ÁLGEBRA 3
Segundo cuatrimestre — 2014

Recuperatorio del primer parcial

APELLIDO Y NOMBRE: .....

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

---

1. Sea $K = \mathbb{F}_7(X)$ con X trascendente sobre $\mathbb{F}_7$, sea $\sigma : K \to K$ el automorfimo de cuerpos tal que $\sigma(X) = 2X + 1$ y sea $G = (\sigma) \subseteq \mathrm{Aut}(K)$ el grupo de automorfismos generado por σ. Encuentre $f \in K$ tal que $K^G = \mathbb{F}_7(f)$.

Solución. Como

$$X \overset{\sigma}{\longmapsto} 2X + 1 \overset{\sigma}{\longmapsto} 4X + 3 \overset{\sigma}{\longmapsto} X,$$

el automorfismo σ tiene orden 3. El grupo $G = (\sigma)$ es entonces cíclico de orden 3 y el teorema de Artin nos dice, en consecuencia, que $[K : K^G] = |G| = 3$. El polinomio

$$f = X\sigma(X)\sigma^2(X) = X(2X + 1)(4X + 3) \in K$$

es evidentemente invariante por σ, de manera que $f \in K^G$. Como f tiene grado 3, sabemos de un ejercicio de la práctica que $[K : \mathbb{F}_7(f)] = 3$. Como $\mathbb{F}_7(f) \subseteq K^G \subseteq K$, y las extensiones K/K^G y $K/\mathbb{F}_7(f)$ tienen el mismo grado, vemos que $K^G = \mathbb{F}_7(f)$. □

2. Sea E/K una extensión galoisiana de un cuerpo K de característica distinta de 2 con $\mathrm{Gal}(E/K) \cong \mathbb{Z}/4\mathbb{Z}$. Muestre que existen $a, b \in K$ con $a \neq 0$, $b \notin K^2$ tales que E es el cuerpo de descomposición de $(X^2 - a)^2 - b$ sobre K.

Solución. Sea σ un generador de $\mathrm{Gal}(E/K)$, que tiene entonces orden 4. Sea $F = E^{\sigma^2)}$; del teorema de Galois sabemos que E/K y F/K son extensiones cuadráticas, y que sus grupos de Galois están generados por σ^2 y por σ, respectivamente. Como la característica de K no es dos, sabemos que existen $\beta \in F$ tal que $\beta^2 \in K \setminus K^2$ y $F = K(\beta)$, y $\alpha \in E$ tal que $\alpha^2 \in F \setminus F^2$ y $E = F(\alpha)$. La descripción de los grupos de Galois de las extensiones E/F y F/K implican que $\sigma^2(\alpha) = -\alpha$ y $\sigma(\beta) = -\beta$.

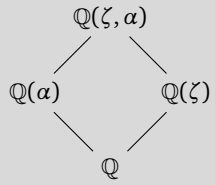
Como $\alpha^2 \in F = K(\beta)$, existen $a, c \in K$ tales que $\alpha^2 = a + c\beta$. Si fuese $c = 0$, $\sigma(\alpha)$ tendria que ser una raíz del polinomio $X^2 - a \in K[X]$, así que o bien $\sigma(\alpha) = \alpha$ o bien $\sigma(\alpha) = -\alpha$: estas dos posibilidades contradicen el hecho de que $\sigma^2(\alpha) = -\alpha$, y entonces vemos que $c \neq 0$. Como entonces $\beta = (\alpha^2 - a)/c \in K(\alpha)$, tenemos que $E = K(\alpha)$. En particular, el polinomio minimal de α sobre K tiene grado 4, ya que $[E : K] = 4$.

Como $\alpha^2 - a = c\beta$, es $(\alpha^2 - a)^2 = c^2\beta^2$, y α es raíz de $f = (X^2 - a)^2 - c^2\beta^2 \in K[X]$. Este polinomio tiene que ser entonces el polinomio minimal de α sobre K y, en particular, ees irreducible. Como E/K es normal, todas las raíces de f están en E y, como este cuerpo esta generado sobre K por una de ellas, vemos que E es el cuerpo de descomposición de f.

Como $c \neq 0$ y $\beta^2 \in K \setminus K^2$, si ponemos $b = c^2\beta^2$ tenemos que $b \in K \setminus K^2$. □

3. Sea E un cuerpo de descomposición de $X^6 - 3$ sobre $\mathbb{Q}$. Determine el grupo de Galois de la extensión $E/\mathbb{Q}$ y la cantidad de extensiones cuadráticas y normales de $\mathbb{Q}$ contenidas en E.

Solución. Sea $\zeta \in \mathbb{C}$ una raíz cúbica primitiva de la unidad, de manera que $-\zeta$ es una raíz sexta primitiva de la unidad. Sea, por otro lado, $\alpha \in \mathbb{R}$ tal que $\alpha^6 = 3$. Las raíces del polinomio son los números $(-\zeta)^i\alpha$ con $0 \leq i < 6$. Claramente, entonces, $E = \mathbb{Q}(\zeta, \alpha)$. Consideremos el diagrama



Claramente $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Como $\mathbb{Q}(\zeta)/\mathbb{Q}$ es normal, el grado $d = [\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}(\zeta)]$ divide entonces a 6. Como $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, el grado d no puede ser ni 1 ni 2, ya que en ese caso $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}]$ sería o 2 o 4 y no podría ser que $\mathbb{Q}(\alpha)$ esté contenido en $\mathbb{Q}(\zeta, \alpha)$. Si fuese $d = 3$, entonces sería $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = 6$ y, en consecuencia, $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta, \alpha)$: esto es imposible porque $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ y ζ no es real. Concluimos así que $d = 6$ y que $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = 12$.

Un automorfismo de la extensión $\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}$ tiene que mandar ζ y α a ζ^i y a $(-\zeta)^j\alpha$ con $1 \leq i \leq 2$ y $0 \leq j < 6$. Esto nos da 12 opciones. Como el grupo de Galois $G = \mathsf{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q})$ tiene orden 12, vemos que todas estas posibilidades efectivamente ocurren y que $G = \{\sigma_{i,j} : i \in \mathbb{Z}_3^\times, j \in \mathbb{Z}_6\}$, con $\sigma_{i,j}(\zeta) = \zeta^i$ y $\sigma_{i,j}(\alpha) = (-\zeta)^j\alpha$.

Pongamos $\rho = \sigma_{1,1}$ y $\tau = \sigma_{2,0}$. Calculando, vemos que $\tau^2 = \rho^6 = \mathsf{id}$ y que $\tau\rho = \rho^{-1}\tau$. Esto nos dice que G es isomorfo a un cociente del grupo diedral $D_{12} = \langle r, t : t^2, r^6, (tr)\rangle$ de orden 12. Como G también tiene orden 12, vemos que, de hecho, $G \cong D_{12}$.

Como toda extensión cuadrática de $\mathbb{Q}$ es normal, para termenar, tenemos que contar la cantidad de subextesiones cuadráticas de $\mathbb{Q}$ contenidas en $\mathbb{Q}(\zeta, \alpha)$. El teorema de Galois nos dice que es lo mismo contar los subgrupos de D_{12} de índice 2. Como todo subgrupo de índice 2 es normal, esto es lo mismo que contar los homomorfismos $D_{12} \to \mathbb{Z}/2\mathbb{Z}$ no triviales.

Un tal homomorfismo $f : D_{12} \to \mathbb{Z}/2\mathbb{Z}$ queda determinado por $\alpha = f(r)$ y $\beta = f(t)$, dos elementos de $\mathbb{Z}/2\mathbb{Z}$ no simultaneamente nulos. Es trivial ver que cualquiera de las tres posibilidades da en efecto un homomorfismos, así que el número de subextensiones buscadas es 3. □

4. Sea p un número primo impar y sea E un cuerpo de descomposición del polinomio $X^p - 2$ sobre $\mathbb{Q}$. Muestre que no hay en E una raíz p^2-ésima primitiva de la unidad.

Solución. Sabemos, de un ejercicio de la práctica, que el grupo de Galois de $X^p - 2$ sobre $\mathbb{Q}$ es isomorfo a $\mathbb{Z}_p^\times \rtimes \mathbb{Z}_p$, que tiene orden $p(p-1)$ y que no es abeliano. Por otro lado, si ζ es una raíz p^2-ésima primitica de la unidad, sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_{p^2} = p(p-1)$. Así, si fuese $\zeta \in E$, sería, de hecho, $E = \mathbb{Q}(\zeta)$. Esto es absurdo, porque sabemos que $\mathbb{Q}(\zeta)/\mathbb{Q}$ tiene grupo de Galois abeliano. □

5. Si E/K es una extensión galoisiana de grado 77, entonces todas sus subextensiones son normales.

Solución. Sea G el grupo de Galois de la extensión. Como $77 = 7 \cdot 11$, los teoremas de Sylow implican inmediatamente que si P_7 y P_{11} son subgrupo de Sylow de ordenes 7 y 11, respectivamente, entonces ambos son normales. En particular, P_7P_{11} es un subgrupo de G y claramente tiene que ser igual a G porque su orden es al menos 77. Como ambos subgrupos de Sylow son normales, vemos que $G \cong P_7 \times P_{11}$. En particular, G es abeliano. El resultado sigue entonces del teorema de Galois. □