Parcial II - Anillos y Campos

Universidad Distrital Francisco José de Caldas

1. ¿El polinomio $x^2 + 3$ es irreducible en $\mathbb{Z}_7$?

   - Para determinar si el polinomio $x^2 + 3$ es irreducible en $\mathbb{Z}_7$, podemos usar el siguiente criterio:

     Teorema (Fraleigh, 7ª edición, Teorema 23.10): Un polinomio cuadrático o cúbico $f(x)$ sobre un campo finito $\mathbb{F}$ es reducible si y solo si tiene una raíz en $\mathbb{F}$.

     Paso 1: Evaluar el polinomio en los elementos de $\mathbb{Z}_7$

     Calculamos $f(a) = a^2 + 3$ para $a \in \mathbb{Z}_7$:

     $$\begin{aligned}
     f(0) &= 0^2 + 3 = 3 \not\equiv 0 \pmod 7\\
     f(1) &= 1^2 + 3 = 4 \not\equiv 0 \pmod 7\\
     f(2) &= 2^2 + 3 = 4 + 3 = 7 \equiv 0 \pmod 7\\
     f(3) &= 3^2 + 3 = 9 + 3 = 12 \equiv 5 \pmod 7\\
     f(4) &= 4^2 + 3 = 16 + 3 = 19 \equiv 5 \pmod 7\\
     f(5) &= 5^2 + 3 = 25 + 3 = 28 \equiv 0 \pmod 7\\
     f(6) &= 6^2 + 3 = 36 + 3 = 39 \equiv 4 \pmod 7
     \end{aligned}$$

     Paso 2: Concluir sobre la reducibilidad

     Observamos que $f(2) \equiv 0 \pmod 7$ y $f(5) \equiv 0 \pmod 7$, lo que significa que $x^2 + 3$ tiene raíces en $\mathbb{Z}_7$, específicamente $x = 2$ y $x = 5$. Según el teorema citado, esto implica que $x^2 + 3$ es **reducible** en $\mathbb{Z}_7$.

     Por lo tanto, el polinomio $x^2 + 3$ **no es irreducible en** $\mathbb{Z}_7$.

2. Dé un ejemplo de un Dominio de Factorización Única que no sea Dominio Euclidiano. *(Es evidente que debe mostrar el porqué no lo es).*

   Ejemplo: Consideremos el anillo $\mathbb{Z}[x]$ de polinomios en una variable con coeficientes enteros.

(a) $\mathbb{Z}[x]$ **es un DFU:**

Se sabe que $\mathbb{Z}$ es un dominio de factorización unica (DFU) y, además, el anillo de polinomios sobre un DFU también es DFU. Por lo tanto, $\mathbb{Z}[x]$ es un DFU.

(b) $\mathbb{Z}[x]$ **no es un Dominio Euclidiano:**

Recordemos que todo dominio euclidiano es, en particular, un dominio principal de ideales (DIP). Demostraremos que $\mathbb{Z}[x]$ no es PID, por lo que no puede ser euclidiano.

Consideremos el ideal

$$I = \langle 2, x \rangle = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}.$$

Supongamos, buscando una contradicción, que I es principal. Entonces existiría un polinomio $h(x) \in \mathbb{Z}[x]$ tal que

$$I = \langle h(x) \rangle.$$

Esto implicaría que $h(x)$ divide a ambos generadores 2 y x.

Analicemos las posibilidades para $h(x)$:

- **Si** $h(x)$ **es una unidad** (es decir, $h(x) = \pm 1$): Entonces $\langle h(x) \rangle = \mathbb{Z}[x]$. Sin embargo, en este caso $1 \in \mathbb{Z}[x]$ estaría en I, lo cual es falso, ya que no es posible expresar 1 como una combinación lineal entera de 2 y x.
- **Si** $h(x)$ **es asociado a** 2 (es decir, $h(x) = \pm 2$): En este caso, aunque $h(x)$ divide a 2, se debe verificar si también divide a x. Pero no es posible que 2 divida a x en $\mathbb{Z}[x]$ ya que, de haberlo, existiría un polinomio $q(x) \in \mathbb{Z}[x]$ tal que

  $$x = 2q(x).$$

  Esto implica que todos los coeficientes de $q(x)$ serían fraccionarios, lo cual es imposible en $\mathbb{Z}[x]$.
- **Si** $\deg(h(x)) \geq 1$**:** Entonces $h(x)$ es un polinomio no constante. Pero en ese caso, $h(x)$ no puede dividir al entero 2 (que es de grado 0), a menos que 2 sea producto de $h(x)$ por algún polinomio, lo que no es posible.

Dado que ninguna de las opciones permite que $h(x)$ divida simultáneamente a 2 y a x, concluimos que el ideal $I = \langle 2, x \rangle$ **no es principal**.

Conclusión: Aunque $\mathbb{Z}[x]$ es un dominio de factorización , no es un dominio euclidiano, ya que no es un dominio principal (el ideal $\langle 2, x \rangle$ no es principal). Este ejemplo ilustra que la propiedad de ser DFU no implica ser DE.

3. Demuestre que en todo dominio euclidiano, para cualesquiera dos elementos a y b, existe el máximo común divisor.

4. Demuestre que todo Dominio Euclidiano es un Dominio de Factorización Única.

5. Sea p un primo de la forma $4n + 3$. Muestre que $\mathbb{Z}_p[i]$ es un campo. *Sugerencia: Use el hecho de que los primos de esta forma no se pueden escribir como suma de cuadrados en los enteros.*