Problemas de Teoría de Cuerpos

Rodrigo Raya Castellano
Universidad de Granada

Índice

1. Problema 1

Lema 1.1.
Dada cualquier extensión de cuerpos $\frac{F}{K}$, el conjunto

$$M = \{\alpha \in F : \alpha \text{ es algebraico sobre } K\}$$

es un subcuerpo de F que contiene a K. Además la extensión $\frac{M}{K}$ es algebraica.

Demostración. Veamos que M es cerrado para sumas y productos. En efecto, si $\alpha, \beta \in M$ entonces $\frac{K(\alpha,\beta)}{K}$ es una extensión finita ya que es de generación finita por generadores algebraicos. Como es una extensión finita, tiene que ser algebraica.

Entonces todo elemento de $K(\alpha, \beta)$ es algebraico sobre K y claramente $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$, luego son algebraicos sobre K.

Por otro lado, es claro que $K \subseteq M$ ya que si $\alpha \in K$ entonces ciertamente, α es raíz del polinomio $X - \alpha$. En particular, $1, -1 \in M$ y por tanto, se tiene que M es un subanillo. Nos falta comprobar que también es cerrado para inversos de los elementos no nulos.

Sea $\alpha \neq 0$ algebraico, entonces α es raíz de algún polinomio con coeficientes en K. Sea este $p = \sum_{i=0}^{n} a_i X^i$ entonces es claro que $\sum_{i=0}^{n} a_{n-i} X^i$, si evaluamos en $\frac{1}{\alpha}$ y multiplicamos por α^n es claro que $\frac{1}{\alpha}$ es raíz de este polinomio. En resumen $\frac{1}{\alpha} \in M$.

Por tanto, M es un cuerpo que contiene a K. Claramente, la extensión $\frac{M}{K}$ es algebraica ya que todos los elementos de α son raíces de algún polinomio con coeficientes en K. □

Lema 1.2.
Sea $\frac{F}{K}$ una extensión de cuerpos, $p \in K[x]$ y $z \in F$ tal que $p(z) = 0$. Si $\sigma : F \to F$ es un endomorfismo de anillos tal que $\sigma|_K = Id|_K$ entonces $\sigma(z)$ es raíz de p.

Demostración. Sea $p(X) = \sum a_i X^i$ entonces $p(\sigma(z)) = \sum a_i \sigma(z)^i$ y ya que σ fija los elementos de K lo anterior es igual a $\sigma(p(z))$ como $p(z) = 0$ por hipótesis, se tiene que $p(\sigma(z)) = 0$. □

Ejercicio 1.1: Se considera F_1 (resp. F_2) el subcuerpo de $\mathbb{R}$ (resp. $\mathbb{C}$) de todos los elementos algebraicos sobre $\mathbb{Q}$. Probar que $\frac{F_i}{\mathbb{Q}}$ es una extensión algebraica y que $[F_2 : F_1] = 2$.

Demostración. Basta tomar $F = \mathbb{R}, \mathbb{C}$ y $K = \mathbb{Q}$ en el lema 1.1

Por otro lado, se tiene la siguiente cadena de cuerpos $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \mathbb{C}$. Vamos a ver que de hecho $F_2 = F_1[i] \cong \frac{F_1[X]}{<X^2+1>}$ de donde la dimensión es claramente dos, esto es, $[F_2 : F_1] = 2$.

$F_1[i] \subseteq) F_2$ Claramente, $1, i \in F_2$ ya que son números complejos y son raíces de los polinomios $X - 1, X^2 - 1 \in \mathbb{Q}[X]$. También se verifica que $F_1 \subseteq F_2$. Como F_2 es un cuerpo, cualquier combinación lineal de sus elementos $\alpha + \beta i$ con $\alpha, \beta \in F_1$ está en F_2. Esto completa la inclusión.

$F_2 \subseteq F_1[i])$ Sea $\alpha + \beta i \in F_2$ raíces de cierto polinomio $p \in \mathbb{Q}[X]$ y queremos ver que $\alpha, \beta \in F_1$. Por el lema 1.2, ya que $\sigma(\alpha + i\beta) = \alpha - i\beta$ es un endomorfismo por cálculo directo, se tiene que la raíz conjugada $\alpha - i\beta$ también es raíz de $p \in \mathbb{Q}[X]$. En consecuencia como claramente $\frac{1}{2}, \frac{1}{2i} \in F_2$ y F_2 es cuerpo y como $\alpha = \frac{\alpha+i\beta}{2} + \frac{\alpha-i\beta}{2} \wedge \beta = \frac{\alpha+i\beta}{2i} - \frac{\alpha-i\beta}{2i}$ se tiene que $\alpha, \beta \in F_2$ y como $\alpha, \beta \in \mathbb{R}$ se verifica claramente que $\alpha, \beta \in F_1$, como se quería. □

Ejercicio 1.2: Calcular:

- $Irr(\sqrt{2}, \mathbb{F}_3)$
- $Irr(\sqrt[4]{2}, \mathbb{F}_3)$
- $Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{F}_3)$
- $Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{Q})$

Para determinar los valores α que corresponden a cada una de las expresiones ambiguas $\sqrt[n]{}$ nos vamos a ir a un cuerpo extensión. Uno natural es $\mathbb{F}_9 \cong \frac{\mathbb{F}_3[X]}{<x^2+2x+2>} \cong \mathbb{F}_3[\sqrt{2}]$.

1. Por definición si $\alpha = \sqrt{2}$ entonces $\alpha^2 - 2 = 0$ y por tanto, α será un número algebraico sobre $\mathbb{F}_3$ que anula al polinomio $p(X) = X^2 - 2$. Este polinomio es irreducible y mónico sobre $\mathbb{F}_3$ ya que no tiene raíces en $\mathbb{F}_3$. Como α es una raíz suya deducimos que $Irr(\alpha, \mathbb{F}_3) = X^2 - 2$.

Obsérvese que en el cuerpo extensión estas raíces son $\alpha = \sqrt{2}, -\sqrt{2}$.

2.Por definición si $\alpha = \sqrt[4]{2}$ entonces $\alpha^4 - 2 = 0$ y por tanto, α será un número algebraico sobre $\mathbb{F}_3$ que anula al polinomio $p(X) = X^4 - 2$. Este polinomio no es irreducible sobre F_3. Veámoslo.

Como p no tiene raíces sobre $\mathbb{F}_3$, no tiene factores de grado 1 ni de grado 3. Luego sólo puede tener factores de grado 2. Los irreducibles de grado 2 en $\mathbb{F}_3[X]$ son $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$ y realizando la división euclídea se tiene que $p(X) = (X^2 + X + 2)(X^2 + 2X + 2)$. Por ser α una raíz del polinomio p será una raíz del polinomio $X^2 + X + 2$ o $X^2 + 2X + 2$ que como son mónicos e irreducibles son candidatos a ser $Irr(\alpha, \mathbb{F}_3)$.

Las raíces $\alpha = 2 + \sqrt{2}, 2 - \sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + 2X + 2$ y las raíces $\alpha = 1 + 2\sqrt{2}, 1 - 2\sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + X + 2$.

3. Primero obtenemos un polinomio que se anule en α mediante cálculo directo:

$$\alpha = \sqrt{2} + \sqrt[4]{2}$$

$$(\alpha - \sqrt{2})^2 = \sqrt{2}$$

$$(\alpha^2 + 2)^2 = ((2\alpha + 1)\sqrt{2})^2$$

$$\alpha^4 - 4\alpha^2 - 8\alpha + 2 = 0$$

$$\alpha^4 - \alpha^2 + \alpha + 2 = 0$$

$$(\alpha - 1)^2(\alpha^2 + 2\alpha^2 + 2)$$

La raíz $\alpha = 1$ tiene $Irr(\alpha, \mathbb{F}_3) = X - 1$ y las raíces $\alpha = 2 + \sqrt{2}, 2 + 2\sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + 2X + 2$.

Nos damos cuenta que esto no puede contener a todas los sumandos de las raíces halladas en los apartados 1 y 2. La razón es que en el primer paso hemos asumido implícitamente que $\sqrt{2} = (\sqrt[4]{2})^2$. Pero también podríamos elegir $\sqrt{2} = -(\sqrt[4]{2})^2$. Los cálculos en este caso son los siguientes:

$$\alpha = \sqrt{2} + \sqrt[4]{2}$$

$$(\alpha - \sqrt{2})^2 = -\sqrt{2}$$

$$(\alpha^2 + 2)^2 = ((2\alpha - 1)\sqrt{2})^2$$

$$\alpha^4 - 4\alpha^2 + 8\alpha + 2 = 0$$
$$\alpha^4 - \alpha^2 - \alpha + 2 = 0$$
$$(\alpha - 2)^2(\alpha^2 + \alpha + 2)$$

Por tanto, si $\alpha = 2$ obtengo que $Irr(\alpha, \mathbb{F}_3) = X - 2$ y si $\alpha = 1 + \sqrt{2}, 1 - \sqrt{2}$ tienen $Irr(\alpha, \mathbb{F}_3) = X^2 + X + 2$.

4. Repitiendo el proceso anterior, llegamos al polinomio

$$\alpha^4 - 4\alpha^2 - 8\alpha + 2 = 0$$

Esto nos da como candidato a polinomio mínimo $p(X) = X^4 - 4X^2 - 8X + 2$.

Sabemos que estudiar la irreducibilidad de un polinomio primitivo en $\mathbb{Z}$ es equivalente a estudiarla en $\mathbb{Q}$. Entonces en nuestro caso basta aplicar el criterio de Eisenstein con un primo $p = 2$ para obtener que es irreducible.

Dado que p es irreducible, mónico y α debe ser raíz de p deducimos que

$$Irr(\sqrt{2} + \sqrt[4]{2}, \mathbb{Q}) = X^4 - 4X^2 - 8X + 2$$

2. Problema2

EJERCICIO 2.1: 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.

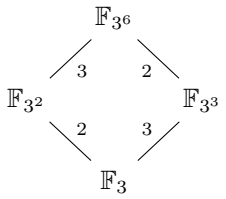
Los factores irreducibles del polinomio $X^{3^6} - X$ son los irreducibles sobre F_3 de grado divisor de 6. En Mathematica esta lista se puede obtener mediante el comando

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

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 2.2: 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 2.3: Analiza qué ocurre al considerar el elemento σ para encontrar elementos que generen las extensiones $\mathbb{F}_{3^2}$ y $\mathbb{F}_{3^3}$.

EJERCICIO 2.4: 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 2.5: 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 2.1.
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 2.2.
Hay 248 generadores de $\mathbb{F}_{729}^x$. Además, si una raíz de un polinomio 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.

Proposición 2.3.
1. Cada treinta raíces de $\mathbb{F}_{3^{30}}-$