Teoría de Galois

Soluciones a algunos ejercicios de la Hoja 3. Carolina Vallejo Rodríguez

Escribiremos E/K para denotar que E es una extensión del cuerpo K. Decimos que E/K es normal si E es el cuerpo de escisión (descomposición) de algún polinomio $f \in K[x]$, y escribimos $E = K(f)$ en tal caso.

1. Construye cuerpos de escisión sobre $\mathbb{Q}$ de los polinomios $x^3 - 1$, $x^4 + 5x^2 + 5$ y $x^6 - 8$ y calcula el grado de la extensión correspondiente.
Extra: Calcula los grupos de Galois asociados a cada extensión.
Solución. Sea $f(x) = x^6 - 8$. Notamos que $\sqrt[6]{8} = \sqrt{2}$. Las raíces de f son de la forma $\sqrt{2}\xi$ donde ξ es una raíz sexta de la unidad. Como una raíz primitiva sexta de la unidad es $\xi = e^{\pi/3i} = 1/2 + \sqrt{3}/2i$ y $\{\xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6\} = \{1/2 + \sqrt{3}/2i, -1/2 + \sqrt{3}/2i, -1, -1/2 - \sqrt{3}/2i, 1/2 - \sqrt{3}/2i, 1\}$ (en ese orden), vemos que $\mathbb{Q}(f) = \mathbb{Q}(\sqrt{3}, \xi) = \mathbb{Q}(\sqrt{2}, \sqrt{3}i)$. Por cierto, $\mathbb{Q}(f) = \mathbb{Q}(\sqrt{3}\xi) = \mathbb{Q}(\sqrt{2} + \sqrt{3}i)$. Llegados a este punto hay distintas formas de calcular el grado de $\mathbb{Q}(f)/\mathbb{Q}$. Si usamos que $\mathbb{Q}(f) = \mathbb{Q}(\sqrt{2}, \sqrt{3}i)$, pues podemos notar que $\mathrm{Irr}(\mathbb{Q}, \sqrt{2}) = x^2 - 2$ e $\mathrm{Irr}(\mathbb{Q}(\sqrt{2}), \sqrt{3}i) = x^2 + 3$, y usar el teorema del elemento algebraico dos veces y luego el teorema de transitividad de grados para obtener que $|\mathbb{Q}(f) : \mathbb{Q}| = 4$. De otro modo, si notamos que $\mathbb{Q}(\sqrt{2}, \xi) = \mathbb{Q}(\sqrt{2}\xi)$ (hacer esta observación sería la parte delicada) y que $x^2 - 2$ divide a $x^6 - 8$, obtenemos que $x^6 - 8 = (x^2 - 2)(x^4 + 2x^2 + 4)$ siendo $\sqrt{2}\xi$ claramente una raíz del segundo factor. La cuestión ahora sería ver que $x^4 + 2x^2 + 4$ es irreducible y aplicar el teorema del elemento algebraico. Este camino es más complicado.

Queremos calcular $G = \mathrm{Gal}(E/\mathbb{Q})$, donde $E = \mathbb{Q}(f)$. Como $\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq E$ y $\mathbb{Q}(\xi)/\mathbb{Q}$ es normal, podríamos usar el Teorema 3.4.6 y extender los elementos de $\mathrm{Gal}(E/\mathbb{Q})$, pero, ¿cuál es $\mathrm{Irr}(\mathbb{Q}, \xi)$? Como aún no hemos visto polinomios ciclotómicos en general, mejor usar otro subextensión normal. Hemos visto que $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}i)$, luego $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = L \subseteq E$ y $L/\mathbb{Q}$ es normal. Además $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma\}$ donde $\sigma(\sqrt{2}) = -\sqrt{2}$ (estamos usando que $|\mathrm{Gal}(L/\mathbb{Q})| = 2$ y el Corolario 3.10). Ahora, por el Corolario 3.4.7 sabemos que cada uno de los automorfismos en $\mathrm{Gal}(L/\mathbb{Q})$ tiene dos extensiones a G. De nuevo, por el Corolario 2.6 por ser $\pm\sqrt{3}i$ raíces de $x^2 + 3 \in L[x]$ irreducible, podemos extender la identidad y σ según $\sqrt{3}i \mapsto -\sqrt{3}i$.

	$\sqrt{2}$	$\sqrt{3}i$
τ_1	$\sqrt{2}$	$\sqrt{3}i$
τ_2	$\sqrt{2}$	$-\sqrt{3}i$
τ_3	$-\sqrt{2}$	$\sqrt{3}i$
τ_4	$-\sqrt{2}$	$-\sqrt{3}i$

En la tabla anterior $\tau_1|_L = 1 = \tau_2|_L$ y $\tau_3|_L = \sigma = \tau_4|_L$. De hecho, podemos notar que $\langle\tau_2\rangle, \langle\tau_3\rangle \triangleleft G$ son dos subgrupos normales de orden 2. Además $\langle\tau_2\rangle \cap \langle\tau_3\rangle = 1$, es decir, $G = \langle\tau_2\rangle \times \langle\tau_3\rangle \cong \mathsf{C}_2 \times \mathsf{C}_2$[1]. Por tanto, el grupo de Galois asociado a f, $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$, es un 4-grupo de Klein.

2. Sean $f(x) = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$ y $g(x) = (x^2 - 2x - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Demuestra que $\mathbb{Q}(\sqrt{3}, i)$ es cuerpo de escisión de f y g sobre $\mathbb{Q}$.

3. Demuestra que $\mathbb{Q}(\sqrt{2}, i)$ es un cuerpo de escisión de $x^2 - 2\sqrt{2}x + 3$ sobre $\mathbb{Q}(\sqrt{2})$.

Solución. Las raíces en $\mathbb{C}$ de $x^2 - 2\sqrt{2}x + 3$ son $\frac{2\sqrt{2} \pm \sqrt{8-12}}{2} = \sqrt{2} \pm i$, luego el cuerpo de escisión sobre $\mathbb{Q}$ del polinomio es $\mathbb{Q}(\sqrt{2} \pm i) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. Como $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i) = E$, entonces E también es cuerpo de escisión del polinomio sobre $\mathbb{Q}(\sqrt{2})$.

[1] Si $N, M \triangleleft G$ son tales que $NM = G$ y $N \cap M$, entonces G es el producto directo de N y M, es decir, $G = N \times M$.

4. Demuestra que $K = \mathbb{F}_2[y]/(y^3 + y + 1)$ es el cuerpo de escisión de $x^3 + x + 1$ y $x^3 + x^2 + 1$ sobre $\mathbb{F}_2$.

Solución. Por un lado, $K = \{0, 1, \overline{y}, \overline{y}+1, \overline{y}^2, \overline{y}^2+1, \overline{y}^2+\overline{y}, \overline{y}^2+\overline{y}+1\}$ (por el algoritmo de la división). Sabemos que $\overline{y} \in K$ es raíz de $x^3 + x + 1$ por el Teorema de Kronecker (Lema 3.3). Además, cada $\sigma \in \mathrm{Gal}(K/\mathbb{F}_2)$ lleva $\overline{y}$ en otra raíz de $f(x) = x^3 + x + 1$ (como f es irreducible y $f' \neq 0$ sabemos que todas las raíces de f en cualquier extension de $\mathbb{F}_2$ son distintas). También sabemos que $\mathrm{Frob} \in \mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{F}_2)$ porque K es finito, y $\mathrm{Frob}^2 \in \mathrm{Gal}(K/\mathbb{F}_2)$. Por tanto, $\mathrm{Frob}(\overline{y}) = \overline{y}^2$ y $\mathrm{Frob}^2(\overline{y}) = \overline{y}^4 = \overline{y}^2 + \overline{y}$ son raíces de $x^3 + x + 1$, como este polinomio tiene como mucho 3 raíces distintas, concluimos que estas son todas las raíces, luego $x^3 + x + 1$ se escinde en K. Como además $K = \mathbb{F}_2(\overline{y}, \overline{y}^2, \overline{y}^2 + \overline{y})$ tenemos que $K = \mathbb{F}_2(x^3 + x + 1)$. Podemos proceder de forma similar para comprobar que K es cuerpo de escisión de $x^3 + x^2 + 1$ (eso sí, primero debemos encontrar una raíz).

Otra forma, habría sido evualuar estos polinomios en los distintos elementos de K y comprobar que cada uno tiene tres raíces distintas en K. Deberíais probarlo de esta forma también.

Una última forma: por la prueba del Teorema 3.5.2, sabemos que K es el cuerpo de escisión de $x^8 - x$ sobre $\mathbb{F}_2$. En particular, $K/\mathbb{F}_2$ es una extensión normal. Ahora, por el Teorema de Kronecker (Lema 3.3), sabemos que $\overline{y} \in K$ es una raíz de $x^3 + x + 1$ y $K = \mathbb{F}_2(\overline{y})$, por ser $K/\mathbb{F}_2$ normal, $x^3 + x + 1$ se escinde (Teorema 3.9) y K es el cuerpo de escisión de $x^3 + x + 1$. Para ver que también lo es de $x^3 + x^2 + 1$ tendríamos que encontrar primero una raíz de $x^3 + x^2 + 1$. Por ejemplo, $(\overline{y} + 1)^3 + (\overline{y} + 1)^2 + 1 = 0$ (haced las comprobaciones) y $K = \mathbb{F}_2(\overline{y}) = \mathbb{F}_2(\overline{y} + 1)$, así que el argumento anterior nos vale.

5. Decide si las siguientes extensiones son normales: $\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$.

Comentario: $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ no es normal porque $x^4 - 5 \in \mathbb{Q}[x]$ es irreducible, tiene una raíz en $\mathbb{Q}(\sqrt[4]{5})$ pero no se escinde. Podemos pensar que $x^2 - 5$ se escinde en $\mathbb{Q}(\sqrt[4]{5})$, ¿Por qué esto no implica normalidad? Pues porque si bien es cierto que $x^2 - 5$ se escinde, $x^2 - 5$ también se escinde sobre $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt[4]{5})$, por lo que $\mathbb{Q}(\sqrt[4]{5})$ no es el cuerpo de escisión de $x^2 - 5$ sino $\mathbb{Q}(\sqrt{5})$.

6. Demuestra que $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión normal de $\mathbb{Q}$. Encuentra una extensión normal de $\mathbb{Q}$ que contenga a $\mathbb{Q}(\sqrt[3]{2})$ como un subcuerpo.

Solución. El polinomio irreducible $x^3 - 2 \in \mathbb{Q}[x]$ tiene una raíz en $\mathbb{Q}(\sqrt[3]{2})$ pero no se escinde porque el resto de sus raíces son complejos no reales y $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

7. Demuestra que $\mathbb{Q}(\xi)$, donde $\xi \in \mathbb{C}$ es una raíz primitiva quinta de la unidad, es una extensión normal de $\mathbb{Q}$ y calcula $\mathrm{Gal}(\mathbb{Q}(\xi))/\mathbb{Q}$. ¿Qué parte del ejercicio puedes y no puedes generalizar fácilmente considerando una raíz primitiva n-ésima de la unidad?

8. Prueba que toda extensión de grado 2 es normal.

Solución. Sea E/K de grado 2 y $a \in E \setminus K$. Como $K \subset K(a) \subseteq E$, el teorema de transitividad de grados fuerza que $K(a) = E$. Por el teorema del elemento algebraico (E/K es algebraica por ser finita) tenemos que el grado de $p = \mathrm{Irr}(K, a)$ es 2. Como $a \in E$ es raíz de p, por Ruffini $p(x) = (x - a)g(x)$ con $g \in E[x]$, ahora como p es mónico de grado 2, se tiene que $g(x) = x - b$ con $b \in E$. Por tanto, p se escinde en E y, de hecho, E es el cuerpo de escisión de p.

9. Si E/L y L/K son extensiones normales, demuestra E/K no es necesariamente normal.

Solución. Sean $E = \mathbb{Q}(\sqrt[4]{2})$, $L = \mathbb{Q}(\sqrt{2})$ y $K = \mathbb{Q}$, las extensiones E/L y L/K son normales mientras que E/K no lo es.

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

a) Sea K un cuerpo y sea $p(x) \in K[x]$. Entonces existe una extensión de K donde $p(x)$ tiene una raíz.

b) Sea K un cuerpo y $p(x) \in K[x]$. Entonces existe una extensión de K donde $p(x)$ se descompone como producto de polinomios de grado 1.

c) Supongamos que $f \in K[x]$ se escinde en $K[x]$, supongamos que $p \in K[x]$ no es constante y que p divide a f en $K[x]$. Entonces p se escinde en $K[x]$.

d) Supongamos que $K \subseteq L \subseteq E$ son extensiones de cuerpos. Sea $f \in K[x]$ no constante. Si E es cuerpo de escisión de f sobre K, entonces E es cuerpo de escisión de f sobre L.

e) Si $E = K(a_1, \ldots, a_n)$ y $\sigma \in \mathrm{Gal}(E/K)$ tal que $\sigma(a_i) = a_i$ para todo i, entonces $\sigma = 1_E$.

f) Sean E/L y L/K extensiones normales. Si todo $\sigma \in \mathrm{Gal}(L/K)$ se puede extender a un automorfismo de E, entonces E es normal sobre K.

Solución. Todas las afirmaciones son verdaderas. a) es el Teorema de Kronecker, b) es el Teorema de existencia de cuerpos de escisión, c) es el Lema 3.1(ii), c) es el Lema 3.2, d) se sigue del Teorema 3.11.d). Veamos que f) es verdadera. Podemos hacerlo de dos maneras atendiendo a las distintas caracterizaciones de normalidad que hemos visto:

- Usando el Corolario 3.12. Consideramos M la clausura normal de E/K (como E/L y L/K son normales, son finitas, en particular E/K es finita y podemos usar la construcción de la clausura normal que vimos en clase). En particular, $E \subseteq M$ y M/K es normal. Por el Corolario 3.12 basta ver que todo $\tau \in \mathrm{Gal}(M/K)$ cumple $\tau(E) = E$. Sea $\tau \in \mathrm{Gal}(M/K)$, escribimos $E_1 = \tau(E)$. Luego, $\sigma = \tau|_E \colon E \to E_1$. Escribimos también $\theta = \sigma|_L = \tau|_L$. Se tiene que $\theta \in \mathrm{Gal}(L/K)$ por ser L/K normal aplicando el Corolario 3.12. Como E/L es normal, tenemos que $E = L(f)$ con $f \in L[x]$. Si $a_1, \ldots, a_n$ son las raíces distintas de f en E entonces $E = L(a_1, \ldots, a_n)$. Ahora, sea $f_1 = \theta^*(f) \in L[x]$ (uso $\theta^* \colon L[x] \to L[x]$ inducido por θ), tenemos que

$$E_1 = \sigma(E) = \sigma(L(f)) = \sigma(L(a_1, \ldots, a_n)) = L(\sigma(a_1), \ldots, \sigma(a_n)) = L(f_1)\,.$$

En particular, E_1 es cuerpo de escisió de f_1 y las raíces de f_1 en M son $\sigma(a_1), \ldots, \sigma(a_n)$. Por otro lado, la hipótesis nos dice que θ se extiende a $\tilde{\theta} \in \mathrm{Gal}(E/K)$. Luego:

$$E = \tilde{\theta}(L(f)) = \tilde{\theta}(L(a_1, \ldots, a_n)) = L(\tilde{\theta}(a_1), \ldots, \tilde{\theta}(a_n)) = L(f_1)\,,$$

luego E es cuerpo de escisión de f_1 y $\tilde{\theta}(a_1), \ldots, \tilde{\theta}(a_n)$ son las raíces de f en M también. Por tanto

$$\{\sigma(a_1), \ldots, \sigma(a_n)\} = \{\tilde{\theta}(a_1), \ldots, \tilde{\theta}(a_n)\}$$

Luego $E = L(\tilde{\theta}(a_1), \ldots, \tilde{\theta}(a_n)) = L(\sigma(a_1), \ldots, \sigma(a_n)\} = \{\tilde{\theta}(a_1)) = E_1$.

- Usando el Teorema 3.9. Sea $f \in K[x]$ irreducible con una raíz $\alpha \in E$, queremos ver que se escinde en E (aplicando el Teorema 3.9 habríamos acabado). Si $\alpha \in L$, como L/K es normal, por el Teorema 3.9 f es escinde en $L \subseteq E$. Podemos suponer que $\alpha \notin L$ (de hecho, que f no tiene raíces en L). Si $f \in L[x]$ es irreducible, como E/L es normal, de nuevo habríamos acabado aplicando 3.9. Así que podemos considerar la descomposición de $f = p_1 \cdots p_r$ en factores irreducibles. Bien, la clave ahora es ver que $\mathrm{Gal}(L/K)$ permuta transitivamente estos factores irreducibles. Sea M el cuerpo de escisión de f sobre L, en particular, cada p_i se escinde sobre M. Además como $M = L(f)$ y, a su vez, $L = K(h)$ con $h \in K[x]$, tenemos que $M = K(f \cdot h)$ con $f \cdot h \in K[x]$. Por tanto, M/K es normal. Sea $\alpha_i \in M$ una raíz de p_i para cada i. Dado $j \neq 1$, α_1 y α_j son raíces de f que es irreducible en $K[x]$. Por tanto, existe un $\sigma_j \in \mathrm{Gal}(M/K)$ tal que $\sigma_j(\alpha_1) = \alpha_j$ por el Teorema 3.11.(e). En particular, $\sigma_j^*(p_1) = \mathrm{Irr}(K, \sigma_j(\alpha_1)) = \mathrm{Irr}(K, \alpha_j) = p_j$. Como $\sigma_j(L) = L$, por el Corolario 3.12.(a) tenemos que si $\theta_j = (\sigma_j)|_L \in \mathrm{Gal}(L/K)$, entonces $\theta_j^*(p_1) = p_j$. Como f tiene una raíz $\alpha \in E$, podemos suponer que α es raíz de p_1 y que $\alpha_1 = \alpha$. En particular, p_1 se escinde en E por

tener una raíz en E. Ahora, dado j, escogemos $\theta_j \in \mathrm{Gal}(L/K)$ tal que $\theta^*(p_1) = p_j$. Como θ_j se extiende a $\tau \in \mathrm{Gal}(E/K)$ y p_1 se escinde en E según $p_1(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_d)$, tenemos que

$$\theta_j^*(p_1(x)) = p_j(x) = \tau^*(p_1(x)) = (x-\tau(\alpha))\cdots(x-\tau(\alpha_d))\,.$$

Es decir, p_j se escinde en E. De esta forma vemos que cada factor irreducible de f se escinde en E, y, por tanto, f se escinde en E.

11. Calcula los siguientes grupos de Galois.

a) Prueba que $\mathrm{Aut}(\mathbb{Q}) = 1$ y $\mathrm{Aut}(\mathbb{R}) = \mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$.

b) Definimos $\sigma\colon \mathbb{C} \to \mathbb{C}$ como $\sigma(a+bi) = a-bi$. Prueba que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$.

Sugerencia: para el primer apartado, si $f \in \mathrm{Aut}(\mathbb{R})$ y $0 < x \in \mathbb{R}$, entonces $x = y^2$ luego $f(x) > 0$. Deduce que $x < y$ implica que $f(x) < f(y)$ y usa que entre dos números reales siempre hay un racional.

Solución. Una vez hayáis probado la sugerencia, supongamos que existe un $1 \neq f \in \mathrm{Aut}(\mathbb{R}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Entonces existe un $x \in \mathbb{R}$ tal que $f(x) \neq x$ (notad que en particular $x \notin \mathbb{Q}$) . Supongamos que $x < f(x)$ (el caso en que $f(x) < x$ es completamente análogo). Por la densidad de los racionales en $\mathbb{R}$, existe un $a \in \mathbb{Q}$ tal que $x < a \leq f(x)$ (esta segunda desigualdad también es estricta, pero no la necesitamos). Aplicando f tenemos que $f(x) < f(a) = a \leq f(x)$, una contradicción. Es fácil probar que $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Como $\mathbb{C} = \mathbb{R}(\pm i)$, siendo $\pm i$ las raíces de $x^2+1 \in \mathbb{R}[x]$ irreducible, por el Teorema 3.11(d) se tiene que $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ es isomorfo a un subgrupo de S_2, en particular, el número de elementos de G está acotado por 2, luego no hay otros elementos no triviales además de σ y $G = \{1, \sigma\}$. (Por el Corolario 3.5.7 $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = |\mathbb{C} : \mathbb{R}| = 2$.)

Bueno, una vez visto el Corolario 3.4.7, como $\mathbb{C}/\mathbb{R}$ es de Galois, sabemos que $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$. (En este caso, la cota superior dada por el Teorema 3.11(d) es muy ajustada, pero notad que a medida que el número de raíces distintas en el cuerpo de escisión aumenta, la cota se dispara, cf. con el ejercicio 7.)

12. Indica cuáles de los siguientes polinomios son separables sobre $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_5$: x^3+1, x^2+x+1, $x^4+x^3+x^2+x+1$.

Solución. Por el Corolario 3.4.2 y el Teorema 3.4.5 los polinomios son separables sobre los cuatro cuerpos. Sabiendo esto, comprueba a mano usando las definiciones que lo son (es un ejercicio muy bueno para aprehender la definición). Por ejemplo, $x^3+1 = (x+1)(x^2-x+1)$ es la descomposición en irreducibles en $\mathbb{Q}$, como $(x+1)' = 1 \neq 0$ y $(x^2-x+1) = 2x-1 \neq 0$, el polinomio es separable sobre $\mathbb{Q}$. Tenemos que $x^3 = (x+1)(x^2+x+1) \in \mathbb{F}_2[x]$ con $x+1$ y x^2+x+1 irreducibles, como sus derivadas no son nulas, x^3+1 es separable sobre $\mathbb{F}_2$, etc.

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

14. Demuestra que $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ no es separable.

15. ¿Cuántas raíces distintas tiene $x^{12}+2x^6+1 \in \mathbb{F}_3[x]$ en su cuerpo de escisión?

Solución. Notamos que $f(x) = x^{12}+2x^6+1 \in \mathbb{F}_3[x^3]$. Por el Teorema 3.4.5, como $f \in \mathbb{F}_3[x^3]$ y $\mathbb{F}_3$ es perfecto, tenemos que f es reducible. Como $2 = 2^3$ en $\mathbb{F}_3$, siguiendo la prueba de dicho teorema, tenemos que $x^{12}+2x^6+1 = (x^4)^3 + (2x^2)^2 + 1^3 = (x^4+2x^2+1)^3$. Ahora hay que decidir si $x^4+2x^2+1 \in \mathbb{F}_3$ es irreducible en $\mathbb{F}_3$ o no. Notamos que $x^4+2x^2+1 = (x^2+1)^2$, luego $f(x) = (x^2+1)^6$. Como $x^2+1 \in \mathbb{F}_3[x]$ es irreducible por no tener raíces y $(x^2+1)' \neq 0$, sabemos que tiene dos raíces distintas en su cuerpo de escisión. Luego, f tiene 2 raíces distintas en su cuerpo de escisión ambas con multiplicidad 6.

Notad que el cuerpo de escisión de f es el mismo que el cuerpo de escisión de x^2+1. El cuerpo de escisión de x^2+1 es $E = \mathbb{F}_3[x]/(x^2+1)$, ya que por Kronecker x^2+1 tiene una raíz en E, y como $E/\mathbb{F}_3$ es normal, consecuencia de la prueba del Teorema 3.5.2, x^2+1 se escinde. También lo podéis comprobar siguiendo las pautas del Ejercicio 4.

16. Construye cuerpos finitos con 8, 9, 25 y 27 elementos.

17. Prueba que para cada primo p y para cada entero positivo n, existe al menos un polinomio irreducible $f \in \mathbb{F}_p[x]$ de grado n.

Solución. Sea $K = \mathbb{F}_{p^n}$ el cuerpo de Galois de p^n elementos (también denotado usualmente por $\mathrm{GF}(p^n)$), tenemos que $K^\times$ es cíclico, sea ξ un generador de $K^\times$, en particular, $K = \mathbb{F}_p(\xi)$, como $\delta(\mathrm{Irr}(\mathbb{F}_p, \xi)) = |K : \mathbb{F}_p|$ por el Teorema del Elemento Algebraico, y $K \cong \mathbb{F}_p^m$ como espacio vectorial donde $m = |K : \mathbb{F}_p|$, concluimos (tomando cardinales) que $n = |K : \mathbb{F}_p|$, por tanto, $p = \mathrm{Irr}(\mathbb{F}_p, \xi) \in \mathbb{F}_p[x]$ es irreducible de grado n.

18. Sea $f(x) = x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$.

a) Demuestra que cualquier polinomio irreducible en $\mathbb{F}_p[x]$ de grado n divide a f.

b) Demuestra que el grado de todos los factores irreducibles de f divide a n.

Solución. a) Por el Teorema de clasificación de cuerpos finitos (Teorema 3.5.2), sea $K = \mathbb{F}_{p^n}$, sabemos que $K = F(f)$ donde $F = \mathbb{F}_p$. Por otro lado, sea $g \in F[x]$ irreducible de grado n, entonces por el Teorema de Kronecker, $F[y]/(g)$ es una extensión de grado n de F que contiene una raíz de g (concretamente $\overline{y}$ es una raíz de g). De nuevo por el teorema de clasificación de cuerpos finitos, sabemos que $K \cong F[y]/(g)$ y como $g \in F[x]$ queda fijado por tal isomorfismo, g tiene una raíz $\alpha \in K$. Como α también es raíz de f, tenemos que $x - \alpha$ divide a $\mathrm{mcd}(f, g)$. Como $f, g \in F[x]$ y g es irreducible, tenemos que $\mathrm{mcd}(f, g) > 1$ implica que g divide a f (repasad el Tema 1).

b) (Adoptamos la notación del apartado anterior.) Sea $g \in F[x]$ un factor irreducible de f con $\delta(g) = d$. Como f se escinde en K, también g se escinde en K por el lema 3.1(b). En particular, sea $\alpha \in K$ una raíz de g. Tenemos que $F(\alpha) \subseteq K$. Por el teorema del elemento algebraico (2.3) $|F(\alpha) : F| = d$, como $|K : F| = n$ el teorema de transitividad de grados implica que d es un divisor de n.

19. Responde, de manera razonada, a las siguientes preguntas:

a) Si en $\mathbb{F}_2[x]$ consideramos $f(x) = x^3 + x + 1$, demuestra que $K = \mathbb{F}_2[x]/(f)$ es un cuerpo finito y enumera sus elementos. Halla el inverso del elemento $x^2 + x + 1 + (f) \in K$. Comprueba que el grupo multiplicativo de K es cíclico, es decir, halla un generador.

b) Halla un generador del grupo multiplicativo del cuerpo $E = \mathbb{F}_3[x]/(x^2+1)$ y expresa todo elemento de $K^\times$ como potencia de dicho generador.

Solución. b) Tenemos que $E^\times = \{1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$[2], así que buscamos un elemento de orden 8 en $E^\times$. No hay un método espeífico a parte de un afortunado ensayo y error. Por ejemplo, $x^2 = 2$, $x^3 = 2x$, $x^4 = 2x^2 = 1$, así que $o(x) = 4$. Si probamos con $(x+1)^2 = x^2 + 2x + 1 = 2x$, $(x+1)^3 = 2x(x+1) = 2x^2 + 2x = 2x + 1$, $(x+1)^4 = (2x+1)(x+1) = 2x^2 + 1 = 2$ (como $(x+1)^4 \neq 1$ y los órdenes de elementos dividen el orden de $E^\times$ ya habríamos acabado, $o(x+1) = 8$) $(x+1)^5 = 2(x+1) = 2+2x$, $(x+1)^6 = 2(x+1)^2 = x$, $(x+1)^7 = x(x+1) = x^2 + x = x + 2$, $(x+1)^8 = (x+2)(x+1) = x^2 + 2 = 1$.

20. Sea E/K una extensión de grado 2. Si la característica de K no es 2, prueba que existe un $u \in E$ de modo que $E = K(u)$ y $u^2 \in K$. Muestra que la hipótesis sobre la característica es necesaria.
Sugerencia: para la segunda parte, considera el cuerpo de 4 elementos.

Solución. Sea $a \in E \setminus K$, como $K \subset K(a) \subseteq E$, por la transitividad de grados concluimos que $K(a) = E$. Ahora, sea $p = \mathrm{Irr}(K, a)$, por el teorema del elemento algebraico $\delta(p) = 2$, y tenemos que $p(x) = x^2 + b + c \in K[x]$. Como la característica de K no es 2, podemos completar cuadrados, y $p(x) = (x - b/2)^2 - b^2/4 + c \in$

[2]Como ya tenemos soltura manejando este tipo de cocientes, podemos eliminar las barras y cuando escribimos un polinomio, entendemos que estamos trabajando con la clase que define.

$K[x]$. Ahora el elemento $u = a - b/2$ es solución de $q(x) = x^2 - b^2/4 + c \in K[x]$, además $K(a) = K(a - b/2) = K(u)$ (esto implica, por cierto, que q es irreducible sobre K).

21. Sea K es un cuerpo de característica p y $a \in K$. Demuestra que el polinomio $f(x) = x^p - x + a$ o bien se se escinde en $K[x]$ o bien es irreducible.
Sugerencia: considera una raíz de f en su cuerpo de escisión y usa el pequeño teorema de Fermat para encontrar la forma del resto de raíces. Nota que $f' = -1$, así que no necesitamos que K sea perfecto para asegurar que sea separable.

Solución. Supongamos que α es una raíz de f en $E = K(f)$. Como $f'(x) = -1 \neq 0$, tenemos que $\mathrm{mcd}(f, f') = 1$ y sabemos que todas las raíces de f en E son simples (Teorema 3.5.1), por tanto, f tiene p raíces distintas. Por otro lado, si β es otra raíz de f, entonces satisface $\beta^p = \beta + a$, como $\alpha^p = \alpha + a$, se sigue que $(\beta - \alpha)^p = \beta^p - \alpha^p = \beta - \alpha$, y, por tanto, $\beta - \alpha$ es raíz de $x^p - x \in F[x]$ (siendo $F \cong \mathbb{F}_p$ el cuerpo primo de K). Ahora bien, sabemos que los ceros de $x^p - x$ son exactamente los elementos de F (por el pequeño teorema de Fermat, por ejemplo, o por ser $\mathrm{Aut}(F) = 1$). Por tanto $\beta - \alpha = b \in F$, y las raíces de f son exactamente $\alpha + b$ con $b \in F$, es decir, son

$$\alpha, \alpha + 1, \ldots, \alpha + (p - 1)\,.$$

Si $\alpha \in K$, entonces todas las raíces de f están en K y f se escinde en K. Veamos que si f no tiene una raíz en K, entonces es irreducible. Como

$$f(x) = \prod_{j=0}^{p-1} (x - (\alpha + j))\,,$$

si $f = gh$ con $g, h \in K[x]$ de grados menores que $\delta(f)$ podemos suponer sin pérdida de generalidad que $g(x) = \prod_{j=0}^{m} (x - (\alpha + j)) \in K[x]$ donde $0 < m < p - 1$. En particular, todos los coeficientes de g están en K. Si nos fijamos en el coeficiente del término x^{m-1} obtenemos que

$$\sum_{j=0}^{m} (\alpha + j) = (m + 1)\alpha + \sum_{j=0}^{m} j \in K\,.$$

Como $(m + 1), \sum_{j=0}^{m} j \in K$, concluimos que $\alpha \in K$, una contradicción.

22. Demuestra que los polinomios de Artin-Schreier $x^p - x + a$ donde p no divide a $a \in \mathbb{Z}$ son irreducibles.
Sugerencia: usa reducción de coeficientes módulo p, considera un cuerpo de escisión sobre $\mathbb{F}_p$ y el ejercicio anterior.

Ejercicios adicionales

23. Sea $f \in \mathbb{F}_p[x]$ irreducible de grado n. Entonces $\mathbb{F}_p[x]/(f)$ es el cuerpo de escisión sobre $\mathbb{F}_p$ de cualquier polinomio irreducible de grado n sobre $\mathbb{F}_p$.

24. Calcula todos los isomorfismos entre:

a) $\mathbb{F}_3[y]/(y^2 + 1)$ y $\mathbb{F}_3[t]/(t^2 + t + 2)$.

b) $\mathbb{F}_3[y]/(y^2 + 1)$ y $\mathbb{F}_2[x]/(x^3 + x + 1)$.

25. Sea $\alpha = \sqrt{1 + \sqrt{7}} \in \mathbb{R}$ y $L = \mathbb{Q}(\alpha)$.

a) Decide si $L/\mathbb{Q}$ es una extensión normal.

b) Calcula $G = \mathrm{Gal}(L/\mathbb{Q})$. ¿Coincide el orden de G con el grado de la extensión $L/\mathbb{Q}$? Usa tu respuesta para dar otra justificación del apartado **a)**.