Example. Let $\mathbf{K}$ be a field of characteristic not dividing n. Let $a \in \mathbf{K}^*$ and let ξ denote a primitive n^{th} root of 1. Then
(1) $\mathbf{L} = \mathbf{K}(\xi, \sqrt[n]{a})$ is a Galois extension of $\mathbf{K}$.
(2) There is an injective homomorphism

$$F\colon Aut_{\mathbf{K}}(\mathbf{L}) \to G := \{\begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix},\ i \in \mathbf{Z}_n^*,\ j \in \mathbf{Z}_n\}.$$

(3) The group G is solvable. Therefore $Aut_{\mathbf{K}}(\mathbf{L})$ is solvable too.

Proof. (1) The field $\mathbf{L}$ is the splitting field of the polynomial $f = x^n - a$. If $char(\mathbf{K}) = 0$, this is already sufficient to conclude that $\mathbf{K} \subset \mathbf{L}$ is a Galois extension. Assume now that $char(\mathbf{K}) = p$ and that p does not divide n. The extension $\mathbf{K} \subset \mathbf{L}$ is finite and normal. In order to show that it is Galois, we need to check that it is separable. The zeros of f are $\{\sqrt[n]{a}\,\xi^j,\ j \in \mathbf{Z}_n\}$. Since p does not divide n, one has $f' = nx^{n-1} \not\equiv 0$ and $\gcd(f, f') = 1$. In particular all the zeros of f are distinct. Observe that the minimal polynomial of ξ divides $x^n - 1$ while the one of $\sqrt[n]{a}$ divides $x^n - a$. Hence they are separable polynomials, implying that ξ and $\sqrt[n]{a}$ are separable elements. Then, by Garling, Cor.2, page. 84, $\mathbf{L}$ is a separable extension of $\mathbf{K}$.
(b) An element $\sigma \in Aut_{\mathbf{K}}(\mathbf{L})$ is determined by $\sigma(\xi) = \xi^i$, with $i \in \mathbf{Z}_n^*$ and $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\xi^j$, with $j \in \mathbf{Z}_n$. So we define the map F by

$$F(\sigma) := \begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix},\ i \in \mathbf{Z}_n^*,\ j \in \mathbf{Z}_n.$$

- F is a homomorphism: given automorphisms σ_1, determined by $\sigma_1(\xi) = \xi^{i_1}$ and $\sigma_1(\sqrt[n]{a}) = \sqrt[n]{a}\,\xi^{j_1}$, and σ_2, determined by $\sigma_2(\xi) = \xi^{i_2}$ and $\sigma_2(\sqrt[n]{a}) = \sqrt[n]{a}\,\xi^{j_2}$, the composition $\sigma_2 \circ \sigma_1$ is determined by

$$\sigma_2 \circ \sigma_1(\xi) = \xi^{i_1 i_2}, \qquad \sigma_2 \circ \sigma_1(\sqrt[n]{a}) = \sigma_2(\sqrt[n]{a}\,\xi^{j_1}) = \sqrt[n]{a}\,\xi^{j_2 + j_1 i_2}.$$

Now it is clear that

$$F(\sigma_2 \circ \sigma_1) = \begin{pmatrix} i_1 i_2 & j_2 + j_1 i_2 \\ 0 & 1 \end{pmatrix} = f(\sigma_2) F(\sigma_1) = \begin{pmatrix} i_2 & j_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i_1 & j_1 \\ 0 & 1 \end{pmatrix}.$$

Note that $\gcd(i_1 i_2, n) = 1$.
- $\ker(F) = \{id\}$: in fact $F(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ if and only if $\sigma(\xi) = \xi$ and $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$, if and only if $\sigma = id$.
- the image of $Aut_{\mathbf{K}}(\mathbf{L})$ in G depends on the field $\mathbf{K}$.
(c) The determinant $\det\colon G \to \mathbf{Z}_n^*$ is a surjective homomorphism with kernel the abelian normal subgroup of G

$$H := \{\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix},\ j \in \mathbf{Z}_n.$$

In particular, $G/H \cong \mathbf{Z}_n^*$ is abelian. This proves that G is solvable. It also implies that $Aut_{\mathbf{K}}(\mathbf{L})$, which isomorphic to a subgroup of G, is solvable. □

Example. Let $\mathbf{L} = \mathbf{K}(\sqrt[4]{2}, \xi_4) = \mathbf{K}(\sqrt[4]{2}, \sqrt{-1})$ be the splitting field of $f = X^4 - 2$ over $\mathbf{K}$. Let's observe how the image of $Aut_{\mathbf{K}}(\mathbf{L})$ in G changes varying the field $\mathbf{K}$.
(a) $\mathbf{K} = \mathbf{Q}$, $\mathbf{L} = \mathbf{Q}(\sqrt[4]{2}, \sqrt{-1})$, $[\mathbf{L} : \mathbf{K}] = 8$, $F(Aut_{\mathbf{K}}(\mathbf{L})) = G$;
(b) $\mathbf{K} = \mathbf{R}$, $\mathbf{L} = \mathbf{C}$, $[\mathbf{L} : \mathbf{K}] = 2$, $F(Aut_{\mathbf{K}}(\mathbf{L})) = \{\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix},\ i \in \mathbf{Z}_4^*\} \cong \mathbf{Z}_2$;

(c) $\mathbf{K}=\mathbf{C}, \quad \mathbf{L}=\mathbf{C} \quad [\mathbf{L}:\mathbf{K}]=1, \quad F(Aut_{\mathbf{K}}(\mathbf{L}))=\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\}$;

(d) $\mathbf{K}=\mathbf{Q}(\sqrt{2}), \quad \mathbf{L}=\mathbf{Q}(\sqrt{2})(\sqrt{\sqrt{2}}, \sqrt{-1}) \quad [\mathbf{L}:\mathbf{K}]=4$,

$$F(Aut_{\mathbf{K}}(\mathbf{L}))=\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 2\\ 0 & 1\end{pmatrix}\}.$$

Solving polynomial equations by radicals.

We briefly discussed an old question answered by Galois theory:

Given a polynomial $f \in \mathbf{Q}[x]$ of degree n, is it always possible to express the solutions of the equation $f = 0$ as radical functions of the coefficients of f?

When this is the case, we call f solvable. Every polynomial of degree $n = 2, 3, 4$ is solvable, by the well known formulas. Around 1800, "using Galois theory" it was proved that similar formulas do not exist in general for $n \geqslant 5$.

Given a polynomial $f \in \mathbf{Q}[x]$, denote by G_f the Galois group of its splitting field $\mathbf{K}_f$. Then f *is solvable if and only if the group G_f is solvable in the sense of group theory.*

The symmetric group $\mathcal{S}_n$ is not solvable, for $n \geqslant 5$. Hence any polynomial f with with Galois group $G_f = \mathcal{S}_n$ is not solvable. A random polynomial f has most probably Galois group $G_f = \mathcal{S}_n$.