Suppose that an irreducible $p(x) \in Q[x]$ of degree $n$ has complex roots $\alpha_1, \ldots, \alpha_n$ and we set $K = Q(\alpha_1, \ldots, \alpha_n)$. Each $\sigma \in \Gamma[K : Q]$ permutes the roots though not every permutation of the roots yields an automorphism $\sigma$.

Suppose $\rho$ is a polynomial function of $\alpha_1, \ldots, \alpha_n$ which is symmetric. Then every $\sigma \in \Gamma[K : Q]$ has $\sigma(\rho) = \rho$. Hence $\rho \in Q$. As an example suppose a cubic $p(x) \in Q[x]$ has roots $\alpha, \beta, \gamma$ and let

$$\rho = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$$

(1)

Any permutation of $\alpha, \beta, \gamma$ fixes $\rho$ and hence $\rho$ is a rational number. (FYI: this is called the discriminant and generalizes the famous $b^2 - 4ac$ term with quadratics.)

When $\rho$ is not fully symmetric in $\alpha_1, \ldots, \alpha_n$ there is still some information to be gleaned. Suppose $\kappa$ is fixed by the alternating group, the even permutations of $\alpha_1, \ldots, \alpha_n$. If $\Gamma[K : Q]$ is contained in the alternating group then $\kappa \in Q$ as before. Otherwise, $\Gamma[K : Q]$ would have more than $n!/2$ elements and so would be the full symmetric group of $\alpha_1, \ldots, \alpha_n$. In that case $\kappa$ would not be in $Q$ since it isn’t fixed by all $\sigma \in \Gamma[K : Q]$. Letting $H$ be the alternating group, as $|H| = |G|/2$, $[H^1 : Q] = 2$. Then $\kappa$ would be in a quadratic extension of $Q$. Continuing the cubic example above, now set

$$\kappa = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$$

(2)

Assume $\Gamma[K : Q] \cong S_3$. Of the six permutations of $\alpha, \beta, \gamma$, three send $\kappa$ to itself and the other three send $\kappa$ to $-\kappa$ (which is not $\kappa$ as $\kappa \neq 0$ as $\alpha, \beta, \gamma$ are distinct). (For example, if $\alpha, \beta$ are flipped and $\gamma$ stays where it is then $\kappa$ goes to $-\kappa$ but if $\alpha$ goes to $\beta$ which goes to $\gamma$ which goes to $\alpha$ then $\kappa$ goes to $\kappa$.) Then $[Q(\kappa) : Q] = 2$ so $\kappa$ can be expressed in terms of a square root. Since, further, $\kappa^2 = \rho \in Q$, $\kappa$ will be the square root of a rational number.