20. Galois extensions

Problem 20.1. Let $K \subseteq L$ be a field extension of finite degree. Let $\theta \in L$ and let $g(x)$ be the minimal polynomial of $\theta$ over $K$. 

1. Show that the size of the $\text{Aut}(L/K)$ orbit of $\theta$ is $\leq [K[\theta] : K]$.
2. If we have equality, show that $g$ is separable and splits in $L$.
3. If $L$ is the splitting field of some separable polynomial $f(x)$, and $g(x)$ is an irreducible factor of $f(x)$, show that we have equality.

The last part of Problem 20.1 is phrased in an awkward way; a better statement, which you can prove once you’ve proved the main results of this worksheet, is “if $L$ is Galois, then we have equality.”

Problem 20.2. Let $K \subseteq L$ be a field extension of finite degree. Show that $\# \text{Aut}(L/K) \leq [L : K]$.

It is natural to ask when we have equality in Problem 20.2. This is answered by the following:

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

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

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

Problem 20.3. Prove the implications $(1) \implies (2) \implies (3) \implies (4)$ of this theorem.

The last statement is a bit harder, here is one route:

Problem 20.4. Assume condition (4). Let $\theta \in L$ and let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be the orbit of $\theta$ under $\text{Aut}(L/K)$. Let $g(x) = \prod_j (x - \theta_j)$.

1. Show that $g(x)$ has coefficients in $K$.
2. Show that $g(x)$ is the minimal polynomial of $\theta$ over $K$.
3. Deduce condition (1).

**Definition:** When $L/K$ is Galois, we denote $\text{Aut}(L/K)$ by $\text{Gal}(L/K)$.

We note that we have just proved the following:

**Theorem:** Let $L/K$ be a Galois extension. Let $\theta \in L$. Then the minimal polynomial of $\theta$ over $K$ is $\prod_{\phi \in \text{Gal}(L/K)} \phi(x - \phi)$. 