

Ejercicio 1. Calcular el número de polinomios monicos irreducibles de grado menor o igual que 3 en $\mathbb{F}_5[x]$.

Consideramos el polinomio $x^{125} - x \in \mathbb{F}_5[x]$. Sabemos por el último teorema del teorema que este se descompone como el producto de todos los polinomios irreducibles de $\mathbb{F}_5[x]$ de grado 1 o 3. Como hay 5 de grado 1 tenemos que habrá $20_5 = 40$ de grado 3. Sustituyendo se consigue que hay 10 de grado 2.

Ejercicio 2. ¿Cuántos subcuerpos tiene \mathbb{F}_{256} ?

Sabemos que $256 = 2^8$ por lo que $[\mathbb{F}_{256} : \mathbb{F}_2] = 8 = |\text{Aut}(\mathbb{F}_{256})| = 8$. Gracias a la conexión de Galois sabemos que la cantidad de subcuerpos de \mathbb{F}_{256} está en biyección con la cantidad de subgrupos de $\text{Aut}(\mathbb{F}_{256})$. Además, sabemos por otro de los teoremas que $\text{Aut}(\mathbb{F}_{256})$ es el cíclico de orden 8. De Álgebra II sabemos que habrá un subgrupo para cada divisor de 8, es decir, habrá 3 subgrupos no triviales y por tanto 2 subextensiones no triviales.

Ejercicio 3. Sea a un elemento primitivo de \mathbb{F}_{81} , exprese los subcuerpos de \mathbb{F}_{81} en función de a .

Como a es un elemento primitivo de \mathbb{F}_{81} tenemos que $a\alpha = \mathbb{F}_{81}^\times$ por lo que $|\alpha| = 80$. Ahora bien, como $\mathbb{F}_{81} = \mathbb{F}_{3^4}$ tenemos que $|\text{Aut}(\mathbb{F}_{81})| = 4$ donde es el cíclico de orden 4. Seguimos con el resultado análogo al ejercicio anterior tenemos que hay un único subgrupo no trivial de orden 2. Equivalentemente, buscamos el subcuerpo de \mathbb{F}_9 , que es $\mathbb{F}_{3^2} = \mathbb{F}_9$.

Ahora bien, como $\mathbb{F}_9 \leq \mathbb{F}_{81}^\times$ es cíclico, buscamos un elemento de $\mathbb{F}_{81}^\times = \langle a \rangle$ cuyo orden multiplicativo sea 8; es válido tomar a^{10} . De hecho, se cumple que $\mathbb{F}_9 \leq \mathbb{F}_9(a^{10}) \leq \mathbb{F}_9(a) \cong \mathbb{F}_{81}$ donde $\mathbb{F}_9(a^{10}) \cong \mathbb{F}_9$ por ser este el único subcuerpo no trivial de \mathbb{F}_{81} .