

1. Sea  $f = x^6 + x + 1 \in \mathbb{F}_2[x]$  y  $K$  su cuerpo de descomposición.

a) Si  $\alpha \in K$  es raíz de  $f$  entonces  $\alpha = \mathbb{F}_2(\alpha)$

b) Dedicar si  $\mathbb{F}_2(\alpha)^6 = \alpha$

c) Resolver en  $K$  la ecuación  $x^6 + x + 1 = 0$

Como estrategia base, trabajemos de estudiar la irreducibilidad de  $f$ , pues en caso que sea irreducible tendríamos que  $\text{Irr}(\alpha, \mathbb{F}_2) = f$  de donde  $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 6$  obteniendo así que  $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$  es una  $\mathbb{F}_2$ -base de  $\mathbb{F}_2(\alpha)$ .

Además, como  $\mathbb{F}_2(\alpha) \subseteq K$ , bastaría ver que  $\mathbb{F}_2(\alpha)$  contiene todas las raíces de  $\text{Irr}(\alpha, \mathbb{F}_2)$  para obtener la igualdad. Sin embargo, como  $\mathbb{F}_2 \leq \mathbb{F}_2(\alpha)$  es una extensión de cuerpos finitos tenemos que es de Galois y, en particular, es una extensión normal. Como  $\alpha \in \mathbb{F}_2(\alpha)$  es raíz de  $\text{Irr}(\alpha, \mathbb{F}_2)$  tenemos que  $\mathbb{F}_2(\alpha)$  debe contener todas las raíces y por lo tanto se tiene la igualdad. El motivo de por qué basta con esto es que tendríamos que  $\mathbb{F}_2(\alpha)$  sería cuerpo de descomposición de  $\text{Irr}(\alpha, \mathbb{F}_2)$ ; por tanto, el Teorema de Unicidad del cuerpo de descomposición nos asegura que  $K$  y  $\mathbb{F}_2(\alpha)$  son isomorfos. Ahora bien, como  $\mathbb{F}_2(\alpha) \leq K$  debe tenerse la igualdad.

a) Con el razonamiento anterior, buscamos probar que  $f$  es irreducible en  $\mathbb{F}_2[x]$ , como  $f(0) = 1 = f(1)$  tenemos que no tiene raíces. Además, debemos probar que  $f$  no tiene factores irreducibles de orden 2 o 3. Dichos factores podrían ser algunos de estos  $\{x^2 + x + 1, x^3 + x + 1\}$ ; sin embargo, se tiene que ninguno de ellos divide a  $f$  (hágase las divisiones). Por lo tanto, tenemos que  $f = \text{Irr}(\alpha, \mathbb{F}_2)$  como se buscaba.

Como añadido, una de las Teoremas sobre cuerpos finitos nos asegura que  $\mathbb{F}_2(\alpha) \cong \mathbb{F}_{64}$  y que el grupo de Galois de la extensión es el cíclico de orden 6 (cavidad de la extensión de Galois), generado por el automorfismo de Frobenius

$$\tau(\alpha) = \alpha^3 \quad \forall \alpha \in \mathbb{F}_2(\alpha)$$

es decir,  $\text{Aut}_{\mathbb{F}_2}(\mathbb{F}_2(\alpha)) = \{\tau_i : i = 1, 2, 4, 8, 16, 32\}$  donde  $\tau_i(\alpha) = \alpha^{3^i}$ .

b) Para ver que  $\mathbb{F}_2(\alpha)^6 = \alpha$  bastaría ver que el orden de  $\alpha$  es 63; para ello, buscaremos descartar las demás posibilidades ofrecidas por el Teorema de LAGRANGE. Tenemos la  $\mathbb{F}_2$ -base obtenida en el razonamiento previo y que  $\alpha^6 + \alpha + 1 = 0 \Leftrightarrow \alpha^6 = \alpha + 1$ .

i) Como  $\alpha$  y  $1$  son  $\mathbb{F}_2$ -linealmente independientes entre sí.

ii) Como  $\alpha^3$  y  $1$  son  $\mathbb{F}_2$ -linealmente independientes entre sí.

iii)  $\alpha^7 = \alpha^6 \alpha = (\alpha + 1) \alpha = \alpha^2 + \alpha \neq 1$  por ser  $\mathbb{F}_2$ -linealmente independientes ( $\alpha^2, \alpha, 1$ ).

iv)  $\alpha^9 = \alpha^6 \alpha^3 = (\alpha + 1) \alpha^3 = \alpha^4 + \alpha + 1$  idem.

$$v) \alpha^{23} = (\alpha^7)^3 = (\alpha^2 + \alpha)^3 = \alpha^3(\alpha + 1)^3 = \alpha^3(\alpha^3 + \alpha + \alpha^2 + 1) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$$

por el mismo motivo.

Por tanto  $\text{O}(\alpha) = 63$  obteniendo el resultado que buscábamos.

c) Este es un ejercicio clásico; como  $\mathbb{F}_2(\alpha) = \mathbb{F}_{8^3}$  se tiene que  $\mathbb{F}_{8^3}$  contiene todas las raíces del polinomio  $x^{64}-x \in \mathbb{F}_2[x]$ . Como dicho polinomio se factoriza como producto de todos los polinomios irreducibles de grado un divisor de 6 contiene las raíces de  $p=x^3+x+1$ ; de hecho, como es único bastará encontrar un elemento con orden multiplicativo 3 sobre  $\mathbb{F}_{8^3}^\times$ , pues si  $b \in \mathbb{F}_{8^3}^\times$  no sea raíz de  $p$  un razonamiento análogo nos prueba que  $\mathbb{F}_2(b) = \mathbb{F}_4$  con  $\{1, b\}$  una  $\mathbb{F}_2$ -base de  $\mathbb{F}_2(b)$  de donde se deduce que  $\text{O}(b)=3$  pues  $b^2 = b+1$ . Por tanto, como  $\alpha^{21}$  tiene orden multiplicativo 3 será raíz de  $p$ ; al hora, usando el automorfismo de frobenius de la extensión  $\mathbb{F}_2 \leq \mathbb{F}_2(\alpha)$  obtenemos que  $\alpha^{42}$  es la otra raíz.