Example 1. *Let ξ be a primitive 7^{th} root of 1. Then $Aut_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong (\mathbf{Z}/7\mathbf{Z})^*$, a cyclic group of 6 elements.*

Sol.: Fix $\xi = e^{2\pi i/7}$, a primitive 7^{th} root of 1. The polynomial $x^7 - 1$ factors as $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ and ξ is a zero of the irreducible factor $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Hence f is the minimum polynomial of ξ and the field $\mathbf{Q}(\xi)$ is a degree 6 extension of $\mathbf{Q}$.

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 the zeros of $x^6+x^5+x^4+x^3+x^2+x+1$ contained in $\mathbf{Q}(\xi)$

$$Z(f) \cap \mathbf{Q}(\xi) = \{\xi,\ \xi^2,\ \xi^3,\ \xi^4,\ \xi^5,\ \xi^6\}.$$

To each zero, there corresponds an element of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$, determined by $\phi_j(\xi) = \xi^j$, for $j = 1, \ldots, 6$. The identity automorphism corresponds to $j = 1$. More precisely, there is a group isomorphism

$$\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) \to (\mathbf{Z}/7\mathbf{Z})^*, \quad \phi_j \mapsto j.$$

The group $(\mathbf{Z}/7\mathbf{Z})^*$ is cyclic group of order 6: it contains as subgroup $G = \{Id,\ \phi_6\} \cong \mathbf{Z}/2\mathbf{Z}$ and a subgroup $H = \{Id,\ \phi_4,\ \phi_4 \circ \phi_4\} \cong \mathbf{Z}/3\mathbf{Z}$.

Now we compute the fixed subfields of the groups G and H.

• $\mathbf{Q}(\xi)^G$:

As $\#G = 2$, one has $[\mathbf{Q}(\xi) : \mathbf{Q}(\xi)^G] = 2$ and therefore $[\mathbf{Q}(\xi)^G : \mathbf{Q}] = 3$.

Observe that $\phi_6(\xi) = \xi^6 = \bar{\xi}$. Then for $\alpha = \xi + \bar{\xi} = 2\cos(2\pi/7)$, we have inclusions $\mathbf{Q} \subset \mathbf{Q}(\alpha) \subset \mathbf{Q}(\xi)^G$.

Since $\alpha \notin \mathbf{Q}$ and the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ divides the degree $[\mathbf{Q}(\xi)^G : \mathbf{Q}]$, then necessarily $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$ and $\mathbf{Q}(\alpha) = \mathbf{Q}(\xi)^G$.

With the same reasoning, one obtains $\mathbf{Q}(\xi)^G = \mathbf{Q}(\beta) = \mathbf{Q}(\gamma)$, for $\beta = \xi^2 + \bar{\xi}^2$ and $\gamma = \xi^3 + \bar{\xi}^3$:

• $\mathbf{Q}(\xi)^H$:

As $\#G = 3$, one has $[\mathbf{Q}(\xi) : \mathbf{Q}(\xi)^G] = 3$ and therefore $[\mathbf{Q}(\xi)^G : \mathbf{Q}] = 2$.

Excercise. (a) Check that $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbf{Q}$. (use the substitution $x = y + 1$ etc...)

(b) Exhibit a basis of the $\mathbf{Q}$-vector space $\mathbf{Q}(\xi)$.