ÁLGEBRA 3

Segundo cuatrimestre — 2014

Primer parcial

APELLIDO Y NOMBRE: ....

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

---

1. (*a*) Si E es un subcuerpo de $\mathbb{C}$ tal que $E/\mathbb{Q}$ es una extensión galoisiana finita y $E \not\subseteq \mathbb{R}$, entonces $[E : E \cap \mathbb{R}] = 2$.

(*b*) Si además la extensión $E/\mathbb{Q}$ es cíclica de grado n, $\alpha \in E \setminus \mathbb{R}$ y d es el grado del polinomio minimal de α sobre $\mathbb{Q}$, entonces d divide a n y n/d es impar.

Solución. (*a*) Como la extensión $E/\mathbb{Q}$ es normal, la restricción de la conjugación $z \in E \mapsto \bar{z} \in \mathbb{C}$ tiene imagen en E y se restringe a un automorfismo $\sigma \in \mathsf{Gal}(E/\mathbb{Q})$. El subgrupo (σ) generado por σ tiene orden 2, así que $[E : E^{(\sigma)}] = 2$. Como $E^{(\sigma)} = E \cap \mathbb{R}$, esto prueba lo que queremos.

(*b*) Como $n = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)]d$, es claro que $d \mid n$. Como la extensión $E/\mathbb{Q}$ es galoisiana, también lo es $E/\mathbb{Q}(\alpha)$ y $n/d = [E : \mathbb{Q}(\alpha)] = |\mathsf{Gal}(E/\mathbb{Q}(\alpha))|$. Supongamos que n/d es par. El teorema de Lagrange nos dice entonces que hay en $\mathsf{Gal}(E/\mathbb{Q}(\alpha)$, que tiene orden n/d, un elemento de orden 2. Como $\mathsf{Gal}(E/\mathbb{Q})$ es cíclico, contiene a lo sumo un elemento de orden 2, y esto nos permite concluir que el automorfismo σ de la primera parte está en $\mathsf{Gal}(E/\mathbb{Q}(\alpha))$. En particular, $\sigma(\alpha) = \alpha$, lo que es absurdo. □

2. Si K es un cuerpo de característica positiva p, entonces $\bigcap_{n\geq 1} K^{p^n}$ es un subcuerpo de K y es el más grande subcuerpo de K que es perfecto.

Solución. Si $n \geq 1$, entonces K^{p^n} es un subcuerpo de K: contiene a 1, es cerrado por productos y cocientes, y —como K tiene característica p positiva— es cerrado por sumas. Se sigue entonces que $P = \bigcap_{n\geq 1} K^{p^n}$ es un subcuerpo de K.

Si $x \in P$, entonces para cada $n \geq 1$ existe $y_n \in K$ tal que $y_n^{p^n} = x$. Si $n \geq 1$, entonces $(y_{n+1}^p)^{p^n} = x$, así que y_n e y_{n+1}^p son raíces del polinomio $X^{p^n} - x$, que tiene una única raíz en la clausura algebraica de K: esto nos dice que $y_{n+1}^p = y_n$ y, vía una inducción evidente, que $y_1 = y_{n+1}^{p^n}$ para cada $n \geq 1$. Vemos que $y_1 \in P$ y, como $y_1^p = x$, que $x \in P^p$. Así, P es perfecto.

Supongamos ahora que $F \subseteq K$ es un subcuerpo de K que es perfecto y sea $x \in F$. Para cada $n \geq 1$ existe $y \in F$ tal que $x = y^{p^n}$, y entonces $x \in F^{p^n} \subseteq K^{p^n}$. Concluimos que $x \in \bigcap_{n\geq 1} K^{p^n} = P$ y, en definitiva, que $F \subseteq P$. □

3. Sea K un cuerpo y $f \in K[X]$ un polinomio separable de grado n tal que si E es el cuerpo de descomposición de f sobre K es $\mathsf{Gal}(E/K) \cong S_n$. Si $\alpha \in E$ es una raíz de f, entonces la extensión $K(\alpha)/K$ no tiene subextensiones propias no triviales. ¿Es $K(\alpha)/K$ una extensión galoisiana?

Solución. Sea $G = \mathsf{Gal}(E/K)$ y sea Si $R = \{\alpha_1, \dots, \alpha_n\}$ es el conjunto de las raíces de f en E, de manera que $\alpha_i \neq \alpha_j$ si $i \neq j$. Sabemos que hay un morfismo de grupos $\phi : G \to S_n$ tal que $\sigma(\alpha_i) = \alpha_{\phi(\sigma)(i)}$ para cada $\sigma \in G$ y cada $i \in \{1, \dots, n\}$. Este morfismo es inyectivo, porque las raíces de f generan a E sobre K y, como G tiene $n!$ elementos, se trata, de hecho, de un isomorfismo. Sea H el subgrupo de G tal que $E^H = K(\alpha_1)$. Es claro que un automorfismo $\sigma \in G$ está en H sii $\sigma(\alpha_1) = \alpha_1$, así que $\phi(H)$ es el subgrupo U de S_1 de las permutaciones que dejan fijo a 1.

El subgrupo U es maximal en S_n. Para verlo, sea $V \subseteq S_n$ un subgrupo tal que $V \supsetneq U$, sea $\sigma \in V \setminus U$, y mostremos que $V = S_n$. Sea $\tau \in S_n \setminus U$. Si $\tau^{-1}(1) = \sigma^{-1}(1)$, entonces $\tau\sigma^{-1} \in U$ y $\tau \in U\sigma \subseteq V$; si en cambio es $\tau^{-1}(1) \neq \sigma^{-1}(1)$, entonces la transposición $\mu = (\tau^{-1}(1)\,\sigma^{-1}(1))$ y $\tau\mu\sigma^{-1}$ están en U, de manera que $\tau \in U\sigma\mu \subseteq V$. Esto nos dice que $S_n \subseteq V$.

Como ϕ es un isomorfismo, el subgrupo H es maximal en G y el teorema de Galois nos dice entonces que el cuerpo $K(\alpha_1) = E^H$ no contiene subcuerpos propios distintos de $\mathbb{Q}$. Por otro lado, si $n \geq 3$, es $(23) \in U$ y $(12)(23)(12)^{-1} = (13) \notin U$, así que U no es normal en S_n y $K(\alpha)/K$ no es una extensión normal. Si en cambio $n \leq 2$, entonces G es abeliano y esta extensión es trivialmente normal. $\square$

4. Si $f(X) = X^4 - 2aX^2 + b \in \mathbb{Q}[X]$ es irreducible y $b \in \mathbb{Q}^2$, determine el grupo de Galois del cuerpo de descomposición de f sobre $\mathbb{Q}$ y exhiba sus subxtensiones cuadráticas.

Solución. El polinomio $g(X) = X^2 - 2aX + b$ es irreducible, porque lo es $f(X) = g(X^2)$, así que $a^2 - b \notin \mathbb{Q}^2$. Las raíces de g son $\alpha = a + \sqrt{a^2 - b}$ y $\beta = a - \sqrt{a^2 - b}$. Si $u^2 = \alpha$ y $v^2 = \beta$, las raíces de f son $\pm u$ y $\pm v$. Como $(uv)^2 = \alpha\beta = b$ es un cuadrado en $\mathbb{Q}$, existe $c \in \mathbb{Q}$ tal que $uv = c$. El cuerpo $\mathbb{Q}(u)$ contiene entonces a las cuatro raíces de f y, como está generado por una de ellas, es el cuerpo de descomposición de f. Como f es irreducible, es $[\mathbb{Q}(u) : \mathbb{Q}] = 4$, el grupo $G = \mathsf{Gal}(\mathbb{Q}(u)/\mathbb{Q})$ tiene cuatro elementos, y éstos quedan determinados por la imagen de u, que es un elemento de $\{\pm u, \pm v\}$. Calculando, vemos entonces que los cuatro elementos de G son

	u	v	$-u$	$-v$
id	u	v	$-u$	$-v$
σ	v	u	$-v$	$-u$
τ	$-v$	$-u$	v	u
$\sigma\tau$	$-u$	$-v$	u	v

Cada uno de estos automorfismos tiene orden 2, así que $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ y, en particular, G tiene exactamente tres subgrupos de índice 2, los tres subgrupos cíclicos generados por los elementos no triviales. Los elementos $x_1 = u + v$, $x_2 = u - v$ y $u^2 = \sqrt{a^2 - b}$ quedan fijos por σ, por τ y por $\sigma\tau$, respectivamente, y no son racionales, ya que $\tau(x_1) = -x_1 \neq 0$, $\sigma(x_2) = -x_2 \neq 0$ y $a^2 - b \notin \mathbb{Q}^2$. Los subcuerpos cuadráticos de E son entonces

$$
\begin{aligned}
\mathbb{Q}(u)^\sigma &= \mathbb{Q}(x_1) = \mathbb{Q}(\sqrt{2a + 2c}),\\
\mathbb{Q}(u)^\tau &= \mathbb{Q}(x_2) = \mathbb{Q}(\sqrt{2a - 2c}),\\
\mathbb{Q}(u)^{\sigma\tau} &= \mathbb{Q}(u^2) = \mathbb{Q}(\sqrt{a^2 - b}).
\end{aligned}
$$

5. Sea K un cuerpo de característica p positiva y sea $a \in K$ un elemento que no es de la forma $b^p - b$ para ningún $b \in K$. Muestre que el polinomio $X^p - X - a$ es irreducible en $K[X]$ y determine su grupo de Galois sobre K.

Solución. Sea $\bar{K}$ una clausura algebraica de K y sea $x \in \bar{K}$ es una raíz de $f(X) = X^p - X - a$. La hipótesis hecha sobre a nos dice que $x \notin K$. Si $t \in \mathbb{F}_p$, entonces es $x + t$ también una raíz de f, así que en $K(x)$ hay al menos p raíces distintas de f y se trata, en consecuencia, del cuerpo de descomposición de f sobre K. Como $f(x) = 0$, es $[K(x) : K] \leq p$.

Sea $h(X) \in K[X]$ el polinomio minimal de x. Como h divide a f, h se factoriza completamente en $K(x)$ y, en particular, tiene al menos una raíz y en $K(x)$ aparte de x. Como y es raíz de f, existe $t \in \mathbb{F}_p^\times$ tal que $y = x + t$. Hay entonces un automorfismo $\sigma : K(x) \to K(x)$ tal que $\sigma(x) = x + t$ y, como $\sigma^p(x) = x + px = x$, el orden de σ divide a p. Como $\sigma(x) \neq x$, el orden es p. El grupo de Galois de la extensión $K(x)/K$ tiene entonces orden al menos p, así que el grado de la extensión es al menos p. Esto y lo anterior muestra que, de hecho, el grado es exactamnte p y, en particular, que f es irreducible sobre K.

Como el grupo de Galois de $K(x)/K$ tiene orden primo, es cíclico de ese orden y está generado por cualquiera de sus elementos no triviales, como σ. $\square$