---

51) Resolviendo la ecuación, se tiene $K = \mathbb{Q}(\omega)$ donde $\omega = \frac{1}{2}(-1 + i\sqrt{3}) = e^{2\pi i/3}$. Claramente $[K : \mathbb{Q}] = 2$ y sabíamos que $L = \mathbb{Q}\big(\sqrt[3]{2}, \omega)$ tiene grado $[L : \mathbb{Q}] = 6$, por tanto $[L : K] = 3$. La extensión L/K es de Galois por serlo $L/\mathbb{Q}$, así pues $|\mathcal{G}(L/K)| = 3$ y la única posibilidad es $\mathcal{G}(L/K) \cong \mathbb{Z}_3$. Explícitamente $\mathcal{G}(L/K) = \{\sigma_0, \sigma_1, \sigma_2\}$ con $\sigma_j(\sqrt[3]{2}) = \omega^j \sqrt[3]{2}$, ya que los elementos de $\mathcal{G}(L/K)$ deben permutar las raíces de $x^3 - 2$. Como $L = K(\sqrt[3]{2})$ basta especificar la imagen de $\sqrt[3]{2}$.

---

58) Las raíces del polinomio son $r_1 = \sqrt{(3 + i\sqrt{7})/2}$, $r_2 = \sqrt{(3 - i\sqrt{7})/2}$, $r_3 = -r_1$ y $r_4 = -r_2$; resolviendo la ecuación bicuadrada. Notando que $r_1 r_2 = 2 \in \mathbb{Q}$ se sigue que el cuerpo de descomposición es $L = \mathbb{Q}(r_1)$. El polinomio de partida es irreducible, posiblemente la forma más rápida de verlo es que no tiene factores lineales ya que $r_1 \notin \mathbb{Q}$ y tampoco de segundo grado porque $(x - r_1)(x - r_j) \notin \mathbb{Q}[x]$ para $1 < j \le 4$. entonces $[L : \mathbb{Q}] = 4$. La extensión es por supuesto de Galois. La teoría asegura que $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ con $\sigma_j(r_1) = r_j$. Si uno quiere saber si es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ o a $\mathbb{Z}_4$ tiene que ver el orden de los automorfismos. Se tiene $\sigma_2^2(r_1) = \sigma_2(r_2) = \sigma_2(2/r_1) = 2/r_2 = r_1$. Obviamente σ_3 también tiene orden 2 (cambiar un signo), por tanto sólo puede ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ porque $\mathbb{Z}_4$ no tiene dos elementos de orden 2.

---

59) Notemos primero que $\mathbb{Q}(\sqrt{2} + i) = \mathbb{Q}(\sqrt{2}, i)$. Esto se sigue como en el segundo capítulo o se deduce del problema 81 o simplemente de $2i = \sqrt{2} + i - 3/(\sqrt{2} + i)$. Entonces el cuerpo de descomposición L contiene a $\mathbb{Q}(\sqrt{2}, i)$ pero de hecho $L = \mathbb{Q}(\sqrt{2}, i)$ porque $\big(x - (\sqrt{2} + i)\big)\big(x - (\sqrt{2} - i)\big)\big(x - (-\sqrt{2} + i)\big)\big(x - (-\sqrt{2} - i)\big) \in \mathbb{Q}[x]$. Dicho sea de paso, éste es el polinomio mínimo de α ya que es mónico de grado $[L : \mathbb{Q}] = 4$. El grupo de Galois es análogo al del segundo ejemplo de la p.55, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\}$ con σ la conjugación real $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(i) = i$ y τ la conjugación compleja habitual.

---

65) Como $\{1, \zeta, \dots, \zeta^5\}$ es una base de $\mathbb{Q}(\zeta)/\mathbb{Q}$, entonces $\{\zeta, \zeta^2, \dots, \zeta^6\}$ también lo es (la independencia lineal de uno implica la de otro y la dimensión es 6 porque el polinomio ciclotómico $x^6 + x^5 + \cdots + x + 1$ es irreducible sobre $\mathbb{Q}$). Sabemos que $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_j \ : \ 0 < j < 7\}$ con $\sigma_j(\zeta) = \zeta^j$. Por tanto hay que ver cuándo al cambiar en $\alpha = \zeta + \zeta^2 + 3\zeta^3 + \zeta^4 + 3\zeta^5 + 3\zeta^6$ cada ζ por ζ^j, la expresión permanece invariante. Obviamente, $\sigma_1(\alpha) = \alpha$, con un cálculo se comprueba que también $\sigma_2(\alpha) = \alpha$. Como al aplicar σ_3, σ_5 y σ_6, aparecen, respectivamente ζ^3, ζ^5 y ζ^6 con coeficiente 1 mientras que en α tienen coeficiente 3, no lo dejan invariante. Finalmente $\sigma_4(\alpha) = \sigma_2(\sigma_2(\alpha)) = \alpha$. En definitiva, el resultado es $\{\sigma_1, \sigma_2, \sigma_4\}$.

---

66) Este ejercicio es muy similar al anterior. Basta hallar los elementos de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ que dejan invariante a $\alpha = \zeta + \zeta^3 + \zeta^9$. En este caso $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_j \ : \ 0 < j < 13\}$ y está claro que los únicos σ_j que pueden dejar α invariante son σ_1, σ_3 y σ_9 (porque no hay otras potencias de ζ en α). Un sencillo cálculo prueba que de hecho lo hacen, así pues $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha)) = \{\sigma_1, \sigma_3, \sigma_9\}$ que es isomorfo a $\mathbb{Z}_3$.

---

74) Sin la indicación este problema no sería fácil. En primer lugar, como $\sigma(\alpha) = \alpha$ para $\alpha = \frac{1}{2} + \zeta^2 + \zeta^3$, entonces se sigue que α está realmente en el cuerpo fijo. Operando, $\alpha^2 = 1/4 + \zeta^4 + \zeta + \zeta^2 + \zeta^3 + 2$ y empleando que ζ es raíz del polinomio ciclotómico, se sigue $\alpha^2 = 5/4$. Por tanto $\mathbb{Q}(\sqrt{5}) \subset \langle\sigma\rangle'$. Por otro lado, $[\langle\sigma\rangle' : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]/|\langle\sigma\rangle| = 2$ y se sigue $\langle\sigma\rangle' = \mathbb{Q}(\sqrt{5})$. *Nota*: Gauss probó que $\mathbb{Q}(\sqrt{p})$ es siempre un subcuerpo de $\mathbb{Q}(e^{2\pi i/p})$, el único de grado 2 sobre $\mathbb{Q}$. La demostración es, como en este caso, sencilla una vez que uno sabe qué hay que elevar al cuadrado.

---

89) el polinomio se escribe como $(x^2 + 3)(x^3 - 3)$ y de ahí es fácil ver que el cuerpo de descomposición es $L = \mathbb{Q}(\sqrt[3]{3}, \omega)$ con $\omega = e^{2\pi i/3}$. Como en el ejemplo de la p.59, $\mathcal{G}(L/\mathbb{Q}) \cong S_3$ y por la correspondencia de Galois basta contar el número de subgrupos de S_3. Con orden 2, están los subgrupos generados por las 3 trasposiciones y con orden 3, los dos 3-ciclos, $(1, 2, 3)$, $(1, 3, 2)$, están en el mismo subgrupo. Por consiguiente hay cuatro subgrupos propios y seis en total.
