

Ayudantía 12

Repaso para la prueba

- Determine los divisores de 0 de $\mathbb{Z}_8$.

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Así, serán 2, 4, 6 y 8.

- Verifique que $\mathbb{Z}[i]$ es dominio integral.

Para verificar que $\mathbb{Z}[i]$, el anillo de los enteros gaussianos, es un **dominio de integridad**, debemos comprobar las siguientes propiedades:

- Es un anillo conmutativo con unidad.

El anillo $\mathbb{Z}[i]$ está formado por todos los números complejos de la forma $a + bi$, donde $a, b \in \mathbb{Z}$, y i es la unidad imaginaria ($i^2 = -1$).

- Es **conmutativo** porque la suma y el producto son conmutativos en los números complejos.
- Tiene una **unidad multiplicativa**, que es 1, porque $1 \cdot (a + bi) = a + bi$.

Por lo tanto, $\mathbb{Z}[i]$ es un anillo conmutativo con unidad.

- No tiene divisores de cero.

Un anillo es un **dominio de integridad** si no tiene divisores de cero, es decir, si $x, y \in \mathbb{Z}[i]$ y $xy = 0$, entonces $x = 0$ o $y = 0$.

Supongamos que $x = a + bi$ y $y = c + di$, con $a, b, c, d \in \mathbb{Z}$. Entonces, el producto es:

$$xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Si $xy = 0$, esto implica que tanto la parte real como la parte imaginaria deben ser cero:

$$ac - bd = 0 \quad \text{y} \quad ad + bc = 0.$$

Resolver este sistema de ecuaciones lineales implica que $x = 0$ o $y = 0$ en $\mathbb{Z}[i]$, porque a, b, c, d son enteros y no hay soluciones no triviales con $a, b, c, d \neq 0$.

Por lo tanto, $\mathbb{Z}[i]$ no tiene divisores de cero.

3. Demuestre $B = \{x \in A : x \cdot a = 0\}$ es un subanillo de A .

Queremos demostrar que el conjunto

$$B = \{x \in A : x \cdot a = 0\}$$

es un subanillo del anillo A , donde $a \in A$. Para ello, verificaremos que cumple las siguientes propiedades:

- B no está vacío Por definición, $0 \cdot a = 0$ para cualquier $a \in A$. Esto implica que $0 \in B$, lo que garantiza que $B \neq \emptyset$.
- Cerradura bajo la suma Sean $x, y \in B$. Por la definición de B , tenemos que $x \cdot a = 0$ y $y \cdot a = 0$. Queremos probar que $(x + y) \in B$, es decir, que:

$$(x + y) \cdot a = 0.$$

Usamos la distributividad del producto en A :

$$(x + y) \cdot a = (x \cdot a) + (y \cdot a).$$

Como $x \cdot a = 0$ y $y \cdot a = 0$, obtenemos:

$$(x + y) \cdot a = 0 + 0 = 0.$$

Por lo tanto, $x + y \in B$, y B es cerrado bajo la suma.

- Cerradura bajo la multiplicación Sean $x, y \in B$. Por la definición de B , tenemos que $x \cdot a = 0$ y $y \cdot a = 0$. Queremos probar que $(x \cdot y) \in B$, es decir, que:

$$(x \cdot y) \cdot a = 0.$$

Usamos la asociatividad del producto en A :

$$(x \cdot y) \cdot a = x \cdot (y \cdot a).$$

Dado que $y \cdot a = 0$, sustituimos:

$$(x \cdot y) \cdot a = x \cdot 0 = 0.$$

Por lo tanto, $x \cdot y \in B$, y B es cerrado bajo la multiplicación.

- Cerradura bajo la negación Sea $x \in B$. Por la definición de B , tenemos que $x \cdot a = 0$. Queremos probar que $-x \in B$, es decir, que:

$$(-x) \cdot a = 0.$$

Usamos la distributividad del producto en A :

$$(-x) \cdot a = -(x \cdot a).$$

Dado que $x \cdot a = 0$, tenemos:

$$(-x) \cdot a = -0 = 0.$$

Por lo tanto, $-x \in B$, y B es cerrado bajo la negación.

4. Valores de $c \in \mathbb{Z}_3$ tales que $\mathbb{Z}_3[x]/(x^3 + x^2 + c)$ sea un cuerpo
Queremos determinar los valores de $c \in \mathbb{Z}_3$ tales que el anillo cociente

$$\mathbb{Z}_3[x]/(x^3 + x^2 + c)$$

sea un cuerpo. Para que esto ocurra, el polinomio $f(x) = x^3 + x^2 + c$ debe ser irreducible sobre $\mathbb{Z}_3$, lo cual significa que $f(x)$ no debe factorizarse como el producto de polinomios de menor grado.

- Verificar si $f(x)$ tiene raíces en $\mathbb{Z}_3 = \{0, 1, 2\}$
Sustituimos los valores de x en $f(x) = x^3 + x^2 + c$ para verificar si tiene raíces en $\mathbb{Z}_3$:

– Para $x = 0$:

$$f(0) = 0^3 + 0^2 + c = c.$$

Entonces, $f(0) = 0$ si $c = 0$.

– Para $x = 1$:

$$f(1) = 1^3 + 1^2 + c = 1 + 1 + c = 2 + c.$$

Entonces, $f(1) = 0$ si $c = 1$.

– Para $x = 2$:

$$f(2) = 2^3 + 2^2 + c = 8 + 4 + c = 12 + c \equiv 0 + c \pmod{3}.$$

Entonces, $f(2) = 0$ si $c = 0$.

• Determinar los valores de c

- Si $c = 0$, entonces $f(x) = x^3 + x^2$, que es factorizable como $x^2(x + 1)$. Por lo tanto, $f(x)$ no es irreducible en este caso.
- Si $c = 1$, entonces $f(x) = x^3 + x^2 + 1$. Al comprobar que $f(x)$ no tiene raíces en $\mathbb{Z}_3$ y no se puede factorizar, concluimos que $f(x)$ es irreducible cuando $c = 1$.
- Si $c = 2$, entonces $f(x) = x^3 + x^2 + 2$. Comprobamos que $f(x)$ no tiene raíces en $\mathbb{Z}_3$ y es irreducible.