

1. Sea K un cuerpo y sean $a \in K$ y $n \geq 2$. Demostrar que $X^n - a$ tiene no tiene raíces múltiples en ninguna extensión de K si y sólo si $na \neq 0$.

Pongamos $f = X^n - a$. Supongamos primero que $na \neq 0$. Entonces $n \neq 0$ y por tanto la única raíz de $f' = nX^{n-1}$ es 0. Además $a \neq 0$ y por tanto 0 no es raíz de f . En conclusión, f y f' no tiene ninguna raíz común en ninguna extensión de K y por tanto f no tiene ninguna raíz múltiple en ninguna extensión de K .

Supongamos ahora que $na = 0$. Eso implica que o bien $a = 0$ o bien n es múltiplo de la característica de K . En el primer caso $f = X^n$, y 0 es una raíz múltiple de f . En el segundo caso $f' = nX^{n-1} = 0$ y por tanto, cualquier raíz de f , es una raíz múltiple.

2. Sea Q el subgrupo de $GL_2(\mathbb{C})$ generado por las dos siguientes matrices:

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Calcular el número de elementos de Q , escribir todos los elementos de G como productos de potencias de a y de b , calcular el orden de cada uno de los elementos y calcular la serie derivada de G .

Vamos a denotar con I la matriz identidad. Como $a^2 = b^2 = -I$, a y b tienen orden 4 y el grupo tiene al menos los siguientes ocho elementos: $I, a, a^2 = b^2 = -I, a^3, b, ab, a^2b, a^3b$. Observamos ahora que

$$ba = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -a \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = a^3b = a^{-1}b.$$

Utilizando esto es fácil ver que $Q = \{1, a, a^2 = b^2 = -I, a^3, b, ab, a^2b, a^3b\}$. La siguiente tabla muestra los órdenes de cada elemento:

elemento	1	a	a^2	a^3	b	ab	a^2b	a^3b
orden	1	4	2	4	4	4	4	4

Como a y b tienen orden 4, entonces $\langle a \rangle$ y $\langle b \rangle$ tienen índice 2 en Q y por tanto son subgrupos normales de Q , con lo que también $\langle a \rangle \cap \langle b \rangle = \langle a^2 \rangle$ es normal en Q . Como $Q/\langle a^2 \rangle$ tiene cuatro elementos, es abeliano y por tanto, $Q' \subseteq \langle a^2 \rangle$. Eso implica que Q' es igual a 1 ó $\langle a^2 \rangle$. Como Q no es abeliano, el primer caso no se da y concluimos que $Q' = \langle a^2 \rangle$.

3. Calcular el número de subcuerpos de $\mathbb{Q}(\xi_8)$ y de $\mathbb{Q}(\xi_{11})$.

Para cada número natural n tenemos un isomorfismo

$$\sigma : \mathbb{Z}_n^* \rightarrow \text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \\ r \mapsto \sigma_r$$

donde σ_r está determinado por $\sigma_r(\xi_n) = \xi_n^r$. En particular $\text{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q}) \simeq \mathbb{Z}_8^*$ y $\text{Gal}(\mathbb{Q}(\xi_{27})/\mathbb{Q}) \simeq \mathbb{Z}_{27}^*$.

Obsérvese que todos los elementos diferentes de 1 de $\mathbb{Z}_8^* = \{1, 3, -3, -1\}$ tienen orden 2 pues $3^2 = (-3)^2 = 9 \equiv (-1)^2 = 1 \pmod{8}$. Por tanto \mathbb{Z}_8^* tiene cinco subgrupos, a saber 1, $\langle 3 \rangle$, $\langle -3 \rangle$, $\langle -1 \rangle$ y \mathbb{Z}_8^* . Luego $\text{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q})$ tiene 5 subgrupos y, por el Teorema Fundamental de la Teoría de Galois, $\mathbb{Q}(\xi_8)$ tiene 5 subcuerpos.

Por otro lado \mathbb{Z}_{11}^* tiene orden $\phi(11) = 10$ y es cíclico pues es el grupo de unidades de un cuerpo finito. Como 10 tiene cuatro divisores (1, 2, 5 y 10), \mathbb{Z}_{11}^* tiene cuatro subgrupos y por tanto también $\text{Gal}(\mathbb{Q}(\xi_{11})/\mathbb{Q})$ tiene 4 subgrupos. Concluimos que $\mathbb{Q}(\xi_{11})$ tiene 4 subcuerpos.

4. Encontrar un polinomio irreducible p de grado 3 con coeficientes en \mathbb{Z}_2 y utilizarlo para construir un cuerpo con 8 elementos. Encontrar un generador del grupo de las unidades de dicho cuerpo.

El polinomio $p = X^3 + X + 1$ es irreducible sobre \mathbb{Z}_2 , con lo que $F = K[X]/(p)$ es un cuerpo de orden 8. Como F^* tiene orden 7, cualquier elemento diferente de 1 es un generador de F^* . Por ejemplo $\alpha = X + (p)$ serviría de generador.

5. Sea L/K una extensión de Galois finita y sea H un subgrupo de $\text{Gal}(L/K)$. Para cada $\alpha \in L$ ponemos $\text{tr}_H(\alpha) = \sum_{h \in H} h(\alpha)$ y $N_H(\alpha) = \prod_{h \in H} h(\alpha)$. Demostrar que se verifican las siguientes condiciones para todo $\alpha, \beta \in L$:

(a) $\text{tr}_H(\alpha)$ y $N_H(\alpha)$ pertenecen a $F^H = \{x \in L : h(x) = x, \text{ para todo } h \in H\}$.

(b) $\text{tr}_H(\alpha + \beta) = \text{tr}_H(\alpha) + \text{tr}_H(\beta)$ y $N_H(\alpha\beta) = N_H(\alpha)N_H(\beta)$.

(c) **Supongamos ahora que $L = \mathbb{Q}(\xi_5)$ y $K = \mathbb{Q}$ y $H = \langle \sigma \rangle$, donde σ es el automorfismo de L dado por $\sigma(\xi_5) = \xi_5^{-1}$. Encontrar un elemento de L^H que no pertenezca a \mathbb{Q} .**

(a) Obsérvese que para cada $x \in H$ la aplicación $h \mapsto xh$ es una biyección de H en si mismo. Por tanto $x(\text{tr}_H(\alpha)) = x(\sum_{h \in H} h(\alpha)) = \sum_{h \in H} xh(\alpha) = \sum_{h \in H} h(\alpha) = \text{tr}_H(\alpha)$. Análogamente $x(N_H(\alpha)) = x(\prod_{h \in H} h(\alpha)) = \prod_{h \in H} xh(\alpha) = \prod_{h \in H} h(\alpha) = N_H(\alpha)$.

(b) $\text{tr}_H(\alpha + \beta) = \sum_{h \in H} h(\alpha + \beta) = \sum_{h \in H} h(\alpha) + h(\beta) = \sum_{h \in H} h(\alpha) + \sum_{h \in H} h(\beta) = \text{tr}_H(\alpha) + \text{tr}_H(\beta)$.

$N_H(\alpha\beta) = \prod_{h \in H} h(\alpha\beta) = \prod_{h \in H} h(\alpha)h(\beta) = (\prod_{h \in H} h(\alpha)) (\prod_{h \in H} h(\beta)) = N_H(\alpha) + N_H(\beta)$.

(c) Obsérvese que $\sigma^2 = 1$, con lo que H tiene orden 2. Entonces $\alpha = \text{tr}(\xi_5) = \xi_5 + \xi_5^{-1}$ pertenece a L^H , por el apartado (a). Para ver que $\alpha \notin \mathbb{Q}$ observamos que $\xi_5^{-1} = \xi_5^4 = -1 - \xi_5 - \xi_5^2 - \xi_5^3$ y por tanto $\alpha = -1 - \xi_5^2 - \xi_5^3$ que no pertenece a \mathbb{Q} pues $\{1, \xi_5, \xi_5^2, \xi_5^3\}$ es una base de L sobre \mathbb{Q} .

6. **Sea $f = X^5 - aX^4 + 1$ un polinomio irreducible sobre \mathbb{Q} con a un número racional mayor que $5/\sqrt[5]{4^4}$. Demostrar que f no es resoluble por radicales sobre \mathbb{Q} .**

$f' = 5X^4 - 4aX^3 = X^3(5X - 4a)$ y por tanto las raíces de f' son 0 y $4a/5$. Además $f(0) = 1$ y

$$f\left(\frac{4a}{5}\right) = \left(\frac{4a}{5}\right)^4 \left(\frac{4a}{5} - a\right) + 1 = -a^5 \frac{4^4}{5^5} + 1 < 1 - \left(\frac{5}{\sqrt[5]{4^4}}\right)^5 \frac{4^4}{5^5} = 0.$$

Esto muestra que f tiene un máximo relativo en 0 y un mínimo relativo en $\frac{4a}{5}$ y que los valores de f en estos extremos relativos es positivo y negativo respectivamente. Por tanto, f tiene tres raíces reales y dos complejas no reales. Eso implica que, si consideramos $\text{Gal}(f/\mathbb{Q})$ como un grupo de permutaciones de las raíces de f , entonces este grupo tiene una transposición y, como es un grupo transitivo, se tiene que $\text{Gal}(f/\mathbb{Q}) = S_5$, que no es resoluble. Aplicando el Teorema de Galois, f no es resoluble por radicales sobre \mathbb{Q} .

7. **Sean α y β dos números complejos tales que $\alpha^2 = 1 + i$ y $\beta^2 = 1 - i$.**

(a) **Calcular $\text{Irr}(\alpha, \mathbb{Q})$ y $\text{Irr}(\beta, \mathbb{Q})$ y demostrar que existe un isomorfismo $f : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\beta)$ tal que $f(\alpha) = \beta$.**

(b) **Demostrar que $\alpha\beta = \pm\sqrt{2} \notin \mathbb{Q}(i)$ y utilizarlo para demostrar que $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$. (Indicación: Recuerda un ejercicio que caracteriza cuándo $K(\sqrt{a}) = K(\sqrt{b})$, para $a, b \in K$.)**

(c) **Demostrar que $K = \mathbb{Q}(\alpha, \beta)$ es una extensión normal de \mathbb{Q} y calcular $[K : \mathbb{Q}]$.**

(a) $i = \alpha^2 - 1 = 1 - \beta^2$ y por tanto $-1 = (\alpha^2 - 1)^2 = (1 - \beta^2)^2 = \alpha^4 - 2\alpha^2 + 1 = \beta^4 - 2\beta + 1$. Luego α y β son raíces de $p = X^4 - 2X^2 + 2$. Como este polinomio es irreducible sobre \mathbb{Q} (Eisenstein), deducimos que $p = \text{Irr}(\alpha, \mathbb{Q}) = \text{Irr}(\beta, \mathbb{Q})$. La existencia del isomorfismo es consecuencia de que α y β son raíces del mismo polinomio irreducible sobre \mathbb{Q} .

(b) $(\alpha\beta)^2 = \alpha^2\beta^2 = (1+i)(1-i) = 2$, lo que prueba que $\alpha\beta = \pm\sqrt{2}$. Como $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ y $\mathbb{Q}(i) \not\subseteq \mathbb{R}$, tenemos $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(i)$ y por tanto $\sqrt{2} \notin \mathbb{Q}(i)$. Obsérvese que $\mathbb{Q}(\alpha) \supset F = \mathbb{Q}(i) \subset \mathbb{Q}(\beta)$ y las dos extensiones $\mathbb{Q}(\alpha)/F$ y $\mathbb{Q}(\beta)/F$ tienen grado 2. De hecho $\mathbb{Q}(\alpha) = F(\sqrt{1+i})$ y $\mathbb{Q}(\beta) = F(\sqrt{1-i})$. Por un ejercicio que hicimos en clase, $F(\sqrt{1+i}) = F(\sqrt{1-i})$ si y sólo si $2 = (1+i)(1-i)$ es un cuadrado en F . Como hemos visto que $\sqrt{2} \notin F = \mathbb{Q}(i)$, se tiene que 2 no es un cuadrado en F y por tanto $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.

(c) Las raíces de $p = \text{Irr}(\alpha, \mathbb{Q}) = \text{Irr}(\beta, \mathbb{Q})$ son $\alpha, -\alpha, \beta$ y $-\beta$. Luego K es el cuerpo de descomposición de p sobre \mathbb{Q} y por tanto K/\mathbb{Q} es una extensión normal. En el apartado (b) hemos visto que $\alpha\beta = \sqrt{2}$, lo que implica que $K = \mathbb{Q}(\alpha, \sqrt{2})$ y tenemos $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \text{gr}(p) = 4$ y $[K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\sqrt{2}) : \mathbb{Q}(\alpha)] \leq 2$. También hemos visto que $K(\alpha) \neq K(\beta)$, con lo que $K \neq \mathbb{Q}(\alpha)$. Por tanto $[K : \mathbb{Q}(\alpha)] = 2$ y deducimos que $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.