22. GALOIS EXTENSIONS

Problem 22.1. Let $K \subseteq L$ be a field extension of finite degree. Let $\theta \in L$ and let $g(x)$ be the minimal polynomial of θ over K.

(1) Show that the size of the $\mathrm{Aut}(L/K)$ orbit of θ is $\leq [K[\theta] : K]$.
(2) Show that we have equality if and only if g is separable and g splits in L.

Problem 22.2. Let $K \subseteq L$ be a field extension of finite degree. Show that $\#\,\mathrm{Aut}(L/K) \leq [L : K]$.

It is natural to ask when we have equality in Problem 22.2. This is answered by the following:

Theorem/Definition Let L/K be a field extension of finite degree. The following are equivalent:

(1) We have $\#\,\mathrm{Aut}(L/K) = [L : K]$.
(2) The fixed field of $\mathrm{Aut}(L/K)$ is K.
(3) For every $\theta \in L$, the minimal polynomial of θ over K is separable and splits in L.
(4) L is the splitting field of a separable polynomial $f(x) \in K[x]$.

A field extension L/K which satisfies these equivalent definitions is called ***Galois***.

The next four problems prove this theorem.

Problem 22.3. Show that (1) implies (2).

Problem 22.4. Let $\theta \in L$ and let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be the orbit of θ under $\mathrm{Aut}(L/K)$. Let $f(x) = \prod_j (x - \theta_j)$.

(1) Assuming condition (2), Show that $f(x) \in K[x]$.
(2) Continuing to assume (2), show that $f(x)$ is the minimal polynomial of θ over K.
(3) Deduce that (2) implies (3).

Remark. The fact that, in a Galois extension, the minimal polynomial of θ is $\prod_{\theta' \in \mathrm{Aut}(L/K)\theta} (x - \theta')$ will be useful many times again.

Problem 22.5. Show that (3) implies (4).

Problem 22.6. Show that (4) implies (1).

Definition When L/K is Galois, we denote $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$ and call it the ***Galois group of*** L ***over*** K.