')^2 + (b')^2 \geqslant 1 \end{aligned}$$

Por tanto, $N(\alpha), N(\beta) \in$. Además, $9 = N(\alpha)N(\beta) \Longrightarrow N(\alpha) = N(\beta) = 3$.

$$N(\alpha) = 3 \Longrightarrow a^2 + b^2 = 3$$

Pero $\nexists a, b \in \mathbb{Z} \mid a^2 + b^2 = 3$, por lo que 3 es irreducible.

Ejercicio 5. En el anillo $\mathbb{Z}[i]$:

- 2 es unidad.
- 2 es irreducible.

- <u>2 no es irreducible.</u>

Justificación:

$$N(2) = 4 \neq 1 \Longrightarrow 2 \notin U(\mathbb{Z}[i])$$

Para ver que 2 no es irreducible, supongamos una factorización: $2 = \alpha \cdot \beta \mid \alpha, \beta \in \mathbb{Z}[i] \setminus U(\mathbb{Z}[i])$.

$$N(2) = N(\alpha\beta) \Longrightarrow 4 = N(\alpha)N(\beta) \Longrightarrow N(\alpha) = N(\beta) = 2$$

Por ejemplo, $\alpha = \beta = 1 + i$

$$-i(1+i)^2 = (1 + i^2 + 2i)(-i) = (-i)(1 - 1 + 2i) = (-i)2i = -2i^2 = 2$$

Luego $2 = -i(1+i)^2$ es la factorización esencialmente única de $2 \Longrightarrow$ es reducible.