# Galois Theory: The Fundamental Theorem



In this handout all fields are of characteristic 0.

**Theorem** (the fundamental theorem of Galois theory in characteristic 0). Let $E$ be a splitting field over $F$. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions $K$ lying between $F$ and $E$ and the set $\{H : H < \operatorname{Gal}(E/F)\}$ of subgroups $H$ of the Galois group $\operatorname{Gal}(E/F)$ of the original extension $E/F$:

$$\{K : E/K/F\} \quad \longleftrightarrow \quad \{H : H < \operatorname{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension $K$ to the subgroup $\operatorname{Gal}(E/K)$ of elements in $\operatorname{Gal}(E/F)$ that preserve $K$,

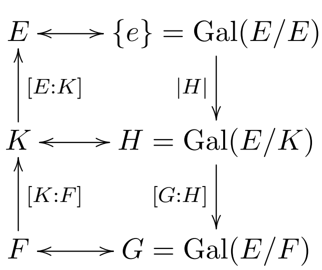
$$K \mapsto \operatorname{Gal}(E/K) := \{\phi : E \to E : \phi|_K = I\},$$

and reversely, by mapping every subgroup $H$ of $\operatorname{Gal}(E/F)$ to its fixed field $E_H$:

$$H \mapsto E_H := \{x \in E : \forall h \in H,\ hx = x\}.$$

This correspondence has the following further properties:

1. It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\operatorname{Gal}(E/K_1) > \operatorname{Gal}(E/K_2)$.
2. It is degree/index respecting: $[E : K] = |\operatorname{Gal}(E/K)|$ and $[K : F] = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K)]$.
3. Splitting fields correspond to normal subgroups: If $K$ in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\operatorname{Gal}(E/K)$ is normal in $\operatorname{Gal}(E/F)$ and $\operatorname{Gal}(K/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.




And if $K$ is splitting, $H$ is normal and $\operatorname{Gal}(K/F) = G/H = \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.

**Proof of $E_{\operatorname{Gal}(E/K)} = K$.** Let $K$ be an intermediate field between $E$ and $F$. The inclusion $E_{\operatorname{Gal}(E/K)} \supset K$ is easy, so we turn to prove the other inclusion. Let $v \in E - K$ be an element of $E$ which is not in $K$. We need to show that there is some automorphism $\phi \in \operatorname{Gal}(E/K)$ for which $\phi(v) \neq v$; if such a $\phi$ exists it follows that $v \notin E_{\operatorname{Gal}(E/K)}$ and this implies the other inclusion. So let $p$ be the minimal polynomial of $v$ over $K$. It is not of degree 1; if it was, we'd have that $v \in K$ contradicting the choice of $v$. $E$ is a splitting extension so we know that $p$ splits in $E$, so $E$ contains all the roots of $p$. Over a field of characteristic 0 irreducible polynomials cannot have multiple roots (as the gcd of an irreducible $p$ with the lower-degree yet non-zero $p'$ must be 1) and hence $p$ must have at least one other root; call it $w$. Since $v$ and $w$ have the same minimal polynomial over $K$, we know that $K(v)$ and $K(w)$ are isomorphic; furthermore, there is an isomorphism $\phi_0 : K(v) \to K(w)$ so that $\phi_0|_K = I$ yet $\phi_0(v) = w$. But $E$ is a splitting field of some polynomial $f$ over $F$ and hence also over $K(v)$ and over $K(w)$. By the uniqueness of splitting fields, the isomorphism $\phi_0$ can be extended to an isomorphism $\phi : E \to E$; i.e., to an automorphism of $E$. but then $\phi|_K = \phi_0|_K = I$ so $\phi \in \operatorname{Gal}(E/K)$, yet $\phi(v) = w \neq v$, as required. □

**Proof of $H = \operatorname{Gal}(E/E_H)$.** Let $H < \operatorname{Gal}(E/F)$ be a subgroup of the Galois group of $E$ over $F$. The inclusion $H < \operatorname{Gal}(E/E_H)$ is easy, so it is enough to show that $\operatorname{Gal}(E/E_H)$ is finite and that $|\operatorname{Gal}(E/E_H)| \leq |H|$.

By the Primitive Element Theorem we know that there is some element $u \in E$ so that $E = E_H(u)$. Let $p$ be the minimal polynomial of $u$ over $E_H$. Let $n := \deg(p)$. To conclude the proof, we will show that

$$|\operatorname{Gal}(E/E_H)| \leq n \leq |H|.$$

Distinct elements of $\operatorname{Gal}(E/E_H)$ map $u$ to distinct roots of $p$, but $p$ splits in $E$ and so it has exactly $n$ roots. This proves the first inequality.

For the second inequality, let $f$ be the polynomial

$$f = \prod_{\sigma \in H} (x - \sigma(u)).$$

Clearly, $f \in E[x]$. Furthermore, if $\tau \in H$, then the action of $\tau$ permutes the $\sigma(u)$'s, hence $\tau(f) = f$ and hence $f \in E_H[x]$. Clearly $f(u) = 0$, so $p|f$, so $n \leq |H|$.

Seeing that $E = E_H(u)$, we have also proven here that $[E : E_H] = \deg(p) = n = |H|$. □

**Proof of Property 1.** Easy. □

**Proof of Property 2.** If $K = E_H$, then $|\operatorname{Gal}(E/K)| = |\operatorname{Gal}(E/E_H)| = [E : E_H] = [E : K]$ as shown above. But every $K$ is $E_H$ for some $H$, so $|\operatorname{Gal}(E/K)| = [E : K]$ for every $K$ between $E$ and $F$. The second equality follows from the first and from the multiplicativity of the degree/order/index in towers of extensions and in towers of groups:

$$[K : F] = \frac{[E : F]}{[E : K]} = \frac{|\operatorname{Gal}(E/F)|}{|\operatorname{Gal}(E/K)|} = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K)]. \qquad \square$$

**Proof of Property 3.** We will define a surjective (onto) group homomorphism $\rho : \operatorname{Gal}(E/F) \to \operatorname{Gal}(K/F)$ whose kernel is $\operatorname{Gal}(E/K)$. This shows that

$\operatorname{Gal}(E/K)$ is normal in $\operatorname{Gal}(E/F)$ (kernels of homomorphisms are always normal) and then by the first isomorphism theorem for groups, we'll have that $\operatorname{Gal}(K/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.

Let $\sigma$ be in $\operatorname{Gal}(E/F)$ and let $u$ be an element of $K$. Let $p$ be the minimal polynomial of $u$ in $F[x]$. Since $K$ is a splitting field $p$ splits in $K[x]$ and hence all the other roots of $p$ are also in $K$. As $\sigma(u)$ is a root of $p$, it follows that $\sigma(u) \in K$ and hence $\sigma(K) \subset K$. But since $\sigma$ is an isomorphism, $[\sigma(K) : F] = [K : F]$ and hence $\sigma(K) = K$. Hence the restriction $\sigma|_K$ of $\sigma$ to $K$ is an automorphism of $K$, so we can define $\rho(\sigma) = \sigma|_K$.

Clearly, $\rho$ is a group homomorphism. The kernel of $\rho$ is those automorphisms of $E$ whose restriction to $K$ is the identity. That is, it is $\operatorname{Gal}(E/K)$. Finally, as $E/F$ is a splitting extension, so is $E/K$. So every automorphism of $K$ extends to an automorphism of $E$ by the uniqueness statement for splitting extensions. But this means that $\rho$ is onto. $\square$