Fundamental Theorem of Galois Theory

Kubi H

September 5, 2024

Theorem. Let K/F be a Galois extension.

1. Suppose that H is a subgroup of $Gal(K/F)$, $H \leq Gal(K/F)$, then the set
$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \sigma \in H\}$$
is an intermediate field of K/F.
2. Let E be an intermediate field of K/F, then K/E is a Galois extension and $Gal(K/E) \leq Gal(K/F)$.

Proof. By definition, $K^H \subset K$ and every element of H fixes F, so $F \subset K^H \subset K$. To prove K^H is a field consider $\alpha, \beta \in K^H$. For any $\sigma \in H$ we have

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$$

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$$
$$\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$$

So, $\alpha + \beta, \alpha\beta, \alpha^{-1} \in K^H$ and it is indeed a field.

Since K/F is a Galois extension, this implies that there exists a separable polynomial $f \in F[x]$ for which K/F is the splitting field. Notice that $f \in E[x]$, and that K/E is still the splitting field of f (which is still separable), so K/E is a Galois extension. Furthermore, if $\sigma \in Gal(K/E)$, then σ fixes E, and since $F \subset E$ it also fixes E so $\sigma \in Gal(K/F)$ and $Gal(K/E) \leq Gal(K/F)$.

Theorem. Let K/F be a Galois extension.

1. If $H \leq Gal(K/F)$, then $H = Gal(K/K^H)$
2. If $K/E/F$ is an intermediate field, then $E = K^{Gal(K/E)}$.

Proof. Suppose that $\sigma \in H$. By definition, $\sigma : K \to K$ is an automorphism which fixes K^H, so $\sigma \in Gal(K/K^H)$ and $H \subset Gal(K/K^H)$.

If $\alpha \in E$, then for any $\sigma \in Gal(K/E)$, $\sigma(\alpha) = \alpha$, so $\alpha \in K^{Gal(K/E)}$ and $E \subset K^{Gal(K/E)}$. To prove equality we could now show that $K^{Gal(K/E)} : E] = 1$. We know that

$$Gal(K/K^{Gal(K/E)}) = Gal(K/E)$$

so the fact that $K/K^{Gal(K/E)}$ and K/E are both Galois extensions shows that

$$[K : K^{Gal(K/E)}] = \sharp Gal(K/K^{Gal(K/E)}) = \sharp Gal(K/E) = [K : E]$$

Additionally we know that

$$[K : E] = [K : K^{Gal(K/E)}][K^{Gal(K/E)} : E] = [K : E][K^{Gal(K/E)} : E]$$

thus $[K^{Gal(K/E)} : E] = 1$ and $K^{Gal(K/E)} = E$.

Corollary. There is a bijection of sets

$$\{\text{intermediate fields of } K/F\} \longleftrightarrow \{\text{subgroups of } Gal(K/F)\}$$

$$E \longrightarrow Gal(K/E)$$
$$K^H \longleftarrow H$$

Theorem. This bijection reverses the inclusions.

$$E_1 \subset E_2 \Longrightarrow Gal(K/E_2) \leq Gal(K/E_1)$$

$$H_1 \subset H_2 \Longrightarrow K^{H_2} \leq K^{H_1}$$

Proof. Suppose $E_1 \subset E_2$, then if $\sigma \in Gal(K/E_2)$ it fixes all of E_2 and thus fixes all of E_1 which means $\sigma \in Gal(K/E_1)$ and $Gal(K/E_2) \leq Gal(K/E_1)$.

Suppose that $H_1 \leq H_2$. If $\alpha \in K^{H_2}$ then $\sigma(\alpha) = \alpha$ for all $\alpha \in H_2$, so $\sigma(\alpha) = \alpha$ for all $\sigma \in H_1$ as well, which means that $\alpha \in K^{H_1}$ and $K^{H_2} \subset K^{H_1}$.