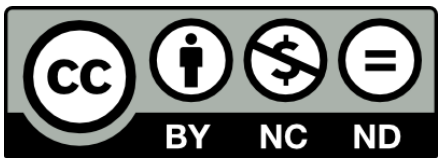
Álgebra I

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 **4**
1.1. Cuestionario I 4
1.2. Cuestionario II 7
1.3. Cuestionario III 11
1.4. Cuestionario IV 14
1.5. Cuestionario V 17
1.6. Cuestionario VI 21
1.7. Cuestionario VII 24
1.8. Cuestionario VIII 29

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:

- Siempre equivalentes.
- 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 $P \Rightarrow R$.
- $P \Rightarrow Q$ siempre que $R \Rightarrow Q$.

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.
- Siempre verdadera.
- 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 $f_*(A) - f_*(B)$.
- $f_*(A - B) = f_*(A) - f_*(B)$.

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:

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

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.
- Siempre verdadera.
- 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 $a \neq 0$:

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

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

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

Justificación:

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

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:

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

Como $\alpha, \beta \notin U(\mathbb{Z}[i]) \implies N(\alpha), N(\beta) \neq \pm 1$ 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, $9 = N(\alpha)N(\beta) \implies N(\alpha) = N(\beta) = 3$.

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

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.

- 2 no es irreducible.

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.

1.6. 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:

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

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.
- $\underline{\text{Puede tener solución o no, depende de } b.}$
- Siempre tiene solución.

Justificación: La ecuación tendrá solución $\iff \text{mcd}(p, b) \mid 1 \iff \text{mcd}(p, b) = 1$. 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 $b = 2p \implies \text{mcd}(p, 2p) = p \neq 1$ 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 $\iff \text{mcd}(p, q) \mid c$. 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 $ax + by = 1 \implies (cx_0, cy_0)$ es solución de $ax + by = c$.
- Sea (x_0, y_0) solución de $ax + bb'y = 1 \implies (x_0, y_0b')$ es solución de $ax + by = 1$ y (x_0, y_0b) es solución de $ax + b'y = 1$.
- $$\left.\begin{array}{rcl} ax + by = 1 \text{ tiene solución} & \implies & \text{mcd}(a, b) = 1 \\ ax + b'y = 1 \text{ tiene solución} & \implies & \text{mcd}(a, b') = 1 \end{array}\right\} \implies \text{mcd}(a, bb') = 1$$

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

1.7. Cuestionario VII

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

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

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

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

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.
- $14^{20} \equiv 1$ mód (33).
- $3^{16} = 3$ en $\mathbb{Z}_{16}$.

Ejercicio 5. Sea p un número primo y considérese la congruencia $ax \equiv 1$ mód (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 $ax \equiv 1$ mód (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:

- Si $\text{mcd}(a,b)=1$, entonces $\text{mcd}(a,b^n)=1$ para todo $n\in\mathbb{N}$.
- Si $a\equiv a'\mod(b)$, entonces $\text{mcd}(a,b)=\text{mcd}(a',b)$.
- 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 $\mathbb{Z}$, $6x\equiv 10\mod(45)$.
- En $\mathbb{Z}$, $100x\equiv 20\mod(15)$.
- 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 $q = i$, $r = 1+i$

r_i	u_i	v_i
$3-i$	1	0
$2+2i$	0	1
$1+i$	1	$-i$

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.

- $\underline{12x = 28 \text{ tiene 4 soluciones.}}$
- $14x = 28$ 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.

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

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

Por tanto:

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

Tiene 4 soluciones.

-

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

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

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

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

Por tanto:

$$x_1 = 2$$
$$x_2 = 34$$

No tiene 4 soluciones, es falso.

- $$12x \equiv 30 \mod (64)$$
$$6x \equiv 15 \mod (32)$$

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

Es falso.

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 $\mathbb{Z}_{16}$.

Justificación:

- $$|U(\mathbb{Z}_{900})| = \varphi(900) = \varphi(3^2 \cdot 2^2 \cdot 5^2) = 3 \cdot 2 \cdot 5 \cdot 2 \cdot 1 \cdot 4 = 240$$
- $$\left.\begin{array}{r} \varphi(33) = \varphi(3 \cdot 11) = 2 \cdot 10 = 20 \\ \text{mcd}(14, 33) = 1 \end{array}\right\} \overset{\text{Fermat}}{\Longrightarrow} 14^{20} \equiv 1 \mod (33)$$
- $$\left.\begin{array}{r} \varphi(16) = \varphi(2^4) = 2^3 \cdot 1 = 8 \\ \text{mcd}(3, 16) = 1 \end{array}\right\} \Longrightarrow 3^8 \equiv 1 \mod (16) \Longrightarrow 3^{16} \equiv 1 \mod (16)$$
$$\Longrightarrow 3^{16} \not\equiv 3 \mod (16)$$

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.

Justificación:

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

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

1.8. 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 $R_q(f) = g_1 g_2 g_3$ 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.

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.

Justificación:

- La primera es falsa:
$$N(2+\text{ì}) = N(2-i) = 5 \neq \pm 1$$
- 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:

- 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.

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

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 $b \mid 1 \implies b = \pm 1$.

  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 $\mathbb{Z} \implies$ 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, $f = x + a_0 \implies x = -a_0$ 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 $f = 1 \in U(\mathbb{Z}[x]) \implies f$ 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 $\implies a/b \in U(\mathbb{Q}) \implies \phi \sim f$, 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.

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

  Por tanto, aplicando el criterio de reducción, $R_p(f)$ es irreducible en $\mathbb{Z}_p[x] \implies$ 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 $(x+1)^4$.