Algunos problemas del Capítulo 3

---

32) Si hubiera una raíz repetida α entonces $x-\alpha$ dividiría a $P = x^{p^n} - x$ y a su derivada P' pero eso es imposible porque $P' = -1$.

---

33) Digamos $n = p^r$ y $\alpha^n = a \in K$, así pues α es raíz de $P = x^{p^r} - a$. Usando que la característica es p, se tiene $(x-\alpha)^n = P$, ya que $p \mid \binom{n}{j}$, $0 < j < n$. Al ser α separable, su polinomio mínimo $Q \in K[x]$, no tiene raíces múltiples y por tanto $\mathrm{mcd}(P, Q) = x - \alpha \in K[x]$ y $\alpha \in K$.

---

75) Los polinomios x^4+x^3+1 y x^2+x+1 son irreducibles en $\mathbb{F}_2[x]$, si no los cocientes no serían cuerpos. L tiene 16 elementos y K tiene 4 (el número de polinomios sobre $\mathbb{F}_2$ con grado menor que 4 y menor que 2, respectivamente). Por el teorema de clasificación de cuerpos finitos, $L \cong \mathbb{F}_{2^4}$ y $K \cong \mathbb{F}_{2^2}$. La teoría (Corolario 3.2.9) implica $\mathcal{G}(L/K) = \langle \phi^2 \rangle \cong \mathbb{Z}_2$ donde ϕ es el automorfismo de Frobenius $\phi(a) = a^2$. Para comprobar que tiene orden 4, basta ver que $\phi^4(\overline{x}) = \overline{x}$ con $\phi^2(\overline{x}) \neq \overline{x}$, donde $\overline{x}$ es la clase de x en $L = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1 \rangle$. Se tiene $\phi^2(\overline{x}) = \overline{x}^4 = \overline{1 + x^3} \neq \overline{x}$ y $\phi^4(\overline{x}) = \phi^2\big(\phi^2(\overline{x})\big) = \overline{1} + \big(\overline{1 + x^3}\big)^3 = \overline{x}^3 + \overline{x}^6 + \overline{x}^9 = \overline{x}$, donde la última igualdad se sigue de $x^9 + x^6 + x^3 = (x^4 + x^3 + 1)(x^5 + x^4 + x^3 + x) + x$ en $F_2[x]$.

---

76) Se sigue simplemente por las propiedades de cancelación de un grupo (existencia del elemento inverso). Así $\sigma^j\tau = \sigma^l\tau$ con $0 \leq l \leq j < 4$ implica $\sigma^{j-l} = \mathrm{Id}$ que lleva a una contradicción si $l \neq j$. De la misma forma, $\sigma^j = \sigma^l\tau$ lleva a $\sigma^{j-l} = \tau$ que contradice los órdenes o $\tau \neq \sigma^2$.

---

77) Empleando que las raíces son $\pm\frac{1}{2}\big(\sqrt{2} \pm \sqrt{-2}\big)$, es fácil ver que $L = \mathbb{Q}(\sqrt{-2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$. En la extensión $L/\mathbb{Q}(\sqrt{-2})$, el polinomio mínimo de $\sqrt{2}$ es $x^2 - 2$ (porque

$\sqrt{2} \notin \mathbb{Q}(\sqrt{-2})$ que se sigue de $[L:\mathbb{Q}] = 4$ o directamente). Entonces los automorfismos de $\mathcal{G}\big(L/\mathbb{Q}(\sqrt{-2})\big)$ sólo pueden actuar como $\sqrt{2} \mapsto \pm\sqrt{2}$ (permutando las raíces) y por supuesto dejando $\sqrt{-2}$ fijo. La extensión es normal finita y separable y su grado es $[L : \mathbb{Q}(\sqrt{-2})] = 2$, por consiguiente $\big|\mathcal{G}\big(L/\mathbb{Q}(\sqrt{-2})\big)\big| = 2$ y se tiene $\mathcal{G}\big(L/\mathbb{Q}(\sqrt{2})\big) = \{\mathrm{Id}, \sigma\}$ con $\sigma(\sqrt{2}) = -\sqrt{2}$ y $\sigma(\sqrt{-2}) = \sqrt{-2}$, o si se prefiere escribir así, $\sigma(\sqrt{2}) = -\sqrt{2}$ y $\sigma(i) = -i$. Un argumento similar, de hecho más sencillo, se aplica para deducir que $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2})$ es $\{\mathrm{Id}, \mathrm{conj}\}$ donde conj es la conjugación compleja habitual.

---

96) Como $\mathbb{Z}_{pq}$ es cíclico, hay exactamente un subgrupo por cada divisor del orden pq, por tanto hay cuatro, los correspondientes a 1, p, q y pq. Por ser una extensión de Galois, hay una biyección entre subcuerpos y subgrupos.

---

98) Errata en el enunciado, debería decir $[L : K] = 2$. Al estar en característica cero, la extensión E/K es separable y por ser cuerpo de descomposición es normal y finita, así pues es de Galois. Por la correspondencia de Galois, si $[L : K] = 2$, se tendría $H < A_4$ con H isomorfo a $\mathcal{G}(E/L)$. Por tanto $|H| = [E : L] = [E : K]/[L : K]$ que coincide con $\big|\mathcal{G}(E/K)\big|/2 = 6$, lo cual es imposible porque A_4 no tiene subgrupos de orden 6 (un 3-ciclo y un producto de dos trasposiciones disjuntas ya generan todo A_4).

---

99) Sabemos que $\mathbb{F}_2(\alpha) \cong \mathbb{F}_{2^4}$ porque $x^4 + x^3 + 1$ es irreducible en $\mathbb{F}_2[x]$. De la teoría también se deduce que $\mathcal{G}\big(\mathbb{F}_2(\alpha)/\mathbb{F}_2\big) = \langle\phi\rangle$ con $\phi(a) = a^2$ que debe tener orden $[\mathbb{F}_{2^4} : \mathbb{F}_2] = 4$. Por la correspondencia de Galois, debe ser $\mathbb{F}_2(\beta) = \langle\phi^2\rangle'$. Como $\langle\phi^2\rangle$ tiene orden dos, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\beta)] = 2$ y $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 2$. Basta entonces tomar un $\beta \in \mathbb{F}_2(\alpha) - \mathbb{F}_2$ que esté en el cuerpo fijo, es decir, que satisfaga $\phi^2(\beta) = \beta$. Escribamos $\beta = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3$. Aplicando ϕ^2 y empleando que $\alpha^4 = \alpha^3 + 1$ (definición de α) y por tanto $\alpha^8 = \alpha^6 + 1 = \alpha^3 + \alpha^2 + \alpha$ y $\alpha^{12} = \alpha^8\alpha^4 = \alpha + 1$, se llega a $\phi^2(\beta) = \lambda_0 + \lambda_1(\alpha^3 + 1) + \lambda_2(\alpha^3 + \alpha^2 + \alpha) + \lambda_3(\alpha + 1)$. al igualar a β se obtiene que el cuerpo fijo es $\{\lambda_0 + \lambda_1(\alpha + \alpha^3)\}$ con $\lambda_0, \lambda_1 \in \mathbb{F}_2$. Podemos tomar por ejemplo $\beta = \alpha + \alpha^3$ y ajustar los coeficientes de $P = x^2 + ax + b$ para que sea raíz de P. Se puede hacer sin cálculos, ya que la irreducibilidad implica $b \neq 0$ y $b = 1$, $a = 0$ llevaría a $\alpha + \alpha^3 = 1$, que es una contradicción, por tanto la única posibilidad es $a = b = 1$.

---

103) Perdón: En una versión anterior de esta solución estaba mal justificada la sobreyectividad. Sin suponer char$(K) = 0$ o $|K| < \infty$, uso para la separabilidad de M_3/M_1 un ejercicio que no hemos hecho. Lo siento.

Consideramos la aplicación $\mathcal{G}(M_3/M_1) \longrightarrow \mathcal{G}\big(M_2/(M_1 \cap M_2)\big)$ dada por la restricción $\sigma \mapsto \sigma|_{M_2}$. Está bien definida porque al ser M_2/K de Galois, cualquier K-automorfismo envía M_2 en sí mismo (aplica raíces en raíces y M_2 es cuerpo raíz). La aplicación es inyectiva ya que $\sigma|_{M_2} = \mathrm{Id}$ y $\sigma|_{M_1} = \mathrm{Id}$, que es obligada porque $\sigma \in \mathcal{G}(M_3/M_1)$, implica $\sigma|_{M_3} = \mathrm{Id}$. Si la aplicación no fuera sobreyectiva, la imagen sería un subgrupo propio de $\mathcal{G}\big(M_2/(M_1 \cap M_2)\big)$, que por la correspondecia de Galois daría lugar a un subcuerpo propio M de $M_2/(M_1 \cap M_2)$, que queda invariante por todos los $\sigma|_{M_2}$ con $\sigma \in \mathcal{G}(M_3/M_1)$. La extensión M_3/M_1 es de Galois (si M_1 y M_2 son cuerpos de descomposición de P_1 y P_2, M_3 lo es de P_1P_2 y es separable por el ejrcicio 35) por tanto $\mathcal{G}(M_3/M_1)' = M_1$, así pues $M \subset M_1$ y se sigue $M = M_1 \cap M_2$, lo que contradice que M sea un subcuerpo propio.

---

106) La implicación directa es obvia porque si n es cubo perfecto $[\mathbb{Q}(\sqrt[3]{n}) : \mathbb{Q}] = 1$. Para el recíproco, nótese que al ser $\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}$ de Galois, en particular normal, si $\sqrt[3]{n} \in \mathbb{Q}(e^{2\pi i/p})$, el resto de las raíces de $x^3 - n$ también estarían en $\mathbb{Q}(e^{2\pi i/p})$ y, por tanto, todo su cuerpo de descomposición L. Ahora bien, $L \subset \mathbb{Q}(e^{2\pi i/p})$, por el teorema fundamental de la teoría de Galois y el hecho de que conocemos $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}\big) \cong \mathbb{Z}_p^*$, lleva a que $\mathcal{G}\big(L/\mathbb{Q}\big)$ es isomorfo a un cociente de $\mathbb{Z}_p^*$, lo cual es una contradicción porque $\mathcal{G}\big(L/\mathbb{Q}\big)$ no es abeliano (es S_3 como en el ejemplo visto en clase, p.59).
