The Fundamental Theorem of Galois Theory
(Expanded statement)
Math 128B

**Definition.** Let $F$ be a field, and let $E$ be an extension field of $F$. An *automorphism* of $E$ is a ring isomorphism $\varphi : E \to E$. The *Galois group of $E$ over $F$* is defined to be

$$\text{Gal}(E/F) = \{ \varphi \in \text{Aut}(E) \mid \varphi(x) = x \text{ for all } x \in F \}. \quad (1)$$

If $H \leq \text{Gal}(E/F)$, we define the *fixed field of $H$* to be

$$E_H = \{ x \in E \mid \varphi(x) = x \text{ for all } \varphi \in H \}. \quad (2)$$

**Theorem** (Fundamental Theorem of Galois Theory (expanded)). Let $F$ be a field of characteristic 0 or a finite field, and let $E$ be the splitting field of some $f(x) \in F[x]$. Let $S$ be the set of all subgroups of $\text{Gal}(E/F)$, and let $F$ be the set of all subfields of $E$ containing $F$. Define functions $\Phi : S \to F$ and $\Psi : F \to S$ by

$$\Phi(H) = E_H = \text{the fixed field of } H, \quad (3)$$

$$\Psi(K) = \text{Gal}(E/K) = \text{the group of all automorphism of } E \text{ fixing } K. \quad (4)$$

Then $\Phi$ and $\Psi$ are inverses of each other, and therefore, bijections. (I.e., for $K$ a subfield of $E$ containing $F$, $E_{\text{Gal}(E/K)} = K$, and for $H$ a subgroup of $\text{Gal}(E/F)$, $\text{Gal}(E/E_H) = H$.) Furthermore, if $K$ and $L$ are subfields of $E$ containing $F$:

1. We have that $K \subseteq L$ if and only if $\text{Gal}(E/K) \supseteq \text{Gal}(E/L)$. (I.e., $\Phi$ and $\Psi$ are inclusion-reversing bijections.)

2. $[E : K] = |\text{Gal}(E/K)|$, and therefore,

$$[K : F] = |\text{Gal}(E/F) : \text{Gal}(E/K)| = \frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/K)|}. \quad (5)$$

3. $K$ is a splitting field of some $g(x) \in F[x]$ if and only if $\text{Gal}(E/K)$ is normal in $\text{Gal}(E/F)$. In that case,

$$\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K). \quad (6)$$

4. The group $\text{Gal}(E/F)$ acts on (permutes) the set $X = \{a_1, \ldots, a_n\}$ of all zeros of $f(x)$ in $E$.

5. If $f(x)$ is irreducible, then $\text{Gal}(E/F)$ acts transitively on $X = \{a_1, \ldots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \text{Gal}(E/F)$ such that $\sigma(a_i) = a_j.$