15. Automorphisms of splitting fields – orbits

Problem 15.1. Let $F \subseteq K$ be fields, let ρ in K be algebraic over F and let $m(x)$ be its minimal polynomial. Let $\{\rho_1, \rho_2, \ldots, \rho_r\}$ be the roots of $m(x)$ in K.

(1) Show that the $\mathrm{Aut}(K/F)$ orbit of ρ is a subset of $\{\rho_1, \ldots, \rho_r\}$.
(2) Show that the stabilizer of ρ is $\mathrm{Aut}(K/F[\rho])$.

As the next example shows, the orbit of ρ can be smaller than $\{\rho_1, \ldots, \rho_r\}$.

Problem 15.2. Let $K = \mathbb{Q}(\sqrt[4]{2})$.

(1) Show that the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.
(2) Show that $x^2 - 2$ splits in K.
(3) Show that $\sqrt{2}$ and $-\sqrt{2}$ are separate in orbits for $\mathrm{Aut}(K/\mathbb{Q})$.

We can do much better when our big field is a splitting field. Here is our goal for today:

Theorem: Let F be a field, let $f(x)$ be a nonzero polynomial in $F[x]$ and let L be a splitting field for $f(x)$. Let ρ be any element of L and let $m(x)$ be the minimal polynomial of ρ over F. Then $m(x)$ splits in $L[x]$, and the $\mathrm{Aut}(L/F)$ orbit of ρ is the set of roots of $m(x)$.

We will want the following lemma:

Problem 15.3. Let $F \subseteq L \subseteq M$ be a chain of fields, where L is a splitting field for some polynomial $f(x)$ in $F[x]$. Let ψ be in $\mathrm{Aut}(M/F)$. Then ψ maps L to itself.

We also need a minor variant of Problem 13.6:

Problem 15.4. Let F be a field, let $f(x)$ be a nonzero polynomial in $F[x]$ and let L be a splitting field for $f(x)$. Let K_1 and K_2 be two fields with $F \subseteq K_1 \subseteq L$ and $F \subseteq K_2 \subseteq L$. Suppose that there is an isomorphism $\phi : K_1 \to K_2$ such that ϕ stabilizes every element of F. Show that there is an automorphism ψ of L making the following diagram commute:

$$\begin{array}{ccccc} F & \subseteq & K_1 & \subseteq & L \\ \| & & \downarrow \phi & & \vdots \psi \\ F & \subseteq & K_2 & \subseteq & L \end{array}$$

We now begin proving the Theorem:

Problem 15.5. With notation as in the Theorem, let ρ_1 and ρ_2 be two roots of $m(x)$ in L. Show that there is some ψ in $\mathrm{Aut}(L/F)$ with $\psi(\rho_1) = \rho_2$.

So we now know that all the roots of $m(x)$ are in the same orbit, but we still need to see that $m(x)$ splits in L. To this end, let M be a splitting field for $f(x)m(x)$. As in Problem 13.8, we can think of L as a subfield of M, so we have a chain $F \subseteq L \subseteq M$. So ρ is in L, but the other roots of $m(x)$ are only, a priori, in M.

Problem 15.6. Let ρ' be any root of $m(x)$ in M.

(1) Show that there is an automorphism ψ in $\mathrm{Aut}(M/F)$ with $\psi(\rho) = \rho'$.
(2) Show that ρ' is in L, as required.