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

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

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

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

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 $\mathcal{S}$ be the set of all subgroups of $\mathrm{Gal}(E/F)$, and let $\mathcal{F}$ be the set of all subfields of E containing F. Define functions $\Phi : \mathcal{S} \to \mathcal{F}$ and $\Psi : \mathcal{F} \to \mathcal{S}$ by*

$$\Phi(H) = E_H = \textit{the fixed field of } H, \tag{3}$$
$$\Psi(K) = \mathrm{Gal}(E/K) = \textit{the group of all automorphism of } E \textit{ fixing } K. \tag{4}$$

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

1. *We have that $K \subseteq L$ if and only if $\mathrm{Gal}(E/K) \geq \mathrm{Gal}(E/L)$. (I.e., Φ and Ψ are inclusion-reversing bijections.)*

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

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

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

$$\mathrm{Gal}(K/F) \approx \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K). \tag{6}$$

4. *The group $\mathrm{Gal}(E/F)$ 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 $\mathrm{Gal}(E/F)$ acts transitively on $X = \{a_1, \ldots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a_i) = a_j$.*