Segunda prueba (sorpresa) de clase

21 Mayo de 2025

1. Demuestra que el cuerpo $\mathbb{F}_{16}$ puede presentarse como $\mathbb{F}_2(a)$, donde $a \in \mathbb{F}_{16}$ cumple la relación $a^4 + a + 1 = 0$.
2. Prueba que a es un elemento primitivo y generador del grupo cíclico $\mathbb{F}_{16}^{\times}$.
3. Resuelve la ecuación $x^2 + x + 1 = 0$ en $\mathbb{F}_{16}$.
4. Describe los homomorfismos de $\mathbb{F}_4$ en $\mathbb{F}_{16}$.

(1) Llamemos $f = x^4+x+1 \in \mathbb{F}_2[x]$, y comprobemos que f es irreducible. Por un lado $f(0) = 1 \neq 0$, $f(1) = 1 \neq 0$, luego f no puede tener factores de grado 1. Por otro lado, el único polinomio cuadrático irreducible en $\mathbb{F}_2[x]$ es x^2+x+1, pero

$$(x^2+x+1)^2 = (x^2+x)^2 + 1 = x^4+x^2+1 \neq f,$$

con lo que tampoco puede tener factores de grado 2 y así f es irreducible. De aquí que el anillo $\mathbb{F}_2[x]/\langle f\rangle$ sea un cuerpo. Consideremos ahora el homomorfismo $\sigma: \mathbb{F}_2 \longrightarrow \mathbb{F}_2[x]/\langle f\rangle$, $\sigma(c) = c + \langle f\rangle$, el cual nos permite ver a $\mathbb{F}_2[x]/\langle f\rangle$ como una extensión de $\mathbb{F}_2$. El elemento $a = x + \langle f\rangle$ satisface la relación

$$\begin{aligned} a^4 + a + 1 &= (x+\langle f\rangle)^4 + x + \langle f\rangle + 1 + \langle f\rangle \\ &= x^4 + x + 1 + \langle f\rangle \\ &= 0 + \langle f\rangle, \end{aligned}$$

luego es raíz de f y por tanto $[\mathbb{F}_2[x]/\langle f\rangle : \mathbb{F}_2] = 4$ y tenemos un isomorfismo de $\mathbb{F}_2$-espacios vectoriales $\mathbb{F}_2[x]/\langle f\rangle \cong (\mathbb{F}_2)^4$, de donde

$$\#\, \mathbb{F}_2[x]/\langle f\rangle = 2^4 = 16.$$

Por la clasificación de cuerpos finitos $\mathbb{F}_2[x]/\langle f\rangle \cong \mathbb{F}_{16}$, por lo que $\mathbb{F}_{16}$ puede presentarse como

$$\mathbb{F}_{16} = \mathbb{F}_2(a), \quad a^4 + a + 1 = 0.$$

(2) Como $|\mathbb{F}_{16}^{\times}| = 16-1 = 15$, por el teorema de Lagrange $|a| = 1, 3, 5$ ó 15. No puede ser 1, ya que $a \neq 1$. Si fuese $|a| = 3$, entonces $a^3 = 1$, es decir $a^3 + 1 = 0$, pero esto no es posible ya que una base de $\mathbb{F}_2(a)$ sobre $\mathbb{F}_2$ es $\{1, a, a^2, a^3\}$. Si fuese $|a| = 5$, entonces $a^5 = 1$, pero la relación $a^4 + a + 1 = 0$, nos da $a^5 = a^2 + a$ y por tanto $a^2 + a + 1 = 0$, lo cual es otra contradicción por el mismo motivo anterior. La única salida es $|a| = 15 = |\mathbb{F}_{16}^{\times}|$ y por tanto $\langle a \rangle = \mathbb{F}_{16}^{\times}$, luego a es un elemento primitivo.

(3 y 4) El polinomio $g = x^2 + x + 1 \in \mathbb{F}_2[x]$ es irreducible, ya que tiene grado 2 y no tiene raíces, pues $g(0) = 1 \neq 0$, $g(1) = 1 \neq 0$. Un argumento análogo al del apartado (1) nos dice que $\mathbb{F}_2[x]/\langle g \rangle$ es una extensión de $\mathbb{F}_2$ con $[\mathbb{F}_2[x]/\langle g \rangle : \mathbb{F}_2] = 2$, y por tanto $\mathbb{F}_2[x]/\langle g \rangle \cong \mathbb{F}_4$. De aquí que $\mathbb{F}_4$ admita una presentación como $\mathbb{F}_4 = \mathbb{F}_2(b)$, $b^2 + b + 1 = 0$. Por el apartado (2) b es un elemento primitivo y $\langle b \rangle = \mathbb{F}_4^{\times}$. Tomemos ahora cualquier homomorfismo $\sigma : \mathbb{F}_4 \to \mathbb{F}_{16}$. Entonces σ induce un homomorfismo de grupos $\mathbb{F}_4^{\times} \to \mathbb{F}_{16}^{\times}$, luego σ queda determinado por la imagen de b y esta ha de cumplir dos condiciones

- $\sigma(b)^3 = 1$, ya que $b^3 = 1$.
- $\sigma(b)$ es raíz de $x^2+x+1 \in \mathbb{F}_{16}[x]$.

Como x^2+x+1 tiene grado 2 hay a lo más dos homomorfismos. Por otra parte, los elementos $a^5, a^{10} \in \mathbb{F}_{16}$ satisfacen $(a^5)^3 = a^{15} = 1$, $(a^{10})^3 = a^{30} = 1$ y

$$(a^5)^2 + a^5 + 1 = a^{10} + a^5 + 1 = a^{10} + a^2 + a + 1$$
$$= a^2+a+1 + a^2+a+1 = 0,$$
$$(a^{10})^2 + a^{10} + 1 = a^{20} + a^{10} + 1 = a^{5} + a^2+a+1 + 1$$
$$= a^2 + a + a^2 + a$$
$$= 0$$

Luego ambos son raíces de $x^2+x+1 \in \mathbb{F}_{16}[x]$. Estas son todas las posibles soluciones de la ecuación $x^2+x+1 = 0$ en $\mathbb{F}_{16}$, y dan lugar a los dos únicos homomorfismos $\sigma_i : \mathbb{F}_4 \longrightarrow \mathbb{F}_{16}$, $i=1,2$; determinados por $\sigma_1(b) = a^5$, $\sigma_2(b) = a^{10}$.