Problemas de Teoría de Cuerpos

Rodrigo Raya Castellano
Universidad de Granada

1. Problema2

EJERCICIO 1.1: Hallar $\sigma \in \mathbb{F}_{3^6}^X$ con $gr(Irr(\sigma, \mathbb{F}_3)) = 6$ y expresarlo como elemento de $\mathbb{F}_3(\alpha)$ donde α es una raíz del polinomio $q = X^6 + X + 2$ (que es un generador de $\mathbb{F}_{3^6}^X$).

Necesitamos un polinomio p mónico e irreducible sobre $\mathbb{F}_3$ tal que algún polinomio X^i con $i < 728$ al divirlo por p de resto 1.

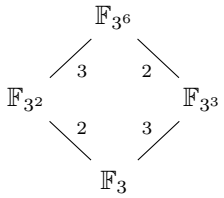
Los factores irreducibles del polinomio $X^{3^6} - X$ son los irreducibles sobre F_3 de grado divisor de 6. En Mathematica esta lista se puede obtener mediante el comando

$$Factor[X^{729} - X, Modulus- > 3]$$

Tras un par de comprobaciones el polinomio $p = 2 + x + x^2 + 2x^3 + x^6$ verifica que x^{104} da 1 de resto al dividirse por p. Tenemos entonces un σ que no puede ser generador. La expresión de σ en $\mathbb{F}_3(\alpha)$ se obtiene al dividir p mediante el polinomio q de donde obtenemos el polinomio $2X^3 + X^2$ visto como elemento en $\frac{\mathbb{F}_3[X]}{<X^6+X+2>}$ el correspondiente elemento en $\mathbb{F}_3(\alpha)$ es $\alpha^2 + 2\alpha^3$.

EJERCICIO 1.2: Un elemento $\beta \in \mathbb{F}_{729}$ de orden 8 en $\mathbb{F}_{3^6}^X$ da una extensión $\mathbb{F}_3(\beta) = \mathbb{F}_9$

Observemos primero la construcción sobre la cual trabajan este ejercicio y el posterior.



Un cuerpo de p^m elementos es subcuerpo de otro con p^n si y sólo si $m|n$.

Volviendo a nuestro problema, si $\beta^8 = 1$ esto implica que β es raíz del polínomio $X^9 - X$ y por tanto, su polinomio mínimo será un factor irreducible de este. Pero los factores irreducibles de este deben tener grado divisor de 2. Luego deben ser de grado 1 o grado 2. De hecho, si observamos la descomposición en Mathematica mediante la orden

$$Factor[X^9 - X, Modulus- > 3]$$

obtenemos los polinomios $X, (1 + X), (2 + X), (1 + X^2), (2 + X + X^2), (2 + 2X + X^2)$. Como β es de orden 8 β no puede ser $0, 1, 2$ ya que estos tienen orden $\infty, 1, 2$ respectivamente luego tiene que ser raíz de los de grado 2. Esto implica que $\mathbb{F}_3(\beta) = \mathbb{F}_9$.

EJERCICIO 1.3: Analiza qué ocurre al considerar el elemento σ para encontrar elementos que generen las extensiones $\mathbb{F}_{3^2}$ y $\mathbb{F}_{3^3}$.

Como ya habíamos comentado el orden es 104. En el primer caso, el método anterior donde tomamos $\sigma^{\frac{104}{8}} = \sigma^1 3$ entonces el método funciona y se obtiene cero al comprobar donde el polinomio irreducible del que es raíz σ resulta ser $X^2 + X + 2$. Sin embargo, aunque $\sigma^{\frac{104}{26}} = \sigma^4$ que es un elemento de orden 26, aparentemente no sirve para generar la extensión $\mathbb{F}_{3^3}$. Actualmente, no sabemos por qué se obtiene este resultado. Podríamos ser un poco tramposos y cambiar el polinomio por uno tal que 26 no divida su orden. Pero dejamos para una posterior revisión determinar la razón de que no funcione para este elemento.

EJERCICIO 1.4: Determina el polinomio $Irr(\alpha, \mathbb{F}_{27})$. Para el elemento σ que encontraste al inicio calcula $Irr(\sigma, \mathbb{F}_9)$ y $Irr(\sigma, \mathbb{F}_{27})$

Primero hacemos algunos comentarios al método del guión de prácticas. α es raíz de un polinomio mónico irreducible de grado 3 sobre $\mathbb{F}_3(\delta)$ ya que el grado de la extensión $\frac{\mathbb{F}_{3^6}}{\mathbb{F}_{3^2}}$ es 3. El resto de cálculos tiene sentido porque los elementos de $\mathbb{F}_3(\delta)$ son las imágenes de clases de $\frac{\mathbb{F}_3[X]}{<X^2+X+2>}$ por la evaluación en δ esto es polinomios $a\delta + b$ con $a, b \in \mathbb{F}_3$.

Cálculo de $Irr(\alpha, \mathbb{F}_{27})$. Del mismo modo expresamos $\mathbb{F}_{27} = \mathbb{F}_3(\epsilon)$ con ϵ una raíz del polinomio X^3+2X+1. Se obtienen tres posibles valores para ϵ:

$$\alpha^2 + 2\alpha^3 + \alpha^4$$

$$1 + \alpha^2 + 2\alpha^3 + \alpha^4$$

$$2 + \alpha^2 + 2\alpha^3 + \alpha^4$$

Observamos que los elementos de $\mathbb{F}_3(\epsilon)$ son polinomios de grado dos evaluados en ϵ y como estamos buscando $Irr(\alpha, \mathbb{F}_{27})$ el sistema a resolver tendrá la forma:

$$(b00 + b01 * \epsilon + b02 * \epsilon^2) + (b10 + b11 * \epsilon + b12 * \epsilon^2)X + X^2$$

Realizando las sustituciones correspondientes a esta observación se obtiene el polinomio

$$2\epsilon + 2\epsilon^2 + X(1 + \epsilon) + X^2$$

Cálculo de $Irr(\sigma, \mathbb{F}_9)$. Repitiendo el proceso que aparece en el guión, cambiando el valor de PF a $X^6 + 2X^3 + X^2 + X + 2$ nos va a aparecer un irreducible de la forma:

$$2 + 2\delta + X(2 + \delta) + X^3$$

Cálculo de $Irr(\sigma, \mathbb{F}_{27})$. Tenemos que combinar las modificaciones de los apartados anteriores respecto al valor de PF y respecto al sistema de ecuaciones a resolver. Obtenemos el polinomio:

$$2 + 2\epsilon + 2\epsilon^2 + X(2 + \epsilon) + X^2$$

Ejercicio 1.5: Determinar el número de polinomios irreducibles de grado 30 sobre $\mathbb{F}_3$ y cuántos de ellos tienen raíces que son generadores del grupo multiplicativo de $\mathbb{F}_{3^{30}}$.

Vamos a clarificar el razonamiento empleado en el texto del ejercicio.

Proposición 1.1.
Cada seis raíces de $\mathbb{F}_{3^6} - \mathbb{F}_{3^2} - \mathbb{F}_{3^3}$ me están determinando polinomios irreducibles de grado 6 en $\mathbb{F}_3[X]$. Por tanto, hay 116 polinomios irreducibles de grado 6 sobre $\mathbb{F}_3$.

Demostración. Nosotros hemos visto que los factores irreducibles de $X^{6^n} - X$ en $\mathbb{F}_3[X]$ son exactamente los polinomios irreducibles de $\mathbb{F}_3[X]$ con grado divisor de 6.

Por otro lado, $\mathbb{F}_{3^6}$ es el cuerpo de descomposición del polinomio $X^{6^n} - X$ y por tanto, el cuerpo que contiene a todas sus raíces.

Entonces los polinomios irreducibles de $\mathbb{F}_3[X]$ con grado divisor de 6 tienen también sus raíces en $\mathbb{F}_{3^6}$.

Una observado lo anterior, cada seis raíces de $\mathbb{F}_{3^6} - \mathbb{F}_{3^2} - \mathbb{F}_{3^3}$ me están determinando polinomios irreducibles de grado 6 en $\mathbb{F}_3[X]$. □

Proposición 1.2.
Hay 248 generadores de $\mathbb{F}_{729}^x$. Además, si una raíz de un polinomio irreducible es generadora (no es generadora) entonces también el resto de las raíces son generadoras (no son generadoras). Como consecuencia de los 116 polinomios irreducibles de grado 6 hay 48 cuyas raíces son generadoras y 68 cuyas raíces no son generadoras.

Demostración. La proposición sobre las propiedades del orden de un elemento de mis apuntes sobre teoría de grupos muestra que un grupo cíclico tiene $\phi(ord(a))$ generadores donde a es un generador del grupo. Entonces, como $\mathbb{F}_{729}^x$ tiene 728 elementos, basta calcular $\phi(728) = \phi(8)\phi(7)\phi(13) = 248$.

Por otra parte, como todo polinomio de grado 6 irreducible sobre $\mathbb{F}_3[X]$ con una raíz α admite 6 raíces distintas α^{3^i} con $i = 0, \cdots, 5$, entonces si una raíz α es generadora esto quiere decir que $ord(\alpha) = 728$ y entonces $ord(\alpha^{3^i}) = \frac{728}{mcd(728,3^i)} = 728$ y por tanto siguen siendo generadoras. Si α no fuera generadora entonces el resto no pueden ser generadoras, ya que si alguna lo fuera entonces también lo sería α.

Agrupando las generadoras en grupos de 6 se obtienen 48 polinomios cuyas raíces son generadoras y agrupando los 68 polinomios restantes, se obtienen polinomios cuyas raíces no son generadoras. □

Veamos ahora el ejercicio.

En vez de calcular el número explícitamente utilizaremos la fórmula de Gauss para el número de polinomios mónicos irreducibles sobre $\mathbb{F}_p[X]$ de grado n (una prueba de este hecho basada en teoría de básica de cuerpos finitos y el principio de exclusión-inclusión aparece en nuestros apuntes):

$|N_n| = \frac{1}{n}\sum_{m|n}\mu(m)p^{\frac{n}{m}}$

donde μ es la función de Mobius:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^s & n = \prod_{i=1}^{s} p_i \text{ para primos distinos } p_i \\ 0 & \text{en otro caso} \end{cases}$$

Entonces

$$|N_{30}| = \frac{1}{30}(\mu(1)p^{30} + \mu(2)p^{15} + \mu(3)p^{10} + \mu(5)p^6 + \mu(6)p^5 + \mu(10)p^3 + \mu(15)p^2 + \mu(30)p)$$

$$|N_{30}| = \frac{1}{30}(p^{30} - p^{15} - p^{10} - p^6 + p^5 + p^3 + p^2 - p)$$

$$|N_{30}| = 6863037256208$$

Por otro lado hay $\phi(3^{30} - 1) = 70207948800000$ generadores de $\mathbb{F}_{30}$ el mismo argumento que hemos hecho para el caso del documento de la práctica sirve aquí y entonces basta dividir por 30 para obtener el número de polinomios irreducibles de grado 30 cuyas raíces son generadoras. Este número es 2340264960000. El resto, 67867683840000 no son generadoras.