Teoría de Galois

Soluciones de algunos ejercicios de la Hoja 2. Carolina Vallejo Rodríguez

Escribiremos E/K para denotar que E es una extensión del cuerpo K. El grado $|E:K|$ de la extensión E/K es la dimensión de E como K-espacio vectorial. Si $a \in E$ es algebraico sobre K, denotaremos por $\mathrm{Irr}(K,a) \in K[x]$ al polinomio mínimo (o irreducible) de a sobre K.

1. Demuestra la igualdad $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, y halla un polinomio irreducible de $\mathbb{Q}[x]$ de grado 4 que tenga una raíz en $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Solución. Obviamente $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$, para probar la otra inclusión basta notar que $(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3}) = -1$, luego $-\sqrt{2}+\sqrt{3} = (\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. En particular, $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ nos da la inclusión que falta.

Escribimos $\alpha = (\sqrt{2}+\sqrt{3})$, entonces $\alpha^2 = 2+2\sqrt{6}+3$, de donde $\alpha^2-5 = 2\sqrt{6}$ y volviendo a elevar al cuadrado $(\alpha^2-5)^2 = 24$. Por tanto, α es raíz del polinomio $x^4-10x+1 \in \mathbb{Q}[x]$.

2. Calcula el polinomio mínimo de $\alpha = \sqrt[3]{9}+\sqrt[3]{3}-1$ sobre $\mathbb{Q}$.

Solución. Elevando al cubo la expresión $\alpha+1 = \sqrt[3]{9}+\sqrt[3]{3}$ obtenemos

$$(\alpha+1)^3 = 9+9\sqrt[3]{3}+9\sqrt[3]{3}+3 = 12+9(\alpha+1)\,.$$

Por tanto, α es raíz del polinomio $f(x) = (x+1)^3-9(x+1)-12 \in \mathbb{Q}[x]$. Para ver que $f(x)$ es irreducible en $\mathbb{Q}[x]$ podemos usar que es lo mismo que ver que $g(x) = f(x-1) = x^3-9x-12$ irreducible, y aplicar el criterio de reducción módulo p con $p=5$ (basta ver que $\overline{g} \in \mathbb{F}_5[x]$ no tiene raíces en $\mathbb{F}_5$). También se puede ver que f es irreducible usando el criterio de Einsestein con $p=3$, y de hecho es mucho más sencillo así.

3. Estudia cuáles de los siguientes subcuerpos de $\mathbb{C}$ coinciden: $\mathbb{Q}(i,\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2}+i)$, $\mathbb{Q}\left(\sqrt{2},\sqrt{1+\sqrt{2}}\right)$ y $\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$.

Solución. Procediendo como en el ejercicio 1 se puede ver que $\mathbb{Q}(i,\sqrt{2}) = \mathbb{Q}(\sqrt{2}+i)$. Podemos ver que $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\sqrt{2}i) \neq \mathbb{Q}(\sqrt{2},i)$ usando, por ejemplo, que $|\mathbb{Q}(\sqrt{2}i):\mathbb{Q}| = 2$ mientras que $|\mathbb{Q}(\sqrt{2},i):\mathbb{Q}| = 4$. Finalmente $\mathbb{Q}\left(\sqrt{2},\sqrt{1+\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$ pues $(\sqrt{1+\sqrt{2}})^2 = 1+2\sqrt{2}+2$ luego $\sqrt{2} \in \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$, y no coinciden con ninguna otra de las extensiones de $\mathbb{Q}$ puesto que son reales mientras que el resto no lo son.

4. Halla el grado y una base de las siguientes extensiones de cuerpos.

(i)	$\mathbb{Q}(\sqrt[6]{3})/\mathbb{Q}$	(ii)	$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$	(iii)	$\mathbb{Q}(\sqrt{2},\sqrt{3},i)/\mathbb{Q}$
(iv)	$\mathbb{Q}(\sqrt{2}i)/\mathbb{Q}$	(v)	$\mathbb{Q}(\sqrt[5]{2},\sqrt[3]{7})/\mathbb{Q}(\sqrt[5]{2})$	(vi)	$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$
(vii)	$\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$	$(viii)$	$\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$	(ix)	$\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$.

Solución. (i) Tenemos que $\sqrt[6]{3}$ es raíz del polinomio $x^6-3 \in \mathbb{Q}[x]$ que es irreducible por el criterio de Einsestein. Por el Teorema del Elemento Algebraico $|\mathbb{Q}(\sqrt[6]{3}):\mathbb{Q}| = 6$ y si $\alpha = \sqrt[6]{3}$, entonces una $\mathbb{Q}$-base de $Q(\sqrt[6]{3})$ viene dada por $\{1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5\}$.

(ii) Por el ejercicio 1 sabemos que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$, además el elemento $\alpha=\sqrt{2}+\sqrt{3}$ es raíz del polinomio $x^4-10x^2+1\in\mathbb{Q}[x]$ que es irreducible sobre $\mathbb{Q}$. Por el Teorema del Elemento Algebraico, tenemos que $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=4$ y una $\mathbb{Q}$-base es $\{1,\alpha,\alpha^2,\alpha^3\}$

(iii) Notamos que $\mathbb{Q}(\sqrt{2},\sqrt{3},i)=\mathbb{Q}(\sqrt{2}+\sqrt{3})(i)$, y por el Teorema de transitividad de grados

$$|\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}|=|\mathbb{Q}(\sqrt{2}+\sqrt{3})(i):\mathbb{Q}(\sqrt{2}+\sqrt{3})||\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|\,.$$

Como $x^2+1\in\mathbb{Q}(\sqrt{2}+\sqrt{3})[x]$ es irreducible (pues no tiene en raíces en $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{R}$) e i es raíz de x^2+1, usando el Teorema del Elemento Algebraico junto con el apartado (ii) de este ejercicio

$$|\mathbb{Q}(\sqrt{2},\sqrt{3},i)/\mathbb{Q}|=|\mathbb{Q}(\sqrt{2}+\sqrt{3})(i):\mathbb{Q}(\sqrt{2}+\sqrt{3})||\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}|=2\cdot 4=8\,,$$

y una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2},\sqrt{3},i)$ es $\{1,\alpha,\alpha^2,\alpha^3,\alpha i,\alpha^2 i,\alpha^3 i\}$.

(iv)$|\mathbb{Q}(\sqrt{2}i):\mathbb{Q}|=2$, porque x^2+2 es irreducible por Einsestein (o por no tener raíces en $\mathbb{Q}$).

(v)$|\mathbb{Q}(\sqrt[5]{2},\sqrt[3]{7}):\mathbb{Q}(\sqrt[5]{2})|=3$ porque x^3-7 no tiene raíces en $\mathbb{Q}(\sqrt[5]{2})$, si $\sqrt[3]{7}\in\mathbb{Q}(\sqrt[5]{2})$, entonces 3 dividiría a 5 por el Teorema 2.1. Comparad con el ejercicio 13.

(vi)$\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})|=2$ puesto que $\sqrt[4]{2}$ es raíz de $x^2-\sqrt{2}$ que es irreducible por no tener raíces en $\mathbb{Q}(\sqrt{2})$.

(vii) Sea $\alpha=\sqrt{1+\sqrt{3}}$, tenemos que $\alpha^2=1+\sqrt{3}$, de donde $(\alpha^2-1)^2=3$. Luego α es raíz del polinomio $x^4-2x^2-2\in\mathbb{Q}[x]$ que es irreducible en $\mathbb{Q}[x]$ por el criterio de Einsestein. Por tanto, $\mathbb{Q}(\sqrt{1+\sqrt{3}}):\mathbb{Q}|=4$ y una $\mathbb{Q}$-base es $\{1,\alpha,\alpha^2,\alpha^3\}$.

(viii) Notad que $e^{2\pi i/5}\in\mathbb{C}$ es una raíz primitiva quinta de la unidad. Sabemos que su polinomio irreducible sobre $\mathbb{Q}$ es $\Phi_5(x)=x^4+x^3+x^2+x+1\in\mathbb{Z}[x]$ (probamos su irreducibilidad así como que $e^{2\pi i/5}$ es raíz en el Tema 1). Por tanto, $|\mathbb{Q}(e^{2\pi i/5}):\mathbb{Q}|=4$ y una $\mathbb{Q}$-base viene dada por las 5 raíces quintas de la unidad.

(ix)Notad que $\sqrt[4]{3}$ es raíz del polinomio $x^2+\sqrt{3}\in\mathbb{R}[x]$ (pues $\sqrt[4]{-1}=-i$) que no tiene raíces en $\mathbb{R}$. Por tanto, $|\mathbb{R}(\sqrt[4]{-3}):\mathbb{R}|=1$ y $\{1,\sqrt[4]{-3}\}$ es

5. Halla el grado y una base de la extensión $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$. Calcula t^{-1} y $(t+1)^{-1}$ como combinación lineal de los elementos de la base que has encontrado.

Solución. Sabemos que $\mathbb{F}_7(t)/\mathbb{F}_7$ es una extensión trascendente (en particular infinita), sin embargo, $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$ es una extensión de grado 2. Notad que $f(x)=x^2-t^2\in\mathbb{F}_7(t^2)[x]$ es irreducible puesto que no tiene raíces en $\mathbb{F}_7(t^2)$ y $f(t)=0$, por tanto t es algebraico sobre $\mathbb{F}_7(t^2)$. Por el Teorema del Elemento Algebraico, $|\mathbb{F}_7(t):\mathbb{F}_7(t^2)|=2$ y una $\mathbb{F}_7(t^2)$-base viene dada por $\{1,t\}$. Es fácil ver que $t^{-1}=1/t^2t$ donde $1/t^2\in\mathbb{F}_7(t)$. Para calcular $(t+1)^{-1}$ en función de la base, la idea es que, al no ser t una raíz de $x+1\in\mathbb{F}_7(t)[x]$, entonces $\mathrm{mcd}(x+1,x^2-t^2)=1$. Aplicando el algoritmo de la división, tenemos que $x^2-t^2=(x+1)(x-1)+(1-t^2)$ donde $1-t^2\in\mathbb{F}_7(t^2)$. Entonces

$$\frac{1}{1-t^2}(x^2-t^2)+(x+1)\frac{1-x}{1-t^2}=1\,.$$

Evaluando en t obtenemos

$$(t+1)\frac{1-t}{1-t^2}=1\,,$$

es decir, $(t+1)^{-1}=\frac{1}{1-t^2}1+\frac{1}{t^2-1}t$.

6. Considera las siguientes cuestiones sobre las raíces de la unidad:

a) Sea p un número primo y sea $1\neq\xi\in\mathbb{C}$ tal que $\xi^p=1$. Demuestra que $|\mathbb{Q}(\xi):\mathbb{Q}|=p-1$.

b) Sea $\omega=\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}=\mathrm{e}^{\frac{\pi}{6}i}\in\mathbb{C}$. Observa que $\omega^{12}=1$ pero que $\omega^r\neq 1$ si $1\leq r<12$. Demuestra que $|\mathbb{Q}(\omega):\mathbb{Q}|=4$ y calcula $\mathrm{Irr}(\mathbb{Q},\omega)$ el polinomio mínimo de ω sobre $\mathbb{Q}$.

c) Sea p un número primo, calcula el grado del polinomio mínimo de $\cos\frac{2\pi}{p}$ sobre $\mathbb{Q}$. Deduce que

$\cos\frac{2\pi}{p} \in \mathbb{Q}$ si, y solo si, $p \in \{2,3\}$. Concluye que sen$\frac{2\pi}{p} \in \mathbb{Q}$ si, y solo si, $p = 2$.

Solución. Para el apartado (a) recordamos que $\Phi_p(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x]$ es irreducible sobre $\mathbb{Q}$. Además, vimos que $\Phi_p(x) = x^p - 1/(x-1)$, es decir las raíces de Φ_p son todas las raíces p-ésimas de la unidad distintas de 1. Como ξ es raíz de Φ_p por el Teorema del Elemento Algebraico $|\mathbb{Q}(\xi) : \mathbb{Q}| = p - 1$. Nos faltó acabar el apartado (c) en clase. Sabemos que $\cos 2\pi/p \in \mathbb{Q}$ si, y solo si, $p \in \{2,3\}$, y, de hecho, si $p > 2$ entonces $|\mathbb{Q}(\cos 2\pi/p) : \mathbb{Q}| = \frac{p-1}{2}$. Si $p = 2$ entonces $\sin \pi = 0$. Supongamos que $p > 3$. Por reducción al absurdo, supongamos que $\alpha = \sin 2\pi/p \in \mathbb{Q}$. Entonces $\cos^2 2\pi/p = 1 - \sin^2 2\pi/p = 1 - \alpha^2 \in \mathbb{Q}$. Más aún, $\cos 2\pi/p$ es raíz del polinomio racional $x^2 - 1 + \alpha^2 \in \mathbb{Q}[x]$. Por el Teorema 2.3, entonces $|\mathbb{Q}(\cos 2\pi/p) : \mathbb{Q}| = \frac{p-1}{2} \leq 2$, pero esto contradice nuestra suposición inicial $p > 3$. Para $p = 3$ es complicado usar estas técnicas, lo mejor es usar que $\sin 2\pi/3 = \sqrt{3}/2 \notin \mathbb{Q}$.

7. Dada E/K una extensión, prueba que el conjunto de elementos de E que son algebraicos sobre K forma un subcuerpo de E. Si $\mathbb{A}$ es el conjunto de elementos de $\mathbb{C}$ que son algebraicos sobre $\mathbb{Q}$, prueba que $\mathbb{A}/\mathbb{Q}$ es una extensión de grado infinito.
Sugerencia: para la segunda parte, usa el criterio de Einsestein.

8. Sea E/K una extensión de cuerpos y $\alpha \in E$. Prueba que $K[\alpha]$ es un cuerpo si, y solo si, $K(\alpha)/K$ es una extensión algebraica.

9. Considera E/K una extensión de cuerpos y un polinomio $p(x) = a_0 + a_1x + \cdots + a_nx^n \in E[x]$ de modo que los coeficientes a_i de p son algebraicos sobre E. Demuestra que si $u \in E$ es una raíz de p, entonces u es algebraico sobre K.
Sugerencia: considera el subcuerpo $L = K(a_0, \ldots, a_n) \subseteq E$.

Solución. Consideramos $L = K(a_0, \ldots, a_n)$. Como los $a_i \in L$ son algebraicos sobre K, la extensión L/K es finita. Ahora u es algebraico sobre L por ser raíz del polinomio $p \in L[x]$. Por el Teorema del Elemento Algebraico $L(u)/L$ es finita. Por la transitividad de grados $L(u)/K$ es finita, luego algebraica, y concluimos que $u \in E$ es algebraico sobre K.

10. Sea E/K una extensión y $\alpha \in E$ algebraico sobre K. Si L es un cuerpo intermedio, demuestra que el polinomio mínimo de α sobre L divide al polinomio mínimo de α sobre K. Concluye que $|L(\alpha) : L| \leq |K(\alpha) : K|$.

Solución. Sean $p = \mathrm{Irr}(L, \alpha)$ y $q = \mathrm{Irr}(K, \alpha)$. Como $q \in K[x] \subseteq L[x]$ y $q(\alpha) = 0$. Por el Teorema del Elemento Algebraico, p divide a q. La segunda parte se sigue directamente pues $|L(\alpha) : L| = \delta(p) \leq \delta(q) = |K(\alpha) : K|$

11. Considera una extensión de cuerpos E/K.

a) Demuestra que si es una extensión de grado primo, entonces los únicos subcuerpos intermedios $K \subseteq L \subseteq E$ son $L = K$ y $L = E$.

b) Demuestra que una extensión de grado primo es simple.

c) Si L_1 y L_2 son cuerpos intermedios tales que L_1/K y L_2/K son extensiones finitas de grados primos entre sí, demuestra que $L_1 \cap L_2 = K$.

d) Si $\alpha \in E$ es tal que $K(\alpha)/K$ es una extensión de grado impar, calcula $K(\alpha^2)/K$.

e) Suponiendo que el polinomio mínimo de un elemento α sobre un cuerpo K es $x^3 + x - 1$, halla el polinomio mínimo de α^2 sobre K.

Solución. **a)** Se sigue del teorema de transitividad de grados.
b) Como $|E : K| = p > 1$ entonces K está estrictamente contenido en K. Sea $a \in E \setminus K$, tenemos que $K \subset K(a) \subseteq E$. Por el apartado a) se tiene que $K(a) = E$.

c) Sea $K \subseteq L = L_1 \cap L_2 \subseteq L_1, L_2$. Tenemos que $|L : K|$ divide a $|L_1 : K|$ y $|L_2 : K|$ por el teorema de transitividad de grados. Por hipótesis estos grados son coprimos, luego $|L : K| = 1$, es decir, $L_1 \cap L_2 = K$.
d) Tenemos que $K \subseteq K(\alpha^2) \subseteq K(\alpha)$. Supongamos que $K(\alpha^2) \neq K(\alpha)$. Entonces a es raíz del polinomio $x^2 - \alpha^2 \in K(\alpha^2)[x]$ que es irreducible por no tener raíces en $K(\alpha^2)$. Por el teorema del elemento algebraico $|K(\alpha) : K(\alpha^2)| = 2$ y por la transitividad de grados, 2 divide a $|K(\alpha) : K|$, contradiciendo nuestra hipótesis inicial. Por tanto, $K(\alpha^2) = K(\alpha)$.
e) Como $|K(\alpha) : K| = 3$ es impar, por el apartado (d) sabemos que $K(\alpha^2) = K(\alpha)$, y, por tanto, el polinomio mínimo de α^2 sobre K tiene grado 3. Ahora α satisface $\alpha^3 + \alpha - 1 = 0$, luego $(\alpha^3 + \alpha)^2 = 1$. Desarrollando obtenemos

$$\alpha^6 - 2\alpha^4 + \alpha^2 - 1 = 0\,.$$

Por tanto, α^2 es raíz del polinomio $x^3 - 2x^2 + x - 1 \in K[x]$, que es irreducible puesto que tiene grado 3.

12. Sea E/K una extensión y sean $a, b \in E$ algebraicos sobre K con $|K(a) : K| = n$ y $|K(b) : K| = m$.

a) Prueba que $|K(a, b) : K(b)| \leq n$.

b) Si n y m son coprimos, prueba que $K(a) \cap K(b) = K$ y $|K(a, b) : K| = nm$. Deduce que $\operatorname{Irr}(K, a) = \operatorname{Irr}(K(b), a)$.

c) Sean $a = \sqrt{3}$ y $b = \sqrt[3]{2}$. Comprueba que $\mathbb{Q}(a, b) = \mathbb{Q}(a + b)$ y calcula $\operatorname{Irr}(\mathbb{Q}, a + b)$

Sugerencia: para probar la igualdad del último apartado, primero prueba que $a \in \mathbb{Q}(a + b)$.

Solución. Escribiendo $L = K(b)$, el primer apartado nos pide probar que $|L(a) : L| \leq |K(a) : K|$, que es exactamente el ejercicio 10. La primera parte del segundo apartado se sigue directamente del ejercicio 11.(c). Usando la transitvidad de grados podemos escribir $|K(a, b) : K|$ de dos formas

$$|K(a, b) : K| = |K(a)(b) : K(a)||K(a) : K| = |K(b)(a) : K(b)||K(b) : K|\,.$$

Por tanto n y m dividen a $|K(a, b) : K|$. Como n y m son coprimos se tiene que nm divide a $|K(a, b) : K|$, por el apartado (a) y la transitividad de grados sabemos que $|K(a, b) : K| \leq nm$ lo que fuerza la igualdad.

El último apartado requiere más trabajo. Sabemos que $|\mathbb{Q}(a, b) : \mathbb{Q}| = 6$ pues $|\mathbb{Q}(a) : \mathbb{Q}| = 2$ y $|\mathbb{Q}(b) : \mathbb{Q}| = 3$. Escribimos $\alpha = a + b$. Entonces $(\alpha - \sqrt{3})^3 = 2$ de donde $\alpha^3 - 3\alpha^2\sqrt{3} + 9\alpha + 3\sqrt{3} - 2 = 0$. Concluimos que

$$\sqrt{3} = \frac{2 - 9\alpha - \alpha^3}{3 - 3\alpha^2} \in \mathbb{Q}(\alpha)\,.$$

Por tanto $\alpha - \sqrt{3} = \sqrt[3]{2} \in \mathbb{Q}(\alpha)$ y, por tanto, $\mathbb{Q}(\alpha) = \mathbb{Q}(a, b)$. Sabemos que $\operatorname{Irr}(\mathbb{Q}, \alpha)$ tiene grado 6, por tanto, para acabar el apartado bastará encontrar un polinomio mónico de grado 6 que se anule en α (rutina).

13. Sea $K = \mathbb{F}_2[x]/(x^2 + x + 1)$.

a) Demuestra que K es un cuerpo con cuatro elementos, y escribe la tabla del producto de K.

b) Determina todos los automorfismos de K.

c) Demuestra que cualquier otro cuerpo con 4 elementos es isomorfo a K.

14. Considera E/K una extensión de cuerpos, y sean $\alpha_1, \ldots, \alpha_n$ elementos de E. Sea $\sigma \colon E \to L$ un isomorfismo de cuerpos. Prueba la igualdad:

$$\sigma(K(\alpha_1, \ldots, \alpha_n)) = \sigma(K)(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))\,.$$

15. Supongamos que E_1/K_1 es una extensión finita y que E_2/K_2 es otra extensión tal que existe un isomorfismo de cuerpos

$$\sigma \colon E_1 \to E_2\,.$$

Demuestra que si $\sigma(K_1) = K_2$, entonces $|E_1 : K_1| = |E_2 : K_2|$.

Diremos que las extensiones E_1/K_1 y E_2/K_2 son isomorfas, y escribiremos $E_1/K_1 \cong E_2/K_2$ si existe un isomorfismo de cuerpos $\sigma\colon E_1 \to E_2$ tal que $\sigma(K_1) = K_2$.

16. Decide justificadamente si cada una de las siguientes afirmaciones es verdadera o falsa:

a) Sea E/K una extensión finita y $p(x) \in K[x]$ irreducible. Si el grado de p y el grado de E/K son coprimos, entonces p no tiene raíces en E.

b) Sea E/K una extensión finita y $p \in K[x]$ un polinomio irreducible. Si p tiene una raíz en E, entonces el grado de p es igual a $|E : K|$.

c) Sea E/K una extensión finita y $p \in K[x]$ un polinomio irreducible. Si p tiene una raíz en E, entonces el grado de p divide a $|E : K|$.

d) Sea E/K una extensión y supongamos que $\alpha, \beta \in E$ son algebraicos sobre K. Si existe un isomorfismo de cuerpos $\theta\colon K(\alpha) \to K(\beta)$ tal que $\theta(\alpha) = \beta$, entonces existe un polinomio irreducible $p(x) \in K[x]$ tal que $p(\alpha) = p(\beta) = 0$.

e) Sea E/K una extensión y supongamos que $\alpha, \beta \in E$ son algebraicos sobre K. Si existe un isomorfismo de cuerpos $\theta\colon K(\alpha) \to K(\beta)$ tal que $\theta(\alpha) = \beta$ y $\theta(k) = k$ para todo $k \in K$, entonces existe un polinomio irreducible $p(x) \in K[x]$ tal que $p(\alpha) = p(\beta) = 0$.

Solución.

(a) Falsa. Por reducción al absurdo supongamos que $a \in E$ es raíz de p. Como p es irreducible, $\delta(p) = |K(a) : K|$ por el teorema 2.3 (elemento algebraico). Por el teorema 2.1 (transitividad de índices) $\delta(p)$ divide a $|E : K|$, una contradicción.

(b) Falsa. Basta considerar $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ que tiene grado 4, y el polinomio $x^2 - 2 \in \mathbb{Q}[x]$ que es irreducible y tiene sus raíces en $\mathbb{Q}(\sqrt[4]{2})$.

(c) Verdadera (ver apartado (a)).

(d) Falsa. Contraejemplo (de Mateo Rodríguez y Pablo Sánchez): No podemos buscar como contraejemplo una extensión E/K donde K sea el cuerpo primo de E porque todo isomorfismo $K(\alpha) \to K(\beta)$ fija elemento a elemento a K y la conclusión se seguiría de la Observación 2.7[1]. Consideramos $\mathbb{C}/\mathbb{Q}(\sqrt{2})$ y los elementos $\sqrt[4]{2}, \sqrt[4]{2}i \in \mathbb{C}$ que son algebraicos sobre $\mathbb{Q}(\sqrt{2})$. La aplicación $\theta\colon \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2}i)$ definida por $\theta(a) = a$ para todo $a \in \mathbb{Q}$ y $\theta(\sqrt[4]{2}) = \sqrt[4]{2}i$ define un isomorfismo (notad que $\theta|_{\mathbb{Q}(\sqrt{2})} = \sigma$ es un isomorfismo mandando $\sqrt{2} \mapsto -\sqrt{2}$ que se extiende a θ por el Teorema 2.5); pero $\sqrt[4]{2}$ y $\sqrt[4]{2}i$ no comparten polinomio irreducible sobre $\mathbb{Q}(\sqrt{2})$. Estos son $p(x) = x^2 - \sqrt{2}$ y $q(x) = x^2 + \sqrt{2}$ respectivamente (lo que sí ocurre es que $\sigma(p) = q$, por eso θ realmente define un isomorfismo aplicando el teorema 2.5).

(e) Es la Obesrvación (Corolario) 2.7 que vimos en clase. Es muy sencilla de probar. Solo hay que usar que $\theta(p(\alpha)) = (\theta(p))(\theta(\alpha)) = p(\beta)$ pues $p \in K[x]$ y θ fija K elemento a elemento.

Ejercicios Adicionales

17. Sea E/K una extensión finita y $\alpha \in E$. Si L es un cuerpo intermedio, entonces $|L(\alpha) : L|$ divide a $|K(\alpha) : K|$.
Sugerencia: puedes suponer que $\alpha \notin L$ porque en caso contrario $|L(\alpha) : L| = 1$, distingue $L(\alpha) = K(\alpha)$ y $L(\alpha) \supset K(\alpha)$, y trabaja con $F = L \cap K(\alpha)$.

18. Sea E/K una extensión algebraica y $K \subseteq D \subseteq E$ un subanillo de E. Demuestra que D es un subcuerpo de E.

[1] En clase escribí Corolario 2.7, pero no es consecuencia del Teorema 2.5 sino un ejercicio fácil de probar. Como lo usaremos a menudo, le damos *status* de Observación 2.7.

19. Comprueba que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{id\}$ y calcula $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}))$.

20. Decide justificadamente si cada una de las siguientes afirmaciones es verdadera o falsa:

a) $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2}i)$ son cuerpos isomorfos.

b) Si $\alpha \in \mathbb{C}$ es una raíz del polinomio $x^3 + \sqrt[5]{3}x^2 - \sqrt[7]{2}x + i$, entonces α es algebraico sobre $\mathbb{Q}$.

c) Sea E/K una extensión y $a \in E$ algebraico sobre K, entonces $a \notin K(a + a^{-1})$.

21. Sean $a, b \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$ tales que $|\mathbb{Q}(a) : \mathbb{Q}| = |\mathbb{Q}(b) : \mathbb{Q}|$. Se tiene que $\mathbb{Q}(a) \cong \mathbb{Q}(b)$ si, y solo si, $\mathbb{Q}(b)$ contiene una raíz de $p = \mathrm{Irr}(\mathbb{Q}, a)$.