

21. TOWERS OF FIELD EXTENSIONS AND GALOIS GROUPS

We recall from last time:

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

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

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

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

Throughout this worksheet, let $F \subseteq K \subseteq L$ be field extensions of finite degree, with L/F Galois.

Problem 21.1. Show that L/K is Galois.

Problem 21.2. Show that $\text{Gal}(L/K)$ is a subgroup of $\text{Gal}(L/F)$.

Problem 21.3. Show that $\# \text{Gal}(L/K) = [L : K]$ and $[\text{Gal}(L/F) : \text{Gal}(L/K)] = [K : F]$.

Problem 21.4. Show that the fixed field of $\text{Gal}(L/K)$ is K .

Problem 21.5. Let L/F be a Galois extension. Show that the map

$$\{\text{fields } K \text{ with } F \subseteq K \subseteq L\} \longrightarrow \{\text{subgroups of } \text{Gal}(L/F)\}$$

given by $K \mapsto \text{Gal}(L/K)$ is injective. (In fact, it is bijective, but I don't think we have the toolkit to prove that yet.)

Problem 21.6. Let $\sigma \in \text{Gal}(L/F)$. Show that $\text{Gal}(L/\sigma(K)) = \sigma \text{Gal}(L/K) \sigma^{-1}$ (as subgroups of $\text{Gal}(L/F)$).

Problem 21.7. Show that the following are equivalent:

- (1) The subgroup $\text{Gal}(L/K)$ is normal in $\text{Gal}(L/F)$.
- (2) For all $\sigma \in \text{Gal}(L/F)$, we have $\sigma(K) = K$.
- (3) For all $\theta \in K$, the minimal polynomial of θ over F splits in K .
- (4) K is the splitting field of a separable polynomial with coefficients in F .
- (5) K/F is Galois.

Problem 21.8. In the situation above, show that we have a short exact sequence $1 \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(L/F) \rightarrow \text{Gal}(K/F) \rightarrow 1$.