Prob. 16.9.2, Artin (2nda edición)

El problema. Sea $K = \mathbb{Q}(\alpha, \alpha') \subset \mathbb{R}$, donde $\alpha := \sqrt{4+\sqrt{5}}, \alpha' := \sqrt{4-\sqrt{5}}$. Encontrar todas las "raices cuadradas anidadas" en K; o sea, números en K de la forma $\pm\sqrt{a+b\sqrt{c}}$, con $a, b, c \in \mathbb{Q}$.

Solución. Primero caracterizamos a las RCAs (=raíces cuadradas anidadas) usando la teoría de campos. Toda RCA γ genera extensiones $\mathbb{Q} \subset \mathbb{Q}(\gamma^2) \subset \mathbb{Q}(\gamma)$, en donde cada paso es claramente de grado ≤ 2, así que γ es de grado 1,2 o 4 sobre $\mathbb{Q}$. Es fácil ver que las RCA de grado ≤ 2 son los números algebráicos de grado ≤ 2: si $\gamma = a + b\sqrt{c}$, con $a, b, c \in \mathbb{Q}$, entonces $\gamma = \pm\sqrt{\gamma^2} = \pm\sqrt{u + v\sqrt{c}}$, con $u = a^2 + b^2 c, v = 2ab$. Así que las RCAs de grado ≤ 2 en K están dadas por los subcampos $L \subset K$ de grado $[L : \mathbb{Q}] \leq 2$.

Para las RCA de grado 4 observamos que ambas extensiones, $\mathbb{Q} \subset \mathbb{Q}(\gamma^2)$ y $\mathbb{Q}(\gamma^2) \subset \mathbb{Q}(\gamma)$ son cuadráticas, así que buscamos subcampos $L' \subset L \subset K$ con $[L : L'] = [L' : \mathbb{Q}] = 2$ y elementos $\gamma \in L$ de grado 4 tal que $\gamma^2 \in L'$.

En nuestro caso, como K es un campo de descomposición, la extensión $K/\mathbb{Q}$ es de Galois, por lo que los subcampos de K son los subcampos fijos por subgrupos de $G := \mathrm{Aut}(K)$. En Ejemplo 16.9.2(a) fue demostrado que $[K : \mathbb{Q}] = 8$ y que la acción de G en las 4 raices del polinomio irreducible de α define un ismorfismo $G \simeq D_4 = \langle (1234), (24) \rangle \subset S_4$, con $\alpha_1 = \alpha, \alpha_2 = \alpha', \alpha_3 := -\alpha, \alpha_4 := -\alpha'$. Cada subcampo $L' \subset K$ con $[L' : \mathbb{Q}] = 2$ es el campo fijo $L' = K^{H'} = \mathbb{Q}(\eta)$ de un subgrupo $H' \subset G$ de orden 4, generado por un elemento $\eta \in K$ de grado 2 sobre $\mathbb{Q}$ fijo por H'. Los 3 subgrupos de G de orden 4 y los elementos fijos asociados son:

- $\langle (1234) \rangle = \{e, (1234), (13)(24), (4321)\} \simeq C_4$ deja fijo a $\alpha\alpha'(\alpha^2 - \alpha'^2)/2 = \sqrt{55}$.
- $\langle (13), (24) \rangle = \{e, (13), (24), (13)(24)\} \simeq D_2$ deja fijo a $(\alpha^2 - \alpha'^2)/2 = \sqrt{5}$.
- $\langle (12)(34), (13)(24) \rangle = \{e, (12)(34), (13)(24), (14)(23)\} \simeq D_2$ deja fijo a $(\alpha + \alpha')^2 - 8 = \sqrt{11}$.

Así que las RCAs en K de grado ≤ 2 son los números de la forma $a + b\sqrt{n}$, con $a, b \in \mathbb{Q}$, $n \in \{5, 11, 55\}$.

Para encontrar las RCA en K de grado 4 determinamos primero los subcampos $L \subset K$ de grado 4 como los campos fijos $L = K^\sigma$ por cada uno de los 5 elementos $\sigma \in G$ de orden 2, y luego las RCA $\gamma \in L$:

- (24) deja fijo a $\alpha \implies K^{(24)} = \mathbb{Q}(\alpha)$. El único subcampo de $\mathbb{Q}(\alpha)$ de índice 2 es $\mathbb{Q}(\sqrt{5})$, el campo fijo de $\langle (13), (24) \rangle$, ya que $\langle (13), (24) \rangle$ es el único subgrupo de G de orden 4 que contiene a (24). Si $\gamma = c + d\alpha \in \mathbb{Q}(\alpha)$, con $c, d \in \mathbb{Q}(\sqrt{5}) \implies \gamma^2 = c^2 + d^2\alpha^2 + 2cd\alpha \in \mathbb{Q}(\sqrt{5})$ ssi $cd = 0$, o sea $\gamma \in \mathbb{Q}(\sqrt{5})$ o $\gamma = d\alpha$. Los siguientes 3 casos son muy similares.
- (13) deja fijo a $\alpha' \implies K^{(13)} = \mathbb{Q}(\alpha')$. Luego $\gamma \in \mathbb{Q}(\alpha')$ es una RCA ssi $\gamma^2 \in \mathbb{Q}(\sqrt{5})$ o $\gamma = d\alpha'$, $d \in \mathbb{Q}(\sqrt{5})$.
- $(12)(34)$ deja fijo a $\beta := \alpha + \alpha' = \sqrt{8 + 2\sqrt{11}} \implies K^{(12)(34)} = \mathbb{Q}(\beta)$. Luego $\gamma \in \mathbb{Q}(\beta)$ es una RCA ssi $\gamma^2 \in \mathbb{Q}(\sqrt{11})$ o $\gamma = d\beta$, $d \in \mathbb{Q}(\sqrt{11})$.
- $(14)(23)$ deja fijo a $\beta' := \alpha - \alpha' = \sqrt{8 - 2\sqrt{11}} \implies K^{(14)(23)} = \mathbb{Q}(\beta')$. Luego $\gamma \in \mathbb{Q}(\beta')$ es una RCA ssi $\gamma^2 \in \mathbb{Q}(\sqrt{11})$ o $\gamma = d\beta'$, $d \in \mathbb{Q}(\sqrt{11})$.
- $(13)(24)$ deja fijos a $\alpha^2 = 4 + \sqrt{5}, \alpha\alpha' = \sqrt{11} \implies K^{(13)(24)} = \mathbb{Q}(\sqrt{5}, \sqrt{11})$. Tiene 3 subcampos de índice 2: $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{11}), \mathbb{Q}(\sqrt{55})$. Buscamos primero los RCAs $\gamma \in \mathbb{Q}(\sqrt{5}, \sqrt{11})$ tal que $\gamma^2 \in \mathbb{Q}(\sqrt{5})$. Escribiendo $\gamma = c + d\sqrt{11}$, con $c, d \in \mathbb{Q}(\sqrt{5})$, $\gamma^2 = c^2 + 11d^2 + 2cd\sqrt{11} \in \mathbb{Q}(\sqrt{5})$ ssi $cd = 0$. Luego $c = 0$ ssi $\gamma \in \mathbb{Q}\sqrt{11} + \mathbb{Q}\sqrt{55}$ y $d = 0$ ssi $\gamma \in \mathbb{Q}(\sqrt{5}) = \mathbb{Q} + \mathbb{Q}\sqrt{5}$. De manera similar analizamos los otros dos casos de $\gamma^2 \in \mathbb{Q}(\sqrt{11})$ y $\gamma^2 \in \mathbb{Q}(\sqrt{55})$.

Resumen. Las RCAs en K son números de la forma $(a + b\sqrt{5})\sqrt{4 \pm \sqrt{5}}$, $(a + b\sqrt{11})\sqrt{8 \pm 2\sqrt{11}}$, $a, b \in \mathbb{Q}$, o una combinación lineal con coeficiente racionales de dos elementos de $\{1, \sqrt{5}, \sqrt{11}, \sqrt{55}\}$.

Nota. Las RCA en K del último tipo son distintos de los otros 4 tipos en que se les puede "desanidar". Ver el Teorema 1 del artículo de Susan Landau. □