ÁLGEBRA 3
Segundo cuatrimestre — 2014

Recuperatorio del segundo parcial

APELLIDO Y NOMBRE: .....

L.U.: ..... HOJAS: .....

---

1. Sea $a \in \mathbb{Q}$ un número racional positivo, sea $E = \mathbb{Q}(\sqrt[n]{a})$ y supongamos que $[E : \mathbb{Q}] = n$. Si $K \subseteq E$ es un subcuerpo tal que $[K : \mathbb{Q}] = d$, muestre que $K = \mathbb{Q}(\sqrt[d]{a})$.

Sugerencia. Considere la norma $N_{E/K}(\sqrt[n]{a})$.

Solución. Sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad y escribamos $\alpha = \sqrt[n]{a}$. Sabemos que todo morfismo $E \to \mathbb{C}$ manda α a $\zeta^i a$ para algún $i \in \{0, \dots, n-1\}$ y, como K es perfecto, que hay $[E : K] = n/d$ morfismos $E \to \mathbb{C}$ que extienden la inclusión $K \to \mathbb{C}$. Esto nos dice que hay $i_1, \dots, i_{n/d} \in \{0, \dots, n-1\}$ tales que

$$N_{E/K}(\alpha) = \prod_{j=1}^{n/d} (\zeta^{i_j} \alpha) = \zeta^{\sum_{j=1}^{n/d} i_j} \alpha^{n/d}.$$

Esta norma es un elemento de $K \subseteq \mathbb{R}$, así que el factor $\zeta^{\sum_{j=1}^{n/d} i_j}$ tiene que ser real, porque $\alpha^{n/d}$ lo es: esto nos dice que $N_{E/K}(\alpha) = \pm\alpha^{n/d}$. Vemos así que $\sqrt[d]{a} \in K$ y, entonces, $\mathbb{Q}(\sqrt[d]{a}) \subseteq K$.

Como $[E : \mathbb{Q}] = n$, el polinomio $X^n - a$ es irreducible en $\mathbb{Q}[X]$. Como d divide a n, esto implica que el polinomio $X^d - a$ también es irreducible en ese anillo, y entonces $[\mathbb{Q}(\sqrt[d]{a}) : \mathbb{Q}] = d$. Vemos así que $K = \mathbb{Q}(\sqrt[d]{a})$, como queríamos. □

2. El grupo de Galois de un polinomio $f \in \mathbb{Q}[X]$ irreducible y cúbico con exactamente una raíz real es isomorfo a S_3.

Solución. Sea E el cuerpo de descomposición de f. Por hipótesis, $E \not\subseteq \mathbb{R}$, así que la conjugación compleja es un elemento de orden dos de $G = \mathsf{Gal}(E/\mathbb{Q})$. Como G es isomorfo a un subgrupo transitivo de S_3 y contiene un elemento de orden dos, necesariamente debe ser isomorfo a S_3 mismo. □

Otra solución. Por hipótesis, sabemos que existe $x, a, b \in \mathbb{R}$ tales que x, $a + ib$ y $a - ib$ son las tres raíces de f y $b \neq 0$. El discriminante de f es, entonces,

$$\begin{aligned} D(f) &= (x - (a + ib))^2 (x - (a - ib))^2 ((a + ib) - (a - ib))^2 \\ &= -4b^2 (x^2 - 2ax + a^2 + b^2)^2 \end{aligned}$$

que, como es negativo, no es un cuadrado en $\mathbb{Q}$. Sabemos que esto implica que el grupo de Galois del polinomio no está contenido en A_3 y, entonces, que es S_3. □

3. Sean n, $m \in \mathbb{N}$ y sea $\zeta = \exp(2\pi i/n) \in \mathbb{C}$. El polinomio $X^m - \zeta$ es irreducible en $\mathbb{Q}(\zeta)$ si y solamente si todo primo que divide a m divide a n.

Solución. El número $\xi = \exp(2\pi i/nm)$ es una raíz del polinomio, así que tenemos que mostrar que $[\mathbb{Q}(\xi) : \mathbb{Q}(\zeta)] = m$ sii vale la condición del enunciado. Como $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(nm)$ y $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$], es $[\mathbb{Q}(\xi) : \mathbb{Q}(\zeta)] = m \iff \phi(nm) = m\phi(n)$. En consecuencia, tenemos que mostrar que

$$\phi(nm) = \phi(n)m \iff \text{todo primo que divide a } m \text{ divide a } n.$$

($\Leftarrow$) Si $m = p_1^{a_1} \cdots p_r^{a_r}$ con $a_i > 0$ para cada i y $p_1, \ldots, p_r$ primos distintos, la hipótesis implica que $n = p_1^{b_1} \cdots p_r^{b_r} n'$ con $b_i > 0$ y $(n', m) = 1$. Entonces

$$\phi(nm) = \phi(p_1^{a_1+b_1} \cdots p_r^{a_r+b_r})\phi(n') = \prod_i p^{a_i+b_i-1}(p_i - 1)\phi(n')$$

y $\phi(n)m = \prod_i p_i^{a_i-1}(p_i - 1)\phi(n')m$ y estas dos cosas son iguales.

($\Rightarrow$) Supongamos que $m = m_1 m_2$ con $(n, m_2) = (m_1, m_2) = 1$ y que todo primo que divide a m_1 divide a n; por lo que ya probamos, es $\phi(nm_1) = \phi(n)m_1$. Por otro lado, $\phi(nm) = \phi(nm_1m_2) = \phi(nm_1)\phi(m_2)$ y $\phi(n)m = \phi(n)m_1m_2$, y la hipótesis implica que estas dos cosas son iguales, de manera que $m_2 = \phi(m_2)$, esto es, $m_2 = 1$. Esto prueba que todo primo que divide a m divide a n. □

4. Sea q una potencia de un número primo y $n \in \mathbb{N}$. El polinomio $\bar{\Phi}_n$ es irreducible en $\mathbb{F}_q[X]$ sii el orden de q en $\mathbb{Z}_n^\times$ es $\phi(n)$.

5. Sea E un subcuerpo de $\mathbb{C}$ tal que la extensión $E/\mathbb{Q}$ es finita y galoisiana de grupo de Galois abeliano. Si $\alpha \in E$ y p es un primo impar tal que $\alpha^p \in \mathbb{Q}$ y $\alpha \notin \mathbb{Q}$, entonces $\mathbb{Q}(\alpha) = \mathbb{Q}(\exp(2\pi i/p))$ y existe $b \in \mathbb{Q}^\times$ tal que α/b es una raíz p-ésima de la unidad.

6. Sea E/K una extensión de cuerpos y $f \in K[X]$ un polinomio irreducible tal que existe $a \in E$ con $f(a) = f(a^2) = 0$. Muestre que f se factoriza como producto de polinomios de grado 1 en $E[X]$.