

Lema. Sean \mathbb{F}_1 y \mathbb{F}_2 dos cuerpos y sea $\sigma: \mathbb{F}_1 \rightarrow \mathbb{F}_2$ un isomorfismo de cuerpos. Consideremos $\Phi_\sigma: \mathbb{F}_1[X] \rightarrow \mathbb{F}_2[X]$, el isomorfismo del lema anterior. Si $f(X) \in \mathbb{F}_1[X]$ es un polinomio irreducible de $\mathbb{F}_1[X]$, entonces $f^\sigma(X)$ es un polinomio irreducible de $\mathbb{F}_2[X]$.

Demostración. Sea $f(X) = a_0 + a_1X + \dots + a_nX^n$ un polinomio irreducible de $\mathbb{F}_1[X]$. Entonces

$$f^\sigma(X) = \sigma(a_0) + \sigma(a_1)X + \dots + \sigma(a_n)X^n$$

Como $f(X)$ es un polinomio no nulo, podemos suponer $a_n \neq 0$, y como σ es un isomorfismo, entonces $\sigma(a_n) \neq 0$, de forma que $\deg(f^\sigma(X)) = \deg(f(X)) \neq 0$ por ser $f(X)$ irreducible.

Por otra parte, supongamos que $f^\sigma(X) = r(X)s(X)$ para ciertos $r(X), s(X) \in \mathbb{F}_2[X]$, y veamos que o bien $\deg(r(X)) = 0$, o bien $\deg(s(X)) = 0$. Como Φ_σ es sobreyectiva (pues, como se probó en el lema anterior, es un isomorfismo), existen $p(X), q(X) \in \mathbb{F}_1[X]$ tales que $r(X) = \Phi_\sigma(p(X))$ y $s(X) = \Phi_\sigma(q(X))$. Tenemos entonces

$$\underbrace{\Phi_\sigma(f(X))}_{f^\sigma(X)} = \underbrace{\Phi_\sigma(p(X))}_{r(X)} \underbrace{\Phi_\sigma(q(X))}_{s(X)} = \Phi_\sigma(p(X)q(X)),$$

así que, por la inyectividad de Φ_σ , debe ser $f(X) = p(X)q(X)$. Pero $f(X)$ es irreducible en $\mathbb{F}_1[X]$, luego o bien $\deg(p(X)) = 0$, o bien $\deg(q(X)) = 0$, y como Φ_σ preserva los grados, entonces $\deg(r(X)) = \deg(\Phi_\sigma(p(X))) = 0$ ó $\deg(s(X)) = \deg(\Phi_\sigma(q(X))) = 0$, concluyéndose que $f^\sigma(X)$ es irreducible en $\mathbb{F}_2[X]$. \square