Example 1. *Let $\mathbf{Q}_f$ be the splitting field of the polynomial $f(x) = x^3 - 2$. Then $Aut_{\mathbf{Q}}(\mathbf{Q}_f) \cong S_3$, the permutation group of 3 elements.*

Sol.: Recall that $\mathbf{Q}_f = \mathbf{Q}(\sqrt[3]{2}, \xi)$, where ξ is a 3^{rd} primitive root of 1, and that $[\mathbf{Q}_f : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}][\mathbf{Q}(\sqrt[3]{2})(\xi) : \mathbf{Q}(\sqrt[3]{2})] = 6$. Recall also that $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) \subset S_3$. We first show that $\#\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) = 6$ by exhibiting an element ϕ of order 3 and an element ψ of order 2 in $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$. Then from the conditions $\#\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) \leqslant 6$, $2, 3 \mid \#\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$ it follows that $\#\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) = 6$. Since $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) \subset S_3$, we conclude that $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f) \cong S_3$.

Consider the extensions $\mathbf{Q} \subset \mathbf{Q}(\xi) \subset \mathbf{Q}_f$ and the subgroup $\mathrm{Aut}_{\mathbf{Q}(\xi)}(\mathbf{Q}_f) \subset \mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$ consisting of the automorphisms of $\mathbf{Q}_f$, fixing $\mathbf{Q}(\xi)$. We have

$$\mathrm{Aut}_{\mathbf{Q}(\xi)}(\mathbf{Q}_f) = \mathrm{Hom}_{\mathbf{Q}(\xi)}(\mathbf{Q}_f, \mathbf{Q}_f)$$

and the above set is in 1-1 correspondence with

$$Z(x^2 - 2) \cap \mathbf{Q}_f = \{\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2\}.$$

The automorphism determined by the condition $\phi(\sqrt[3]{2}) = \sqrt[3]{2}\xi$ is an element of order 3 of $\mathrm{Aut}_{\mathbf{Q}(\xi)}(\mathbf{Q}_f)$ and therefore of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$.

Consider now the extensions $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{Q}_f$ and the subgroup $\mathrm{Aut}_{\mathbf{Q}(\sqrt[3]{2})}(\mathbf{Q}_f)$ of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$ consisting of the automorphisms of $\mathbf{Q}_f$, fixing $\mathbf{Q}(\sqrt[3]{2})$. We have

$$\mathrm{Aut}_{\mathbf{Q}(\sqrt[3]{2})}(\mathbf{Q}_f) = \mathrm{Hom}_{\mathbf{Q}(\sqrt[3]{2})}(\mathbf{Q}_f, \mathbf{Q}_f)$$

and the above set is in 1-1 correspondence with

$$Z(x^2 + x + 1) \cap \mathbf{Q}_f = \{\xi, \xi^2\}.$$

The automorphism determined by the condition $\psi(\xi) = \xi^2$ is an element of order 2 of $\mathrm{Aut}_{\mathbf{Q}(\sqrt[3]{2})}(\mathbf{Q}_f)$ and therefore of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}_f)$.

One can also proceed as follows. Consider the extensions $\mathbf{Q} \subset \mathbf{Q}(\xi) \subset \mathbf{Q}_f$.
$\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$ consists of two elements: the identity and the automorphism of order 2 determined by $\phi(\xi) = \xi^2$. The cardinality of

$$\mathrm{Aut}_{\mathbf{Q}(\xi)}(\mathbf{Q}(\sqrt[3]{2}, \xi)) = \mathrm{Hom}_{\mathbf{Q}(\xi)}(\mathbf{Q}(\sqrt[3]{2}, \xi), \mathbf{Q}(\sqrt[3]{2}, \xi))$$

tells in how many ways an element $\phi \in \mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$ can be extended to an automorphism in $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \xi))$. Such cardinality is equal to 3, as $x^3 - 2$ is the minimum polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}(\xi)$. The polynomial $x^3 - 2$ is indeed it is irreducible over $\mathbf{Q}(\xi)$, because otherwise it would define a degree 3 extension of $\mathbf{Q}$ inside $\mathbf{Q}(\xi)$. Absurd.

Excercise Determine all automorphisms $\phi \in \mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}, \xi))$ specifying the images of each element of the $\mathbf{Q}$-basis of $\mathbf{Q}(\sqrt[3]{2}, \xi)$ given by $1, \xi, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt[3]{2}\xi, (\sqrt[3]{2})^2\xi$.

Example 2. *Let ξ be a primitive 8^{th} root of 1. Then $Aut_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong V_4$, the Klein group with 4 elements.*

Sol.: Set $\xi = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. The field $\mathbf{Q}(\xi)$ is a degree 4 extension of $\mathbf{Q}$: the polynomial $x^8 - 1$ factors as $x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$ and ξ is a zero of the irreducible factor $f(x) = x^4 + 1$, which is its minimum polynomial.

One has

$$\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) = \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\xi), \mathbf{Q}(\xi)),$$

and the above set is in 1-1 correspondence with

$$Z(x^4 + 1) \cap \mathbf{Q}(\xi) = \{\xi,\ \xi^3,\ \xi^5,\ \xi^7\},$$

which are the zeros of x^4+1 contained in $\mathbf{Q}(\xi)$. To each zero, there corresponds an element of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$, determined by
$\phi_1(\xi)=\xi$ (the identity automorphism),
$\phi_3(\xi)=\xi^3$,
$\phi_5(\xi)=\xi^5$,
$\phi_7(\xi)=\xi^7$, respectively.

All the above automorphisms, different from the identity, have order 2: as they are completely determined by the image of ξ, it is sufficient to verify that $\phi_i\circ\phi_i=Id$, for $i=3,5,7$. Indeed, using the relation $\xi^8=1$, we find
$\phi_3(\phi_3(\xi))=\phi_3(\xi^3))=\xi^9=\xi$,
$\phi_5(\phi_5(\xi))=\phi_5(\xi^5))=\xi^{25}=\xi$,
$\phi_7(\phi_7(\xi))=\phi_7(\xi^7))=\xi^{49}=\xi$.

It follows that as a group $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$ is isomorphic to the Klein group with 4 elements V_4. In particular it contains 3 subgroups with 2 elements, generated by ϕ_3, ϕ_5, ϕ_7, respectively.

Remark. (a) The field $\mathbf{Q}(\xi)$ contains $\mathbf{Q}(\sqrt{2})$ as a subfield. It is obtained as

$$\mathbf{Q}(\sqrt{2})=\mathbf{Q}(\xi+\xi^7)=\mathbf{Q}(\xi^3+\xi^5).$$

(b) One can verify that the subfield $\mathbf{Q}(\sqrt{2})$ is the fixed subfield of the subgroup generated by $\phi_7(\xi)=\xi^7=\bar{\xi}$.

(c) Consider now the subgroup generated by ϕ_3 and compute its fixed subfield:
let $Z=x+y\xi+z\xi^2+u\xi^3$, with $x,y,z,u\in\mathbf{Q}$, be an element in $\mathbf{Q}(\xi)$.
One has $\phi_3(x+y\xi+z\xi^2+u\xi^3)=x+y\xi^3+z\xi^6+u\xi^9=x+u\xi-z\xi^2+y\xi^3$. Hence $\phi_3(Z)=Z$ if an only if $y=u$ and $z=0$. in other words $Z=x+y(\xi+\xi^3)=x+i\sqrt{2}y\in\mathbf{Q}(i\sqrt{2})$.

(d) Consider now the subgroup generated by ϕ_5 and compute its fixed subfield:
$\phi_5(Z)=Z$ if an only if $y=u=0$ and $Z=x+z\xi^2=x+iz\in\mathbf{Q}(i)$.

Conclusion: $\mathbf{Q}(\xi)$ contains 3 quadratic subfields

$$\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset\mathbf{Q}(\xi),\quad \mathbf{Q}\subset\mathbf{Q}(i\sqrt{2})\subset\mathbf{Q}(\xi),\quad \mathbf{Q}\subset\mathbf{Q}(i)\subset\mathbf{Q}(\xi).$$

Excercise. (a) Check that X^4+1 is irreducible over $\mathbf{Q}$.
(b) Exhibit a basis of the $\mathbf{Q}$-vector space $\mathbf{Q}(\xi)$.
(c) In that basis, determine the representative matrix of $\phi_3\colon\mathbf{Q}(\xi)\to\mathbf{Q}(\xi)$, viewed as a $\mathbf{Q}$-linear map.
(d) What does the automorphism ϕ_5 do on the subfield $\mathbf{Q}(\sqrt{2})$?