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 Olivares Martos

Granada, 2023-2024

Índice

1. Relaciones de ejercicios

1.1. Relación I

En los siguientes enunciados, $A, B, C, \ldots$ refieren a subconjuntos arbirarios de un conjunto dado X, y se pide demostrar la veracidad de las equivalencias o igualdades propuestas.

Ejercicio 1.

$$A \subseteq B \Longleftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$$

Solución:

$\Longrightarrow$) Sea $E \in \mathcal{P}(A) \Longrightarrow E \subseteq A \subseteq B \Longrightarrow E \in \mathcal{P}(B) \Longrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$

$\Longleftarrow$) $A \in \mathcal{P}(A) \subseteq \mathcal{P}(B) \Longrightarrow A \in \mathcal{P}(B) \Longrightarrow A \subseteq B$

Ejercicio 2.

$$A \subseteq B \Longleftrightarrow A \cap B = A \Longleftrightarrow A \cup B = B$$

Solución: Dividimos la demostración en dos partes, demostrando dos equivalencias:

1. $A \subseteq B \Longleftrightarrow A \cap B = A$

   $\Longrightarrow$) $A \cap B = \{x \in X \mid x \in A \wedge x \in B\} \stackrel{?}{=} A$

   $\subseteq$) Sea $x \in A \cap B \Longrightarrow x \in A \wedge x \in B \Longrightarrow x \in A$, y por la arbitrariedad de $x \in A \cap B$, deducimos que $A \cap B \subseteq A$.

   $\supseteq$) Sea $x \in A \subseteq B \Longrightarrow x \in B \Longrightarrow x \in A \wedge x \in B \Longrightarrow x \in A \cap B$, y por la arbitrariedad de $x \in A$, tenemos que $x \in A \cap B$.

   $\Longleftarrow$) Sea $x \in A = A \cap B \Longrightarrow x \in A \wedge x \in B \Longrightarrow x \in B$, y por la arbitrariedad de $x \in A$, $A \subseteq B$.

2. $A \subseteq B \Longleftrightarrow A \cup B = B$

   $\Longrightarrow$) $A \cup B = \{x \in X \mid x \in A \vee x \in B\} \stackrel{?}{=} B$

   $\subseteq$) Sea $x \in A \cup B \Longrightarrow x \in A \vee x \in B$.
   - Si $x \in A \subseteq B \Longrightarrow x \in B$.
   - Si $x \in B$, está claro.

   Por la arbitrariedad de $x \in A \cup B$, deducimos que $A \cup B \subseteq B$.

   $\supseteq$) Sea $x \in B \Longrightarrow x \in A \vee x \in B$, y por la arbitrariedad de $x \in B$, tenemos que $B \subseteq A \cup B$.

   $\Longleftarrow$) Sea $x \in A \Longrightarrow x \in A \cup B = B$, y por la arbitrariedad de $x \in A$, tenemos que $A \subseteq B$.

Ejercicio 3.

(a) $A \cap B = \emptyset \Longleftrightarrow A \subseteq c(B) \Longleftrightarrow B \subseteq c(A)$.

(b) $A \cup B = X \Longleftrightarrow c(A) \subseteq B \Longleftrightarrow c(B) \subseteq A$.

Solución:

(a) Lo dividimos en dos equivalencias:

(i) $A \cap B = \emptyset \Longleftrightarrow A \subseteq c(B)$

$\Longrightarrow$) Sea $x \in A \Longrightarrow x \notin B$ (ya que si no $x \in A \cap B = \emptyset$) $\Longrightarrow x \in c(B)$, y por la arbitrariedad de $x \in A$, deducimos que $A \subseteq c(B)$.

$\Longleftarrow$) Supongamos que $A \cap B \neq \emptyset \Longrightarrow \exists x \in A \cap B \Longrightarrow x \in A \subseteq c(B) \wedge x \in B \Longrightarrow x \notin B \wedge x \in B$, contradicción. Por lo que $A \cap B = \emptyset$.

(ii) $A \cap B = \emptyset \Longleftrightarrow B \subseteq c(A)$

Por la conmutatividad de la intersección, tenemos que $A \cap B = B \cap A$ y, aplicando el apartado (i), obtenemos que $B \cap A = \emptyset \Longleftrightarrow B \subseteq c(A)$.

(b) Procedemos también mediante dos equivalencias:

(i) $A \cup B = X \Longleftrightarrow c(A) \subseteq B$

$\Longrightarrow$) Sea $x \in c(A) \Longrightarrow x \in X = A \cup B \wedge x \notin A \Longrightarrow (x \in A \vee x \in B) \wedge x \notin A \Longrightarrow x \in B$, de donde tenemos que $c(A) \subseteq B$.

$\Longleftarrow$)

$\subseteq$) $A \cup B = \{x \in X \mid x \in A \vee x \in B\} \subseteq X$

$\supseteq$) Sea $x \in X$:

- Si $x \in A \Longrightarrow x \in A \cup B$.
- Si $x \notin A \Longrightarrow x \in c(A) \subseteq B \Longrightarrow x \in B \Longrightarrow x \in A \cup B$

En conclusión, tenemos que $X \subseteq A \cup B$

(ii) $A \cup B = X \Longleftrightarrow c(B) \subseteq A$

Por la conmutatividad de la unión, tenemos que $A \cup B = B \cup A$ y, aplicando el apartado (i), obtenemos que $B \cup A = X \Longleftrightarrow c(B) \subseteq A$.

Ejercicio 4.

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

Solución: Procedemos por doble inclusión, como suele ser habitual en este tipo de ejercicios.

$\subseteq$) Sea $x \in (A - B) \cap (A - C) \Longrightarrow x \in A - B \wedge x \in A - C \Longrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \Longrightarrow x \in A \wedge x \notin B \cup C$ (ya que si no, tendríamos que $x \in B$ o que $x \in C$, lo que nos llevaría a una contradicción en ambos casos) $\Longrightarrow x \in A - (B \cup C)$, de donde deducimos que $(A - B) \cap (A - C) \subseteq A - (B \cup C)$

$\supseteq$) Sea $x \in A - (B \cup C) \Longrightarrow x \in A \wedge x \notin B \cup C \Longrightarrow x \in A \wedge x \notin B \wedge x \notin C$ (ya que si no llegaríamos a contradicción, al ser $B, C \subseteq B \cup C$) $\Longrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \Longrightarrow x \in (A - B) \wedge x \in (A - C) \Longrightarrow x \in (A - B) \cap (A - C)$, y tenemos que $A - (B \cup C) \subseteq (A - B) \cap (A - C)$

Ejercicio 5.

(a) $A - B = A \Longleftrightarrow A \cap B = \emptyset$.

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

Solución:

(a)

- $\Longrightarrow$) Si $x \in A \cap B = (A - B) \cap B \Longrightarrow (x \in A \wedge x \notin B) \wedge x \in B$, lo que es una contradicción, luego $x \notin A \cap B \Longrightarrow A \cap B = \emptyset$
- $\Longleftarrow$) Lo vemos por doble inclusión:
  - $\subseteq$) $A - B = \{x \in X \mid x \in A \wedge x \notin B\} \subseteq A$
  - $\supseteq$) Sea $x \in A$, supongamos que $x \in B \Longrightarrow x \in A \cap B = \emptyset$, contradicción. Luego tenemos que $x \notin B \Longrightarrow x \in A - B$, de donde $A \subseteq A - B$

(b)

- $\subseteq$) Sea $x \in A \cap (B - C) \Longrightarrow x \in A \wedge (x \in B \wedge x \notin C) \Longrightarrow (x \in A \wedge x \in B) \wedge x \notin C \Longrightarrow x \in (A \cap B) - C \subseteq (A \cap B) - (A \cap C)$, por ser $A \cap C \subseteq C$, de donde tenemos que $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$
- $\supseteq$) Sea $x \in (A \cap B) - (A \cap C) \Longrightarrow (x \in A \wedge x \in B) \wedge x \notin A \cap C \Longrightarrow (x \in A \wedge x \in B) \wedge x \notin Cx \in A \wedge (x \in B \wedge x \notin C) \Longrightarrow x \in A \cap (B - C)$, de donde $(A \cap B) - (A \cap C) \subseteq A \cap (B - C)$

Ejercicio 6. Siendo la "diferencia simétrica" $A\Delta B$ de A y B el subconjunto

$$A\Delta B = (A - B) \cup (B - A)$$

demostrad:

(a) $A\Delta B = (A \cup B) - (A \cap B)$.

(b) $A\Delta B = B\Delta A$.

(c) $A\Delta\emptyset = A$.

(d) $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

(e) $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Solución:

(a)

(b) $A\Delta B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B\Delta A$

(c) $A\Delta\emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

(d)

(e)

Ejercicio 7. Si A y B son finitos, $|A \cup B| + |A \cap B| = |A| + |B|$.
Solución Demostraremos que $|A \cup B| = |A| + |B| - |A \cap B|$:

Sean $|A| = a \in \mathbb{N}$, $|B| = b \in \mathbb{N}$ y $|A \cap B| = s \in \mathbb{N}$, intuitivamente $A \cup B$ contiene a todos los elementos de A y a todos los de B, sabiendo que los repetidos sólo se tienen en cuenta una vez. Por tanto, $|A \cup B|$ es $a + b - s$, ya que si fuera $a + b$, contaríamos a los repetidos dos veces.

Ejercicio 8. Si A, B y C son finitos,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

En los siguientes ejercicios, P, Q, R, ... refieren a las propiedades que pueden ser satisfechas, o no, por los elementos de un conjunto X.

Ejercicio 9. Argumentar que las siguientes proposiciones son equivalentes.

(a) $P \Longrightarrow Q$.

(b) $P \vee Q \Longleftrightarrow Q$.

(c) $P \wedge Q \Longleftrightarrow P$.

Ejercicio 10. Argumentar la veracidad de las siguientes equivalencias.

(a) $P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R)$.

(b) $P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R)$.

(c) $\neg(P \vee Q) \Longleftrightarrow \neg P \wedge \neg Q$.

(d) $\neg(P \wedge Q) \Longleftrightarrow \neg P \vee \neg Q$.

(e) $(P \vee \neg Q) \vee (P \vee \neg R) \Longleftrightarrow P \vee \neg(Q \wedge R)$.

(f) $P \vee Q \vee \neg R \Longleftrightarrow P \vee Q \vee \neg(P \vee R)$.

(g) $(P \vee \neg Q) \wedge (Q \vee \neg P) \Longleftrightarrow (P \wedge Q) \vee \neg(P \vee Q)$.

Ejercicio 11. Sean S y T conjuntos, $A \subseteq S$ y $B \subseteq T$.

(a) Probar $A \times B$ es un subconjunto de $S \times T$.

(b) Probar, con el siguiente ejemplo, que no todo subconjunto X de $S \times T$ es de la forma $X = A \times B$:

$$S = T = \{0, 1\} \qquad X = \{(0, 0), (1, 1)\} \subseteq S \times T$$

Ejercicio 12. Sean $f : S \to T$ y $g : T \to U$ aplicaciones.

(a) Probar que si ambas son inyectivas, entonces su composición $g \circ f : S \to U$ es también inyectiva.

(b) Probar que si ambas son sobreyectivas, entonces su composición $g \circ f : S \to U$ es también sobreyectiva.

(c) Si su compuesta $g \circ f : S \to U$ es inyectiva o sobreyectiva, ¿qué podemos decir sobre f y g?

Ejercicio 13. Sea $f : S \to T$ una aplicación.

(a) Probar que f es inyectiva si y solo si tiene una *inversa por la izquierda*, es decir, existe una aplicación $g : T \to S$ tal que $g \circ f = id_S$.

(b) Dar un ejemplo de una aplicación inyectiva con dos diferentes inversas por la izquierda.

(c) Probar que f es sobreyectiva si y solo si tiene una *inversa por la derecha*, es decir, existe una aplicación $g : T \to S$ tal que $f \circ g = id_T$.

(b) Dar un ejemplo de una aplicación sobreyectiva con dos diferentes inversas por la derecha.

Ejercicio 14. Denotemos por $2 = \{0, 1\}$ al conjunto con dos elementos. Sea X un conjunto no vacío y sea 2^X el conjunto de todas las aplicaciones $f : X \to 2$. Si $A \in \mathcal{P}(X)$, se define su **aplicación característica** $\chi_A : X \to 2$ por:

$$\chi_A(x) = \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \notin A \end{cases}$$

Probar que la correspondencia $A \longmapsto \chi_A$ define una aplicación biyectiva

$$\chi : \mathcal{P}(X) \xrightarrow{\cong} 2^X$$

Toda aplicación $f : S \to T$ determina otras

$$f_* : \mathcal{P}(S) \to \mathcal{P}(T) \qquad f^* : \mathcal{P}(T) \to \mathcal{P}(S)$$

llamadas las aplicaciones **imagen** e **imagen inversa** por f, respectivamente, que están definidas, para cada $A \subseteq S$ y $X \subseteq T$, por

$$f_*(A) = \{f(a) \mid a \in A\} \qquad f^*(X) = \{a \in S \mid f(a) \in X\}$$

En los ejercicios siguientes, $f : S \to T$ refiere a una aploicación dada, A, $B \subseteq S$ son subconjuntos de S y $X, Y \subseteq T$ son subconjunos de T.

Observación. Es común en matemáticas usar las aplicaciones imagen e imagen inversa, aunque la notación usual para estas es f y f^{-1}, respectivamente. Estas no deben confundirse con la aplicación y con la inversa de la aplicación, dada una aplicación $f : A \to B$, tenemos:

$$f : \mathcal{P}(A) \to \mathcal{P}(B) \qquad f^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)$$

que son las aplicaciones imagen e imagen inversa, mientras que la inversa (en caso de existir), es una aplicación $f^{-1} : B \to A$.

Ejercicio 15. Probar que $f^*(X \cup Y) = f^*(X) \cup f^*(Y)$ y $f_*(A \cup B) = f_*(A) \cup f_*(B)$.

Ejercicio 16. Probar que $f^*(X \cap Y) = f^*(X) \cap f^*(Y)$ y $f_*(A \cap B) \subseteq f_*(A) \cap f_*(B)$.

Ejercicio 17. Demostrar que si f es inyectiva, entonces $f_*(A \cap B) = f_*(A) \cap f_*(B)$.

Ejercicio 18. Demostrar con el siguiente ejemplo que, en general, $f_*(A \cap B) \neq f_*(A) \cap f_*(B)$:
Sea $f = || : \mathbb{R} \to \mathbb{R}$ la aplicación "valor absoluto", $A = (0, 1)$ y $B = (-1, 0)$.

Ejercicio 19. $f_*(f^*(X)) \subseteq X$, y se da la igualdad si f es sobreyectiva.

Ejercicio 20. $A \subseteq f^*(f_*(A))$, y se da la igualdad si f es inyectiva.

Ejercicio 21. Probar que, si f es una biyección, entonces las aplicaciones $f_* : \mathcal{P}(S) \to \mathcal{P}(T)$ y $f^* : \mathcal{P}(T) \to \mathcal{P}(S)$ son biyectivas e inversas una de la otra.

1.2. Relación II

Ejercicio 1. Dar ejemplos de relaciones binarias en un conjunto que verifiquen una sola de ls siguientes propiedades: reflexiva, simétrica, transitiva.

Ejercicio 2. Sea $\mathbb{N} = \{0, 1, 2, \ldots\}$ el conjunto de los nńumeros naturales, sobre $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ definimos $(a, b) \sim (c, d)$ si $a + d = b + c$.

(a) Verificar que $\sim$ es una relación de equivalencia.

(b) Sea $f : \mathbb{N}^2 \to \mathbb{Z}$ la aplicación definida por $f(a, b) = a - b$. Verificar que f induce una biyección $\mathbb{N}^2/\sim \cong \mathbb{Z}$.

Ejercicio 3. Sea $f : S \to T$ una aplicación.

(a) Probar que f define una relación de equivalencia R_f en S, donde aR_fb si $f(a) = f(b)$ (esta relación se llama *la relación núcleo de* f).

(b) Probar que, si f es sobreyectiva, se inducie una biyección $S/R_f \cong T$.

Ejercicio 4. Sea $Y \subseteq X$ un subconjunto. Sea $f : \mathcal{P}(X) \to \mathcal{P}(Y)$ la aplicación tal que $f(A) = A \cap Y$, para cada $A \in \mathcal{P}(X)$.

(a) Probar que f es una sobreyección.

(b) Describir la relación R_f, núcleo de f.

(c) Probar que f induce una biyección $\mathcal{P}(X)/R_f \cong \mathcal{P}(Y)$.

Ejercicio 5. Sea R una relación de equivalencia sobre un conjunto S. La aplicación $p : S \to S/R$ definida por $p(A) = \overline{a}$ es la llamada **proyección canónica** de S sobre el cociente. ¿Qué relación hay entre R y R_p?

Ejercicio 6. Un subconjunto $P \subseteq \mathcal{P}(S)$ es llamado una **partición del conjunto** S si

(a) $\forall A \in P$, $A \neq \emptyset$.

(b) $\bigcup_{A \in P} A = S$.

(c) Para cualesquiera $A, B \in P \mid A \neq B$, se verifica que $A \cap B = \emptyset$.

Así, por ejemplo, el conjunto cociente S/R, para R una relación de equivalencia sobre S es una partición.

Sea P una partición de S. Definimos la aplicación $p : S \to P$ por $p(a) = A$ si $a \in A$. ¿Qué relación hay entre P y S/R_p?

Ejercicio 7. Sea $X = \{1, 2, 3\}$. Calcular todas las particiones de X.

Ejercicio 8. Sea $X = \{0, 1, 2, 3\}$, $Y = \{a, b, c\}$ y $f : X \to Y$ la aplicación dada por:

$$f(0) = c \qquad f(1) = f(2) = a \qquad f(3) = b$$

Consideremos la aplicación $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$.

(a) ¿Es f^* inyectiva, sobreyectiva o biyectiva?

(b) Describir la relación R_{f^*} asociada a f^* y el conjunto cociente $\mathcal{P}(Y)/R_{f^*}$.

Ejercicio 9. Sea X un conjunto e $Y \subseteq X$ un subconjunto suyo. En el conjunto $\mathcal{P}(X)$ se define la siguiente relación binaria:

$$A \sim B \Longleftrightarrow A \cap Y = B \cap Y$$

Demostrad que dicha relación es de equivalencia. Para $X = \{1,2,3,4,5\}$ e $Y = \{1,4\}$, describir del conjunto cociente.

Ejercicio 10. Sea X un conjunto e $Y \in \mathcal{P}(X)$. Definimos la aplicación $f : X \to \mathcal{P}(X)$ por $f(x) = Y \cup \{x\}$, para $x \in X$ y consideramos en X la relación de equivalencia R_f (Ejercicio 3). Describir el conjunto cociente X/R_f. Si X es un conjunto finito con n elementos e Y tiene m elementos, calcular el cardinal de X/R_f.

1.3. Relación III

Ejercicio 1.

(a) Si A y B son anillos conmutativos, probar que el conjunto producto cartesiano $A \times B$ con las operaciones

$$(a, a') + (b, b') = (a + b, a' + b') \qquad (a, a')(b, b') = (ab, a'b')$$

es efectivamente un nillos conmutativo. Se llama el "*anillo producto cartesiano*" de A y B o "*anillo producto directo*" de A y B.

(b) Escribir las tablas de sumar y multiplicar del anillo producto $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ejercicio 2. En el conjunto $\mathbb{Z}$ definimos las operaciones de suma $\oplus$ y producto $\otimes$ por

$$a \oplus b = a + b - 1$$
$$a \otimes b = a + b - ab$$

Así, por ejemplo, $2 \oplus 3 = 4$ y $2 \otimes 3 = -1$. ¿Es $\mathbb{Z}$ un anillo conmutativo con estas operaciones?

Ejercicio 3.

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a') \cdot (b, b') = (ab, ab' + a'b)$$

¿Es $\mathbb{Z} \times \mathbb{Z}$ un anillo conmutativo con estas operaciones?

Ejercicio 4. Calcula el cociente y el resto de dividir.

(a) 17544 entre 123.

(b) -17544 entre -123.

(c) 17544 entre -123.

(d) -17544 entre 123.

Ejercicio 5. Escribir las tablas de sumar y multiplicar de los anillos $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Ejercicio 6. Sea $R : \mathbb{Z} \to \mathbb{Z}_n$ la aplicación que asigna a cada entero su resto al dividirlo por n ($n \geqslant 2$). Probar que, para cualquier natural $m \geqslant 1$ y $r \in \mathbb{Z}_n$, se verifica que

$$mr = R(mr) = R(m)r$$

donde el término $mr = \sum_1^m r$ es el resultado de sumar, en $\mathbb{Z}_n$, r consigo mismo m veces, el término $R(mr)$ es el resto de dividir por n el número natural producto de m y r; y el término $R(m)r$ es el producto en $\mathbb{Z}_n$, del resto de dividir m entre n por r.

Utilizando lo anterior, ¿es verdad que si, en $\mathbb{Z}_8$, sumas 7 consigo mismo 23 veces obtienes 1, o que si sumas 6 consigo mismo 125 veces obtienes 6?

Ejercicio 7. Efectuar los siguientes cálculos en el anillo $\mathbb{Z}\left[\sqrt{3}\right]$:

$$(3+2\sqrt{3})+(4-5\sqrt{3}) \qquad (3+2\sqrt{3})(4-5\sqrt{3}) \qquad (2-\sqrt{3})^3$$

Ejercicio 8. ¿Cuáles de los siguientes son subanillos de los anillos indicados?

(i) $\{a \in \mathbb{Q} \mid 3a \in \mathbb{Z}\} \subseteq \mathbb{Q}$.

(ii) $\{m + 2n\sqrt{3} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{R}$.

Ejercicio 9. Determinar las unidades del anillo definido por el conjunto $\mathbb{Z} \times \mathbb{Z}$, con las operaciones (ver Ejercicio 3)

$$(a,a') + (b,b') = (a+b, a'+b') \qquad (a,a') \cdot (b,b') = (ab, ab' + a'b)$$

Ejercicio 10. Encontrar todas las unidades de los anillos $\mathbb{Z}_6, \mathbb{Z}_7$ y $\mathbb{Z}_8$.

Ejercicio 11. ¿Cuáles de los siguientes son subanillos de los anillos indicados?

(i) $\sum a_i x^i \in \mathbb{Z}[x] \mid a_1$ es par$\} \subseteq \mathbb{Z}[x]$.

(ii) $\sum a_i x^i \in \mathbb{Z}[x] \mid a_2$ es par$\} \subseteq \mathbb{Z}[x]$.

Ejercicio 12. Efectuar las siguientes operaciones en el anillo $\mathbb{Z}_5[x]$:

$$\begin{gathered}
(3+4x+x^2+2x^3)+(3+4x+4x^4+3x^3) \\
(3+4x+x^2+2x^3)+(3+4x+4x^4+3x^3) \\
(2-4x+x^2-2x^3)+(3-4x+4x^2-3x^3) \\
(2-4x+x^2-2x^3)(3-4x+4x^2-3x^3)
\end{gathered}$$

Ejercicio 13. Si $p(X) \in \mathbb{Z}_5[x]$ es cualquiera de los cuatro polinomio obtenidos al realizar el ejercicio anterior, calcular $p(1)$ y $p(-1)$ en cada caso.

Ejercicio 14. Ej conjunto $\mathbb{R}^2$ es un anillo con las operaciones:

$$(a,a') + (b,b') = (a+b, a'+b') \qquad (a,a') \cdot (b,b') = (ab - a'b', ab' + a'b)$$

Probar que hay un isomorfismo $\mathbb{R}^2 \cong \mathbb{C}$.

Ejercicio 15. Sea A un anillo conmutativo y $u \in A$ una unidad del anillo. Demostrar que la aplicación $f_u : A \to A$ dada por $f_u(x) = uxu^{-1}$ es un automorfismo de A.

Ejercicio 16. Dado un anillo A, demostrar que existe un único homomorfismo de anillos de $\mathbb{Z}$ en A.

Ejercicio 17. Para un anillo A, se define la **característica** de A como el menor entero positivo n tal que $n \cdot 1 = \overbrace{1 + \cdots + 1}^{n} = 0$, siendo 1 el uno del anillo A. Si no existe tal n, diremos que la característica de A es 0.

Demostrar que si A es un anillo de característica $n \geqslant 2$, entonces existe un único homomorfismo de anillos de $\mathbb{Z}_n$ en A.

Ejercicio 18. Dados dos números naturales, $n, m \geqslant 2$, dar condiciones par que exista un homomorfismo de anillos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$.

1.4. Relación IV

Ejercicio 1. Argumenta si los siguientes anillos son, o no, Dominios de Integridad:

$$\mathbb{Z}_8 \qquad \mathbb{Z}\left[\sqrt{2}\right] \qquad \mathbb{Z}_3 \qquad \mathbb{Z}\times\mathbb{Z} \qquad \mathbb{Z}_6[x] \qquad \mathbb{Z}[i] \qquad \mathbb{Z}_5[x]$$

Ejercicio 2. ¿Es el anillo definido por el conjunto $\mathbb{Z}\times\mathbb{Z}$ con las operaciones:

$$(a,a')+(b,b')=(a+b,a'+b') \qquad (a,a')(b,b')=(ab,ab'+a'b)$$

un Dominio de Integridad? (ver Ejercicio 3 de la Relación III).

Ejercicio 3. ¿Es el anillo definido por el conjunto $\mathbb{Z}$ de los números enteros con las operaciones:

$$a\oplus b=a+b-1 \qquad a\otimes b=a+b-ab$$

un Dominio de Integridad? (ver Ejercicio 2 de la Relación III).

Ejercicio 4. Demuestra que un Dominio de Integridad finito es un cuerpo.

Ejercicio 5. Sea $n\in\mathbb{Z}$ un entero no cuadrado en $\mathbb{Z}$. Demuestra que el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ es $\mathbb{Q}[\sqrt{n}]$.

Ejercicio 6. Se define el cuerpo $\mathbb{Q}(x)$ como el cuerpo de fracciones del anillo $\mathbb{Z}[x]$, esto es, $\mathbb{Q}(x):=\mathbb{Q}(\mathbb{Z}[x])$. Demuestra que $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$ tienen el mismo cuerpo de fracciones. Esto es:

$$\mathbb{Q}(\mathbb{Q}[x])=\mathbb{Q}(x)$$

Ejercicio 7. Sea $A=\{\frac{m}{2^k}\in\mathbb{Q}\mid m\in\mathbb{Z}\wedge k\geqslant 0\}$. Argumentar que:

(a) A es subanillo de $\mathbb{Q}$.

(b) $\mathbb{Z}\subsetneq A$.

(c) El cuerpo de fracciones de A es el mismo que el de $\mathbb{Z}$, o sea, $\mathbb{Q}$.

Ejercicio 8. Sea A un DI y consideremos en A la relación binaria $\sim$ de ser asociados. Esto es, $a\sim b$ si a es asociado con b.

(a) Probar que $\sim$ es una relación de equivalencia en A.

(b) Sea $A/\sim=\{[a]\mid a\in A\}$, el correspondiente conjunto cociente. Establecemos entre sus elementos ls relación por la cual $[a]\leqslant[b]$ si a es un divisor de b en el anillo A. ¿Está bien definida esa relación en $A/\sim$? ¿Es una relación de orden?

Ejercicio 9. Para n un número natural, calcular $\text{mcd}(n,n^2)$, $\text{mcd}(n,n+1)$ y $\text{mcd}(n,n+2)$.

Ejercicio 10. ¿Podremos rellenar con precisión un depósito de 5388033 litros usando un recipiente de 371? En caso afirmativo, ¿cuántas veces usaremos el recipiente?

Ejercicio 11. Determinar, si existe, un polinomio $p(x)\in\mathbb{Q}[x]$ tal que:

$$\left(\frac{3}{5}x^3+\frac{1}{2}x+\frac{2}{3}\right)p(x)=\frac{9}{20}x^5+\frac{147}{40}x^3+\frac{1}{2}x^2+\frac{11}{4}x+\frac{11}{3}$$

Ejercicio 12. Calcular el cociente y el resto de dividir, en el anillo $\mathbb{Q}[x]$, el polinomio p entre el polinomio q:

$$p = \frac{9}{20}x^5 + \frac{147}{40}x^3 + \frac{1}{2}x^2 + \frac{17}{4}x + \frac{17}{3}$$
$$q = \frac{3}{5}x^3 + \frac{1}{2}x + \frac{2}{3}$$

Ejercicio 13. Determinar, si existe, un polinomio $p(x) \in \mathbb{Z}_3[x]$ tal que

$$(2x^2 + x + 2)p(x) = 2x^7 + x^6 + 2x^4 + 2$$

Ejercicio 14. En el anillo $\mathbb{Z}[i]$, calcular cociente y resto de dividir $1 + 15i$ entre $3 + 5i$.

Ejercicio 15. ¿Es $2 + 5\sqrt{3}$ un divisor de $39 - 9\sqrt{3}$ en el anillo $\mathbb{Z}\left[\sqrt{3}\right]$?

Ejercicio 16. Resolver en $\mathbb{Z}$ las ecuaciones diofánticas

$$10x + 46y = 4050 \qquad 60x + 36y = 12 \qquad 35x + 6y = 8 \qquad 12x + 18y = 11$$

Ejercicio 17. "Cuarenta y seis náufragos cansados arribaron a una bella isla. Allí encontraron ciento veintiséis montones de cocos, de no más de cincuenta cada uno, y catorce cocos sueltos, y se los repartiron equitativamente..." ¿Cuántos cocos había en cada montón?

Ejercicio 18. Disponemos de 15 euros para comprar 40 sellos de correso, de 10, 40, y 60 céntimos y, al menos, necesitamos 2 de cata tipo ¿Cuántos sellos de cada clase podremos comprar?

Ejercicio 19. En una torre eléctrica se nos ha roto una pata de 4 m de altura. Para equilibrarlo provisionalmente, disponemos de 7 discos de madera de 50 cm de grosor y de otros 12 de 30 cm. ¿Cuál de las siguientes afirmaciones es verdadera?

- No podremos equilibrar la torre.
- Podremos equilibrar la torre, y de una única manera.
- Podremos equilibrar la torre, y de dos únicas maneras.
- Podremos equilibrar la torre, y de más de 2 maneras distintas.

Ejercicio 20. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{R}[x]$, de los polinomios $x^3 - 2x^2 - 5x + 6$ y $x^3 - 3x^2 - x + 3$. Encontrar todos los polinomios $p(x)$ y $g(x)$ en $\mathbb{R}[x]$, ambos de grado 3, tales que

$$(x^3 - 2x^2 - 5x + 6)p(x) + (x^5 + x^4 - x - 1)g(x) = x^4 + x^2 + 1$$

Ejercicio 21. En el anillo $\mathbb{Z}\left[\sqrt{2}\right]$, calcular

$$\operatorname{mcd}\left(2 - 3\sqrt{-2}, 1 + \sqrt{-2}\right) \qquad \operatorname{mcm}\left(2 - 3\sqrt{-2}, 2 + \sqrt{-2}\right)$$

Ejercicio 22. En $\mathbb{Z}\left[\sqrt{3}\right]$, calcula $\operatorname{mcd}(3 + \sqrt{3}, 2)$ y $\operatorname{mcm}(3 + \sqrt{3}, 2)$.

Ejercicio 23. Determina los enteros $x, y \in \mathbb{Z}$ tales que, en el anillo $\mathbb{Z}[i]$, se verifique la ecuación

$$(-2 + 3i)x + (1 + i)y = 1 + 11i$$

Ejercicio 24. Resolver la siguiente ecuación en el anillo $\mathbb{Z}\left[\sqrt{2}\right]$:

$$(4 + \sqrt{2})x + (6 + 4\sqrt{2})y = \sqrt{2}$$

1.5. Relación V

Ejercicio 1. Demostrad

1. $3^{2n} - 2^n$ es divisible por 7 para todo entero $n \geqslant 1$.
2. $3^{2n+1} + 2^{n+2}$ es divisible por 7 cualquiera que sea el entero $n \geqslant 1$.
3. $3^{2n+2} + 2^{6n+1}$ es divisible por 11 para todo entero $n \geqslant 1$.
4. $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17 cualquiera que sea el entero $n \geqslant 1$.
5. Un número es divisible por 4 si y solo si el número formado por sus dos últimas cifras es múltiplo de 4.

Ejercicio 2. Sean $a, b \in \mathbb{Z}$. Demostrad que si $3 \mid (a^2 + b^2)$ entonces $3 \mid a$ y $3 \mid b$.

Ejercicio 3. Demostrad las reglas del 2, 3, 5 y 11 para la división.

Ejercicio 4. Discutir y resolver el sistema de congruencias

$$\left\{ \begin{array}{rcll} 5x & \equiv & 1 & \text{mód } (14) \\ 11x & \equiv & 10 & \text{mód } (16) \end{array} \right.$$

Ejercicio 5. Calculad la menor solución positiva del sistema de congruencias

$$\left\{ \begin{array}{rcll} 3x & \equiv & 1 & \text{mód } (4) \\ 2x & \equiv & 2 & \text{mód } (5) \\ x & \equiv & -1 & \text{mód } (3) \end{array} \right.$$

Ejercicio 6. Una banda de 13 piratas se repartir N monedas de oro, pero le sobran 8. Dos mueren, las vuelven a repartir y sobran 3. Luego 3 se ahogan y sobran 5. ¿Cuál es la mínima cantidad posible N de monedas?

Ejercicio 7. En el anillo $\mathbb{Z}\left[\sqrt{3}\right]$, resolved la congruencia

$$(1+\sqrt{3})x \equiv 9 - 4\sqrt{3} \quad \text{mód } (2\sqrt{3})$$

Ejercicio 8. En el anillo $\mathbb{Z}[i]$, resolved el siguiente sistema de congruencias

$$\left\{ \begin{array}{rccl} x & \equiv & i & \text{mód } (3) \\ x & \equiv & 1+i & \text{mód } (3+2i) \\ x & \equiv & 3+2i & \text{mód } (4+i) \end{array} \right.$$

Ejercicio 9. Determinad todos los polinomios $f(x) \in \mathbb{Z}_5[x]$ tales que

$$(x^4 + 3x^3 + 2x^2 + 3x + 1)f(x) \equiv x^4 - 2x^3 - x + 2 \quad \text{mód } (x^3 + 3x^2 + 4x + 2)$$

Ejercicio 10. Determinad los polinomios $f(x) \in \mathbb{Q}[x]$ de grado menor o igual que tres que satisfacen el sistema de congruencias

$$\begin{array}{rcll} f(x) & \equiv & x-1 & \text{mód } (x^2+1) \\ f(x) & \equiv & x+1 & \text{mód } (x^2+x+1) \end{array}$$

Ejercicio 11. Probad el Teorema de Ruffini:
Si $f(x) \in A[x]$, para cualquier $a \in A$, $f(a)$ es igual al resto de dividir $f(x)$ entre $(x-a)$.

Ejercicio 12. Encontrad un polinomio $f(x) \in \mathbb{Q}[x]$ de grado 3 tal que:

$$f(0) = 6 \qquad f(1) = 12 \qquad f(x) \equiv (3x+3) \mod (x^2+x+1)$$

Ejercicio 13. Determinad todos los polinomios $f(x) \in \mathbb{Z}_2[x]$ de grado menor o igual que 4, tales que:

1. El resto de dividir $f(x)$ entre x^2+1 es x.
2. El resto de dividir $xf(x)$ entre x^2+x+1 es $x+1$.
3. $f(1) = 1$.

Ejercicio 14. Calculad el resto de dividir 279^{323} entre 17.

Ejercicio 15. Calculad las dos últimas cifras de $3^{3^{100}}$.

Ejercicio 16. Resolved, si es posible, la congruencia $43^{51}x \equiv 2 \mod (36)$

Ejercicio 17. Estudiad si 5^{10077} es una unidad en $\mathbb{Z}_{38808}$. Calculad su inverso en caso de que lo tenga.

Ejercicio 18. Resuelve las ecuaciones siguientes.

1. $12x = 8$ en el anillo $\mathbb{Z}_{20}$.
2. $19x = 42$ en $\mathbb{Z}_{50}$.
3. $9x = 4$ en $\mathbb{Z}_{1453}$.
4. $5^{30}x = 2$ en $\mathbb{Z}_7$.
5. $20x = 984$ en $\mathbb{Z}_{1984}$.

Ejercicio 19. Determina los inversos (si existen) de

1. 15 en $\mathbb{Z}_{16}$.
2. 9 en $\mathbb{Z}_{20}$.
3. 12 en $\mathbb{Z}_{21}$.
4. 22 en $\mathbb{Z}_{31}$.

Ejercicio 20. Determina cuántas unidades tienen los anillos

1. $\mathbb{Z}_{125}$.
2. $\mathbb{Z}_{72}$.
3. $\mathbb{Z}_{88}$.

4. $\mathbb{Z}_{1000}$.

Ejercicio 21. Determina si la igualdad $a = b$ es cierta en los siguientes casos:

1. $a = 9^{55^9}$ y $b = 7^{70^{55}}$, en el anillo $\mathbb{Z}_{21}$.
2. $a = 2^{5^{70}}$ y $b = 5^{70^2}$, en el anillo $\mathbb{Z}_{21}$.
3. $a = 12^{55^{70}}$ y $b = 10^{70^{55}}$, en el anillo $\mathbb{Z}_{22}$.
4. $a = 5^{5^{70}}$ y $b = 10^{70^{22}}$, en el anillo $\mathbb{Z}_{22}$.

Ejercicio 22. Sea K un cuerpo. Dado un polinomio $f \in K[x]$ cuyo grado es 2 ó 3, demostrar que f es irreducible si, y sólo si, f no tiene raíces en K.

Ejercicio 23. Sea I el ideal principal de $\mathbb{Z}_3[x]$ generado por x^2+2x+2. Demostrar que el anillo cociente $\mathbb{Z}_3[x]/I$ es un cuerpo y hallar el inverso de $(ax + b) + I$.

Ejercicio 24. Determinar los inversos (si existen) de

1. La clase de $x^2 + x + 1$ en el anillo $\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$.
2. La clase de $x + 1$ en el anillo $\mathbb{R}[x]/\langle x^3 - 2x - 3\rangle$.
3. La clase de $x^2 + x$ en el anillo $\mathbb{Z}_2[x]/\langle x^2 + 1\rangle$.
4. La clase de $x^3 + x + 1$ en el anillo $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$.
5. La clase del polinomio $2x + 1$ en el anillo $\mathbb{Q}[x]/\langle x^3 + 2x^2 + 4x - 2\rangle$.
6. La clase de x en el anillo $\mathbb{Q}[x]/\langle x^4 + x + 1\rangle$.

Ejercicio 25. Determinar los inversos (si existen) de

1. La clase de $1 + i$ en el anillo $\mathbb{Z}[i]/\langle 3 + 2i\rangle$.
2. La clase de $2 - \sqrt{2}$ en el anillo $\mathbb{Z}\left[\sqrt{2}\right]/\langle 3\rangle$.
3. La clase de $3 + 3i\sqrt{2}$ en el anillo $\mathbb{Z}[i\sqrt{2}]/\langle 4 - 2i\sqrt{2}\rangle$.
4. La clase de $1 + \sqrt{3}$ en el anillo $\mathbb{Z}\left[\sqrt{3}\right]/\langle\sqrt{3}\rangle$.

Ejercicio 26. Construir cuerpos con 4 y 8 elementos.

Ejercicio 27. Calcular las unidades de los anillos cocientes $\mathbb{Z}_5[x]/\langle x^2 + x + 1\rangle$, $\mathbb{Z}_5[x]/\langle x^2 + 1\rangle$ y $\mathbb{Z}_2[x]/\langle x^2 + 2\rangle$.

Ejercicio 28. Demostrar que el anillo cociente $\mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$ es un cuerpo y calcular el inverso de la clase de $x^2 + 1$.

1.6. Relación VI

Ejercicio 1. Estudiar la irreducibilidad de los siguientes polinomios de $\mathbb{Z}[x]$ (factorizando en irreducibles en su caso):

$2x^5-6x^3+9x^2-15$	x^4+15x^3+7	$50x^5+30x^4+100x^2+100x+27$
$12x^7+6x^4+9x+8$	$x^3+17x+36$	x^5-x^2+1
$x^4+10x^3+5x^2-2x-3$	$x^4+6x^3+4x^2-15x+1$	$6x^4+9x^3-3x^2+1$
$x^5+5x^4+7x^3+x^2-3x-11$	$x^5-10x^4+36x^3-53x^2+26x+1$	$x^4+6x^3+4x^2-15x+1$
$x^6+3x^5-x^4+3x^3+3x^2+3x-1$	$x^4+4x^3-x^2+4x+1$	$x^5-6x^4+3x^3+2x-1$
$2x^4+2x^3+6x^2+4$	$2x^4+3x^3+3x^2+3x+1$	$x^4-x^3+9x^2-4x-1$
$x^7+5x^6+x^2+6x+5$	$3x^5+42x^3-147x^2+21$	$x^5+3x^4+10x^2-2$
x^4+3x^2-2x+5	$3x^6+x^5+3x^2+4x+1$	$2x^4+x^3+5x+3$
$2x^5-2x^2-4x-2$	$x^6-2x^5-x^4-2x^3-2x^2-2x-1$	$3x^4+3x^3+9x^2+6$
$x^4+3x^3+5x^2+1$	$2x^4+8x^3+10x^2+2$	$x^4+4x^3+6x^2+2x+1$

Ejercicio 2. En el anillo $\mathbb{Z}[i]$, factorizar -300 como producto de una unidad por irreducibles no asociados entre sí.

Ejercicio 3. En el anillo $\mathbb{Z}[i]$, factorizar $66+12i$ como producto de una unidad por irreducibles no asociados entre sí.

Ejercicio 4. En el anillo $\mathbb{Z}\left[\sqrt{2}\right]$, factorizar $8+14\sqrt{2}$ como producto de una unidad por irreducibles no asociados entre sí (Indicación: Observar primero que $\sqrt{2}$ es un irreducible en este anillo).

Ejercicio 5. En $\mathbb{Z}\left[\sqrt{3}\right]$, factoriza $6+2\sqrt{3}$ como producto de una unidad por irreducibles no asociados entre sí (Indicación: Observar primero que $1+\sqrt{3}$, $1-\sqrt{3}$ y $\sqrt{3}$, son irreducibles en este anillo. Observar también que los dos primeros son asociados).

2. Cuestionarios

2.1. 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:

- <u>Siempre verdadera.</u>
- 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:

- $(A \cup B) \cap C = A$.
- <u>$(A \cup B) \cap (A \cup C) = A$.</u>
- $(A \cap B) \cup (A \cap C) = A$.

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.
- <u>A veces verdadera y a veces falsa, depende de A y B.</u>

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 $X_R \subseteq X_Q \Rightarrow X_P \subseteq X_Q = X_Q \cup X_R$.

2.2. 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 $\exists c \in X \mid c \not R c$.

2.3. 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 "$\mathbb{Z}$ 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.
- $\underline{\mathcal{P}(X) \text{ no es un anillo conmutativo, falla un axioma.}}$
- $\mathcal{P}(X)$ 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.
- <u>Siempre falsa.</u>

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).

- <u>3 es una unidad y $4 \cdot 3^{-1} = 4$.</u>
- 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.
- <u>Siempre verdadera.</u>

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 "$\mathbb{Z}$ es un subanillo de A" es:

- <u>Siempre verdadera.</u>
- 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 $\mathbb{R}$.

2.4. 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.
- <u>Siempre cierta.</u>
- 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.
- <u>Siempre verdadera.</u>

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:

- <u>En anillo $\mathbb{Z}$ no tiene subanillos propios.</u>
- 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.
- <u>No hay ninguno.</u>

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.

2.5. 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, $N(\alpha), N(\beta) \in \mathbb{N}$. 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.

2.6. Cuestionario VI

Ejercicio 1. En relación a las siguientes proposiciones, referidas a elementos cualesquiera de un DI, selecciona las verdaderas:

- $c \mid ab \Longrightarrow c \mid a \vee c \mid b$.
- $a \mid c \wedge b \mid c \Longrightarrow ab \mid c$.
- $c \mid a \vee c \mid b \Longrightarrow c \mid ab$.

Ejercicio 2. Entre los siguientes DE, selecciona aquellos en los que el máximo común divisor y el mínimo común múltiplo son únicos salvo signo:

- $\mathbb{Z}\left[\sqrt{-2}\right]$.
- $\mathbb{Z}\left[\sqrt{3}\right]$.
- $\mathbb{Z}_3[x]$.

Ejercicio 3. En un DE, tenemos la ecuación diofántica $px + by = 1$, donde p es irreducible. Entre las siguientes afirmaciones, selecciona la que es verdad.

- Nunca tiene solución.
- Puede tener solución o no, depende de b.
- Siempre tiene solución.

Ejercicio 4. En un DE, tenemos la ecuación diofántica $px + qy = c$, donde p y q son irreducibles no asociados entre sí. Entre las siguientes afirmaciones, selecciona la que es verdad.

- Nunca tiene solución.
- Puede tener solución o no, depende de p y de q.
- Siempre tiene solución.

Ejercicio 5. Entre las siguientes proposiciones, referidas a un DE, selecciona las verdaderas.

- Si la ecuación $ax + by = 1$ tiene solución, entonces la ecuación $ax + by = c$ tiene solución para todo c.
- Si la ecuacióin $ax+bb'y = 1$ tiene solución, entonces las ecuaciones $ax+by = 1$ y $ax + b'y = 1$ tienen solución.
- Si las ecuaciones $ax + by = 1$ y $ax + b'y = 1$ tienen solución, entonces la ecuación $ax + bb'y = 1$ tiene solución.

Ejercicio 1. En relación a las siguientes proposiciones, referidas a elementos cualesquiera de un DI, selecciona las verdaderas:

- $c \mid ab \Longrightarrow c \mid a \lor c \mid b$.
- $a \mid c \land b \mid c \Longrightarrow ab \mid c$.
- $\underline{c \mid a \lor c \mid b \Longrightarrow c \mid ab.}$

Justificación:

- La primera es falsa, en $\mathbb{Z}$, $6 \mid 12 = 4 \cdot 3$ pero $6 \nmid 4$.
- La segunda es falsa, en $\mathbb{Z}$, $2 \mid 6$ pero $2 \cdot 2 \nmid 6$.
- La tercera es verdadera. De hecho, basta con que c divida a uno de ellos para que divida al producto:

$$a = ca' \Longrightarrow ab = c(a'b)$$

Ejercicio 2. Entre los siguientes DE, selecciona aquellos en los que el máximo común divisor y el mínimo común múltiplo son únicos salvo signo:

- $\underline{\mathbb{Z}\left[\sqrt{-2}\right].}$
- $\mathbb{Z}\left[\sqrt{3}\right]$.
- $\underline{\mathbb{Z}_3[x].}$

Justificación: Serán aquellos cuyas unidades sean ± 1:

- En $\mathbb{Z}\left[\sqrt{-2}\right]$, $a+b\sqrt{-2}$ es unidad si y sólo si $a^2+2b^2 = 1$, lo que sólo se verifica si $a = 1$ y $b = 0$.
- En $\mathbb{Z}\left[\sqrt{3}\right]$, $a + b\sqrt{3}$ es unidad si y sólo si $a^2 - 3b^2 = \pm 1$, lo que verifica por ejemplo $2 + \sqrt{3} \neq \pm 1$, luego aquí el mcd y el mcm no son únicos salvo signo.
- En $\mathbb{Z}_3[x]$:
$$U\left(\mathbb{Z}_3[x]\right) = U\left(\mathbb{Z}_3\right) = \{1, 2\} = \{1, -1\} = \{\pm 1\}$$

Ejercicio 3. En un DE, tenemos la ecuación diofántica $px + by = 1$, donde p es irreducible. Entre las siguientes afirmaciones, selecciona la que es verdad.

- Nunca tiene solución.
- <u>Puede tener solución o no, depende de b.</u>
- Siempre tiene solución.

Justificación: La ecuación tendrá solución $\Longleftrightarrow \operatorname{mcd}(p, b) \mid 1 \Longleftrightarrow \operatorname{mcd}(p, b) = 1$. Como p es irreducible, equivale a que $p \nmid b$, luego puede tener solución o no, dependiendo de b:

- Para $b = 1$ sí tiene solución.
- Pero para $b = 2p \Longrightarrow \text{mcd}(p, 2p) = p \neq 1$ no tiene solución.

Ejercicio 4. En un DE, tenemos la ecuación diofántica $px + qy = c$, donde p y q son irreducibles no asociados entre sí. Entre las siguientes afirmaciones, selecciona la que es verdad.

- Nunca tiene solución.
- Puede tener solución o no, depende de p y de q.
- Siempre tiene solución.

Justificación: La ecuación tendrá solución $\Longleftrightarrow \text{mcd}(p, q) \mid c$. Como p y q son irreducibles no asociados, tenemos que $\text{mcd}(p, q) = 1$ y como $1 \mid c\ \forall c \in A$, la ecuación siempre tendrá solución.

Ejercicio 5. Entre las siguientes proposiciones, referidas a un DE, selecciona las verdaderas.

- Si la ecuación $ax + by = 1$ tiene solución, entonces la ecuación $ax + by = c$ tiene solución para todo c.
- Si la ecuacióin $ax + bb'y = 1$ tiene solución, entonces las ecuaciones $ax + by = 1$ y $ax + b'y = 1$ tienen solución.
- Si las ecuaciones $ax + by = 1$ y $ax + b'y = 1$ tienen solución, entonces la ecuación $ax + bb'y = 1$ tiene solución.

Justificación:

- Sea (x_0, y_0) solución de $ax + by = 1 \Longrightarrow (cx_0, cy_0)$ es solución de $ax + by = c$.
- Sea (x_0, y_0) solución de $ax + bb'y = 1 \Longrightarrow (x_0, y_0b')$ es solución de $ax + by = 1$ y (x_0, y_0b) es solución de $ax + b'y = 1$.
- $$\left.\begin{array}{lcc} ax + by = 1 \text{ tiene solución} & \Longrightarrow & \text{mcd}(a, b) = 1 \\ ax + b'y = 1 \text{ tiene solución} & \Longrightarrow & \text{mcd}(a, b') = 1 \end{array}\right\} \Longrightarrow \text{mcd}(a, bb') = 1$$

  Luego $ax + bb'y = 1$ tiene solución.

2.7. Cuestionario VII

Ejercicio 1. En relación a las siguientes proposiciones sobre elementos de un DE, selecciona las verdaderas:

- Si $\operatorname{mcd}(a, b) = 1$, entonces $\operatorname{mcd}(a, b^n) = 1$ para todo $n \in \mathbb{N}$.
- Si $a \equiv a' \mod (b)$, entonces $\operatorname{mcd}(a, b) = \operatorname{mcd}(a', b)$.
- Si $a \equiv a' \mod (b)$, entonces $\operatorname{mcm}(a, b) = \operatorname{mcm}(a', b)$.

Ejercicio 2. Entre las siguientes ecuaciones en congruencias, selecciona las que tienen solución.

- En $\mathbb{Z}$, $6x \equiv 10 \mod (45)$.
- En $\mathbb{Z}$, $100x \equiv 20 \mod (15)$.
- En $\mathbb{Z}[i]$, $(2 + 2i)x \equiv 5 \mod (3 - i)$.

Ejercicio 3. Entre las siguientes afirmaciones relativas a ecuaciones en el anillo $\mathbb{Z}_{64}$, selecciona las que son verdad.

- $12x = 28$ tiene 4 soluciones.
- $14x = 28$ tiene 4 soluciones.
- $12x = 30$ tiene 4 soluciones.

Ejercicio 4. Entre las siguientes proposiciones, selecciona las verdaderas.

- El anillo $\mathbb{Z}_{900}$ tiene 240 unidades.
- $14^{20} \equiv 1 \mod (33)$.
- $3^{16} = 3$ en $\mathbb{Z}_{16}$.

Ejercicio 5. Sea p un número primo y considérese la congruencia $ax \equiv 1 \mod (p^2)$. En relación a las siguientes proposiciones, selecciona las verdaderas:

- No tiene solución, pues p^2 no es primo.
- Tiene solución si y sólo si la congruencia $ax \equiv 1 \mod (p)$ tiene solución.
- Tiene solución salvo que a sea múltiplo de p^2.

Ejercicio 1. En relación a las siguientes proposiciones sobre elementos de un DE, selecciona las verdaderas:

- <u>Si $\text{mcd}(a, b) = 1$, entonces $\text{mcd}(a, b^n) = 1$ para todo $n \in \mathbb{N}$.</u>
- <u>Si $a \equiv a' \mod (b)$, entonces $\text{mcd}(a, b) = \text{mcd}(a', b)$.</u>
- Si $a \equiv a' \mod (b)$, entonces $\text{mcm}(a, b) = \text{mcm}(a', b)$.

Justificación:

- Es cierto, lo probamos por inducción:

  Para $n = 0$: $\text{mcd}(a, b^0) = \text{mcd}(a, 1) = 1$, cierto.
  Para $n = 1$: $\text{mcd}(a, b) = 1$, cierto.
  Supuesto cierto para $n - 1$, lo vemos para n:

$$\left.\begin{array}{r}\text{mcd}(a, b) = 1 \\ \text{mcd}(a, b^{n-1}) = 1\end{array}\right\} \text{mcd}(a, b^n) = \text{mcd}(a, b^{n-1}b) = 1$$

- Es cierto, sea A el DE:

$$\begin{aligned} a \equiv a' \mod (b) &\Longrightarrow \exists q \in A \mid a - a' = qb \\ &\Longrightarrow a' = a - qb \end{aligned}$$

$$\text{mcd}(a, b) = \text{mcd}(a - qb, b) = \text{mcd}(a', b)$$

- Es falso, por ejemplo en $\mathbb{Z}$, sean $a = 6$, $a' = 2$, $b = 4$

$$6 \equiv 2 \mod (4)$$
$$\text{mcm}(6, 4) = 12 \neq 4 = \text{mcm}(2, 4)$$

Ejercicio 2. Entre las siguientes ecuaciones en congruencias, selecciona las que tienen solución.

- En $\mathbb{Z}$, $6x \equiv 10 \mod (45)$.
- <u>En $\mathbb{Z}$, $100x \equiv 20 \mod (15)$.</u>
- En $\mathbb{Z}[i]$, $(2 + 2i)x \equiv 5 \mod (3 - i)$.

Justificación:

- $\text{mcd}(6, 45) = 3$, como $3 \nmid 10 \Longrightarrow$ no tiene solución.
- $\text{mcd}(100, 15) = 5$, como $5 \mid 20 \Longrightarrow$ tiene solución:

$$20x \equiv 4 \mod (3) \qquad \text{mcd}(20, 3) = 1$$

$$\begin{aligned} 1 = 20(-1) + 7 \cdot 3 &\Longrightarrow 20 \cdot 1 = -1 \mod (3) \\ &\Longrightarrow 20(-4) \equiv 4 \mod (3) \end{aligned}$$

$$x_0 = -4 \text{ es solución particular}$$
$$x_0 = 2 \text{ es solución óptima}$$
$$x_0 = 2 + 3k \quad k \in \mathbb{Z}$$

- Calculamos $\text{mcd}(2+2i, 3-i)$ en $\mathbb{Q}[i]$:

$$\frac{3-i}{2+2i} = \frac{(2-2i)(3-i)}{8} = \frac{6-2i-6i-2}{8} = \frac{4}{8} - \frac{8i}{8} = \frac{1}{2} - i$$

Tenemos $q = i$, $r = 1+i$

$$\begin{array}{rcc} r_i & u_i & v_i \\ 3-i & 1 & 0 \\ 2+2i & 0 & 1 \\ 1+i & 1 & -i \end{array}$$

Existe solución $\iff 1+i \mid 5$, pero como $1+i \nmid 5$, no existe solución.

Ejercicio 3. Entre las siguientes afirmaciones relativas a ecuaciones en el anillo $\mathbb{Z}_{64}$, selecciona las que son verdad.

- <u>$12x = 28$ tiene 4 soluciones.</u>
- $14x = 28$ tiene 4 soluciones.
- $12x = 30$ tiene 4 soluciones.

Justificación:

- $$\begin{aligned} 12x &\equiv 28 \mod (64) \\ 6x &\equiv 14 \mod (32) \\ 3x &\equiv 7 \mod (16) \end{aligned}$$

Como $\text{mcd}(16, 3) = 1$, tiene solución.

$$\begin{aligned} 1 = 16 \cdot 1 + 3(-5) &\Longrightarrow 3 \cdot 5 \equiv -1 \mod (16) \\ &\Longrightarrow 3 \cdot 5(-7) \equiv 7 \mod (16) \end{aligned}$$

$$\begin{gathered} 5(-7) = -35 \text{ es solución particular} \\ x_0 = 13 \text{ es solución óptima} \\ x = 13 + 16k \quad k \in \mathbb{Z} \end{gathered}$$

Por tanto:

$$\begin{array}{ll} x_1 = 13 & x_2 = 29 \\ x_3 = 45 & x_4 = 61 \end{array}$$

Tiene 4 soluciones.

- $$\begin{aligned} 14x &\equiv 28 \mod (64) \\ 7x &\equiv 14 \mod (32) \end{aligned}$$

$\text{mcd}(7,32) = 1$, tiene solución.

$$\begin{aligned} 1 = 32 \cdot 2 + 7(-9) &\Longrightarrow 7 \cdot 9 \equiv -1 \quad \text{mód } (32) \\ &\Longrightarrow 7 \cdot 9(-14) \equiv 14 \quad \text{mód } (32) \end{aligned}$$

$$\begin{aligned} x_0 = 9(-14) = -126 &\text{ es solución particular} \\ y_0 = 2 &\text{ es solución óptima} \\ x = 2 + 23k \quad & k \in \mathbb{Z} \end{aligned}$$

Por tanto:

$$\begin{aligned} x_1 &= 2 \\ x_2 &= 34 \end{aligned}$$

No tiene 4 soluciones, es falso.

- $$\begin{aligned} 12x &\equiv 30 \quad \text{mód } (64) \\ 6x &\equiv 15 \quad \text{mód } (32) \end{aligned}$$

  $$\text{mcd}(6,32) = 2 \nmid 15 \Longrightarrow \text{ no tiene solución}$$

  Es falso.

Ejercicio 4. Entre las siguientes proposiciones, selecciona las verdaderas.

- $\underline{\text{El anillo } \mathbb{Z}_{900} \text{ tiene 240 unidades.}}$
- $\underline{14^{20} \equiv 1 \text{ mód } (33).}$
- $3^{16} = 3$ en $\mathbb{Z}_{16}$.

Justificación:

- $$|U(\mathbb{Z}_{900})| = \varphi(900) = \varphi(3^2 \cdot 2^2 \cdot 5^2) = 3 \cdot 2 \cdot 5 \cdot 2 \cdot 1 \cdot 4 = 240$$

- $$\left.\begin{aligned} \varphi(33) = \varphi(3 \cdot 11) = 2 \cdot 10 = 20 \\ \text{mcd}(14,33) = 1 \end{aligned}\right\} \overset{\text{Fermat}}{\Longrightarrow} 14^{20} \equiv 1 \quad \text{mód } (33)$$

- $$\begin{aligned} \left.\begin{aligned} \varphi(16) = \varphi(2^4) = 2^3 \cdot 1 = 8 \\ \text{mcd}(3,16) = 1 \end{aligned}\right\} &\Longrightarrow 3^8 \equiv 1 \quad \text{mód } (16) \Longrightarrow 3^{16} \equiv 1 \quad \text{mód } (16) \\ &\Longrightarrow 3^{16} \not\equiv 3 \quad \text{mód } (16) \end{aligned}$$

Ejercicio 5. Sea p un número primo y considérese la congruencia $ax \equiv 1 \mod (p^2)$. En relación a las siguientes proposiciones, selecciona las verdaderas:

- No tiene solución, pues p^2 no es primo.
- Tiene solución si y sólo si la congruencia $ax \equiv 1 \mod (p)$ tiene solución.
- Tiene solución salvo que a sea múltiplo de p^2.

Justificación:

$$\begin{aligned}\text{La equación tiene solución } &\Longleftrightarrow \operatorname{mcd}(a, p^2) \mid 1 \Longleftrightarrow \operatorname{mcd}(a, p^2) = 1 \\ &\Longleftrightarrow \operatorname{mcd}(a, p) = 1 \Longleftrightarrow ax \equiv 1 \mod (p) \text{ tiene solución}\end{aligned}$$

Luego la segunda opción es verdadera. Estudiamos ahora la tercera, si $a = kp^2$ con $k \in A \Longrightarrow \operatorname{mcd}(a, p^2) = p^2$ por lo que es cierto que no tiene solución. Sin embargo, si p^2 es múltiplo de $a \Longrightarrow \operatorname{mcd}(a, p^2) = a$, por lo que tampoco tiene solución. Luego la tercera es falsa, al existir más casos en los que no tiene solución.

2.8. Cuestionario VIII

Ejercicio 1. En el anillo $\mathbb{Z}[i]$, selecciona las afirmaciones verdaderas:

- $2+i$ y $2-i$ son unidades.
- $2+i$ y $2-i$ son asociados.
- $2+i$ y $2-i$ son irreducibles.

Ejercicio 2. Entre las siguientes afirmaciones, selecciona las afirmaciones verdaderas:

- En el anillo $\mathbb{Z}\left[\sqrt{2}\right]$, los número $2+\sqrt{2}$ y $2-\sqrt{2}$ son asociados.
- En el anillo $\mathbb{Z}\left[\sqrt{2}\right]$, los número $2+\sqrt{2}$ y $2-\sqrt{2}$ son primos.
- En el anillo $\mathbb{Z}\left[\sqrt{2}\right]$, el número 2 no es primo.

Ejercicio 3. Entre las siguientes afirmaciones, selecciona las correctas.

- En $\mathbb{Z}[x]$, todo polinomio de grado 1 es irreducible.
- En $\mathbb{Z}[x]$, todo polinomio mónico de grado menor o igual que 3 y sin raíces en $\mathbb{Z}$ es irreducible.
- Todo polinomio de grado mayor o igual que 1 en $\mathbb{Q}[x]$ es asociado a un primitivo de $\mathbb{Z}[x]$.

Ejercicio 4. Entre las siguientes afirmaciones relativas a un polinomio $f \in \mathbb{Z}[x]$, selecciona las que son verdad:

- Si el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.
- Si f es mónico y el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.
- Si f es primitivo y el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.

Ejercicio 5. Entre las siguientes afirmaciones relativas a un polinomo mónimo $f \in \mathbb{Z}[x]$, selecciona las que son verdad:

- Si f no tiene raíces en $\mathbb{Z}$ y para un primo entero $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1 \cdot f_2$ con $\deg(f_1) = 1$, entonces f es irreducible en $\mathbb{Z}[x]$.
- Si para un entero primo $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1^2$ con $\deg(f_1) = 3$ y para un entero primo $q \geqslant 2$, el reducido $R_q(f)$ factoriza en irredcuibles $\mathbb{Z}_q[x]$ en la forma $R_q(f) = g_1g_2g_3$ con $\deg(g_1) = 1 = \deg(g_2)$ y $\deg(g_3) = 4$, entonces f es irreducible.
- Si para un entero primo $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1^2$ con $\deg(f_1) = 2$ y para un entero primo $q \geqslant 2$, el reducido $R_q(f)$ factoriza en irreducibles $\mathbb{Z}_q[x]$ en la forma $R_q(f) = g_1g_2g_3g_4$ con $\deg(g_1) = 1$, entonces f es irreducible.

Ejercicio 1. En el anillo $\mathbb{Z}[i]$, selecciona las afirmaciones verdaderas:

- $2+i$ y $2-i$ son unidades.
- $2+i$ y $2-i$ son asociados.
- $\underline{2+i \text{ y } 2-i \text{ son irreducibles.}}$

Justificación:

- La primera es falsa:
$$N(2+i) = N(2-i) = 5 \neq \pm 1$$
- La segunda también:
$$\frac{2+i}{2-i} = \frac{(2+i)(2+i)}{5} = \frac{3+4i}{5} = \frac{3}{5} + \frac{4}{5}i$$
Luego tenemos $q = i+1$ y $r = (2+i) - (2-i)(1+i) = -1 \neq 0$, así que $2-i \nmid 2+i$, luego no son asociados.
- La tercera es verdad:
$$N(2+i) = N(2-i) = 5 \text{ que es un primo de } \mathbb{Z}$$

Ejercicio 2. Entre las siguientes afirmaciones, selecciona las afirmaciones verdaderas:

- $\underline{\text{En el anillo } \mathbb{Z}\left[\sqrt{2}\right]\text{, los número } 2+\sqrt{2} \text{ y } 2-\sqrt{2} \text{ son asociados.}}$
- $\underline{\text{En el anillo } \mathbb{Z}\left[\sqrt{2}\right]\text{, los número } 2+\sqrt{2} \text{ y } 2-\sqrt{2} \text{ son primos.}}$
- $\underline{\text{En el anillo } \mathbb{Z}\left[\sqrt{2}\right]\text{, el número 2 no es primo.}}$

Justificación: Vemos que $2+\sqrt{2}y2-\sqrt{2}$ son asociados, ya que:
$$\frac{2+\sqrt{2}}{2-\sqrt{2}} = \frac{(2+\sqrt{2})^2}{2} = \frac{6+4\sqrt{2}}{2} = 3+2\sqrt{2}$$
$$\frac{2-\sqrt{2}}{2+\sqrt{2}} = \frac{(2-\sqrt{2})^2}{2} = 3-2\sqrt{2}$$

Luego $2+\sqrt{2} = (2-\sqrt{2})(3+2\sqrt{2})$ y $2-\sqrt{2} = (2+\sqrt{2})(3-2\sqrt{2})$, así que $2+\sqrt{2}$ y $2-\sqrt{2}$ se dividen mutuamente, luego son asociados (la primera es verdad).

Puesto que $\mathbb{Z}\left[\sqrt{2}\right]$ es un DE, es un DFU y ser primo es equivalente a ser irreducible. Como:
$$N\left(2+\sqrt{2}\right) = (2+\sqrt{2})(2-\sqrt{2}) = 4-2 = 2$$
Es un primo de $\mathbb{Z}$, vemos que tanto $2+\sqrt{2}$ como $2-\sqrt{2}$ son primos (la segunda es verdad):. Como:
$$2 = (2+\sqrt{2})(2-\sqrt{2})$$
Deducimos que 2 no es irreducible y, por tanto, no es primo (se verifica la tercera).

Ejercicio 3. Entre las siguientes afirmaciones, selecciona las correctas.

- En $\mathbb{Z}[x]$, todo polinomio de grado 1 es irreducible.
- En $\mathbb{Z}[x]$, todo polinomio mónico de grado menor o igual que 3 y sin raíces en $\mathbb{Z}$ es irreducible.
- Todo polinomio de grado mayor o igual que 1 en $\mathbb{Q}[x]$ es asociado a un primitivo de $\mathbb{Z}[x]$.

Justificación:

- Falsa, sea $f = 6x - 2$, $\deg(f) = 1$ y no es irreducible: $f = 2 \cdot (3x - 1)$.
- Sea $f = x^3 + a_2x^2 + a_1x + a_0$. Por ser mónico, es primitivo. Sus posibles raíces en $\mathbb{Q}$ son de la forma $^a/_b$ donde $a \mid a_0$ y $b \mid 1 \Longrightarrow b = \pm 1$.

  Luego sus posibles raíces en $\mathbb{Q}$ son de la forma $\pm a$, donde $a \mid a_0$, luego sus raíces son enteras. Como f no tiene raíces en $\mathbb{Z} \Longrightarrow$ no tiene raíces en $\mathbb{Q}$.

  Supuesto $\deg(f) = 2 \vee \deg(f) = 3$ Entonces, es irreducible en $\mathbb{Q}$ y, por el criterio de al raíz, es irreducible en $\mathbb{Z}$.

  Supuesto $\deg(f) = 1$ Entonces, $f = x + a_0 \Longrightarrow x = -a_0$ es raíz de f en $\mathbb{Z}$, contradicción, luego no puede ser $\deg(f) = 1$.

  Supuesto $\deg(f) = 0$ Entonces, $f \in \mathbb{Z}$ y como es mónico, $f = 1 \in \mathbb{Z}$. Pero $f = 1 \in U(\mathbb{Z}[x]) \Longrightarrow f$ no es irreducible.

  Por lo que es falsa, sólo es cierto si $f \neq 1$.
- Se ha demostrado que todo $\phi \in \mathbb{Q}[x] \mid \deg(\phi) \geqslant 1$ se puede expresar como $\phi = {^a/_b}f$ con $^a/_b \in \mathbb{Q}$ y $f \in \mathbb{Z}[x]$ primitivo.

  Como $^a/_b \in \mathbb{Q}$ y $\mathbb{Q}$ es un cuerpo $\Longrightarrow {^a/_b} \in U(\mathbb{Q}) \Longrightarrow \phi \sim f$, cierto.

Ejercicio 4. Entre las siguientes afirmaciones relativas a un polinomio $f \in \mathbb{Z}[x]$, selecciona las que son verdad:

- Si el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.
- Si f es mónico y el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.
- Si f es primitivo y el reducido $R_p(f)$ es irreducible en $\mathbb{Z}_p[x]$, entonces f es irreducible.

Justificación:

- Falso, peude ser que $\deg(R_p(f)) \neq \deg(f)$:

$$\text{Sea } f = 2x^2 - 3x + 1 = (2x - 1)(x - 1) \in \mathbb{Z}[x]$$

  $R_2(f) = x + 1 \in \mathbb{Z}_2[x]$ es irreducible, pero f es reducible.

- $$f \text{ mónico } \Longrightarrow \begin{cases} f \text{primitivo} \\ \deg(R_p(f)) = \deg(f) \end{cases}$$

  Por tanto, aplicando el criterio de reducción, $R_p(f)$ es irreducible en $\mathbb{Z}_p[x] \Longrightarrow$ f es irreducible, cierto.

- Falso, puede ser que $\deg(R_p(f)) = \deg(f)$ y tenemos el mismo contraejemplo que para el primer punto.

Ejercicio 5. Entre las siguientes afirmaciones relativas a un polinomo mónimo $f \in \mathbb{Z}[x]$, selecciona las que son verdad:

- Si f no tiene raíces en $\mathbb{Z}$ y para un primo entero $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1 \cdot f_2$ con $\deg(f_1) = 1$, entonces f es irreducible en $\mathbb{Z}[x]$.
- Si para un entero primo $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1^2$ con $\deg(f_1) = 3$ y para un entero primo $q \geqslant 2$, el reducido $R_q(f)$ factoriza en irredcuibles $\mathbb{Z}_q[x]$ en la forma $R_q(f) = g_1 g_2 g_3$ con $\deg(g_1) = 1 = \deg(g_2)$ y $\deg(g_3) = 4$, entonces f es irreducible.
- Si para un entero primo $p \geqslant 2$, el reducido $R_p(f)$ factoriza en irreducibles $\mathbb{Z}_p[x]$ en la forma $R_p(f) = f_1^2$ con $\deg(f_1) = 2$ y para un entero primo $q \geqslant 2$, el reducido $R_q(f)$ factoriza en irreducibles $\mathbb{Z}_q[x]$ en la forma $R_q(f) = g_1 g_2 g_3 g_4$ con $\deg(g_1) = 1$, entonces f es irreducible.

Justificación:

- Como f es mónico, f y $R_p(f)$ tienen el mismo grado, n, y como f no tiene raíces en $\mathbb{Z}$, no tiene divisores de grado 1 ni de grado $n-1$. Además, como $R_p(f)$ no tiene divisores de grado r para cualquier $1 < r < n-1$ (sus únicos divisores propios son, salvo asociados, f_1 y f_2) f tampoco los puede tener. Como es mónico, es primitivo y no tiene divisores propios de grado 0. Luego f es irreducible.

- Como es mónico, f, $R_p(f)$ y $R_q(f)$ tienen el mismo grado, 6. Como $R_p(f)$ no tiene divisores de grados 1, 2, 4 o 5 f tampoco los puede tener. Como $R_q(f)$ no tiene divisores de grado 3, f tampoco los puede tener. Como es mónico, es primitivo y no tiene divisores propios de grado 0. Luego f es irreducible.

- La tercera es falsa: la información sobre $R_p(f)$ nos garantiza que f no tiene divisores de grado 1 o 3, pero puede tenerlos de grado 2, y la segunda información sobre $R_q(f)$ no nos garantiza que f no puede tenerlos. Un contraejemplo sería $f = x^4 + 2x + 1 = (x^2+1)^2$. La factorización en irreducibles de $R_3(f)$ en $\mathbb{Z}_3[x]$ es $(x^2+1)^2$ y la de $R_2(f)$ en $\mathbb{Z}_2[x]$ es $(x+1)^4$.