

Fundamental Theorem of Galois Theory

October 2, 2020

Definition 1. Let E and F be extension fields of a field K . A nonzero map $\sigma : E \rightarrow F$ which is both a field homomorphism and a K -module homomorphism is called a **K – homomorphism**. Similarly, if an isomorphism $\sigma \in \text{Aut} F$ is also a K -module homomorphism, then σ is called a **K – automorphism** of F . The group of all K -automorphism is called the **Galois group** of F over K , which is denoted by $\text{Aut}_K F$

REMARK. If $\sigma \in \text{Aut}_K F$, then for any $k \in K, u \in F^*$ we have:

$$\sigma(ku) = \sigma(k)\sigma(u)\sigma(ku) = k\sigma(u)$$

as a result of σ is both K -module automorphism but also a field automorphism. Hence we have $\sigma(k) = k, \forall k \in K$ as $\sigma(u)$ has inverse in F . In contrast, if $\sigma \in \text{Aut} F$ with $\sigma(k) = k, \forall k \in K$, then we have $\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$, which means σ is a K -module isomorphism, hence a K -automorphism.

Theorem 1. Let F be an extension field of K , $f(x) \in \mathbf{K}[x]$. If $u \in F$ is a root of $f(x)$ and $\sigma \in \text{Aut}_K F$ then $\sigma(u)$ is also a root of $f(x)$.

Proof. Let $f(x) = \sum_{i=0}^n f_i x^i$, then

$$f(\sigma(u)) = \sum_{i=0}^n f_i \sigma(u)^i = \sum_{i=0}^n f_i \sigma(u^i) = \sigma\left(\sum_{i=0}^n f_i u^i\right) = \sigma(0) = 0$$

which shows $\sigma(u)$ is also a root of $f(x)$

With Theorem 1, we have the following results: Let $u \in F$ is algebraic over K with $f(x)$ the minimal polynomial of u , if $f(x)$ has m distinct roots over K , then $|\text{Aut}_K K(u)| \leq m$. It's easy to see that $\forall \sigma, \delta \in \text{Aut}_K K(u)$, if $\sigma \neq \delta$, then $\sigma(u) \neq \delta(u)$, otherwise σ and δ has the same effect on $\{1, u, u^2, \dots, u^{n-1}\}$, which is a basis of $K(u)$, hence σ and δ has the same effect on all elements of $K(u)$, which contradicts the fact that $\sigma \neq \delta$. By **Theorem 1** we know that $\sigma(u)$ and $\delta(u)$ are distinct roots of $f(x)$, so there are at most m distinct K -automorphism as there are at most m distinct roots.

Definition 2. Let F be an extension field of K , E an intermediate field and H a subgroup of $\text{Aut}_K F$ Then:

1. $H' = \{v \in F | \sigma(v) = v, \forall \sigma \in H\}$
2. $E' = \{\sigma \in \text{Aut}_K F | \sigma(u) = u, \forall u \in E\}$

REMARK. In other words, H' is the set of all those elements in F such that these elements contains itself under the isomorphism effect, it's also easy to see that H' is an intermediate field of K , hence H' is called the **fixed field of H** .

E' contains all those K -automorphism such that they remains identity maps on E . By the corollary we mentioned earlier, we know that $E' = \text{Aut}_E F$. Specifically, we have:

$$F' = \text{Aut}_F F = \{1_F\}, K' = \text{Aut}_K F$$

On the other hand, we have $\{1_F\} < \text{Aut}_K F$ and $\{1_F\}' = F$. This reminds us to think about the relationships between the sets of all subgroups of $\text{Aut}_K F$ and the sets of intermediate fields of F

Definition 3. Let F be an extension field of K , $\text{Aut}_K F$ the Galois group of F over K , if the fixed field of $\text{Aut}_K F$ is K , then F is said to be a **Galois extension** of K or **be Galois over K**

Theorem 2. Let F be an extension field of K , $K_0 = \text{Aut}_K F'$. Then $\text{Aut}_{K_0} F = \text{Aut}_K F$, therefore F is Galois over K_0

Proof. For any $k \in K$, we know that $\sigma(k) = k, \forall \sigma \in \text{Aut}_K F$, hence $k \in K_0$, therefore $K \subset K_0$. Then $\forall \sigma \in \text{Aut}_{K_0} F$, σ maps all elements in K_0 to itself, of cause maps every element in K to itself as $K \subset K_0$. Hence $\sigma \in \text{Aut}_K F$ and $\text{Aut}_{K_0} F < \text{Aut}_K F$. For any $\sigma \in \text{Aut}_K F$, by the definition of K_0 , $\sigma(k_0) = k_0, \forall k_0 \in K_0$, hence $\sigma \in \text{Aut}_{K_0} F$ and $\text{Aut}_K F < \text{Aut}_{K_0} F$. These two results show that $\text{Aut}_K F = \text{Aut}_{K_0} F$. And we have $\text{Aut}_{K_0} F' = \text{Aut}_K F' = K_0$. Therefore F is Galois over K_0

In the rest section, we will prepare and prove the fundamental theorem of Galois theory, which demonstrates a **one-to-one correspondence** between the sets of all intermediate fields of the extension F over K and the sets of all subgroups of the Galois group $\text{Aut}_K F$. But there are some rather lengthy preliminaries to do.

Lemma 3. Let F be an extension field of K with intermediate field L and M . Let H and J be subgroups of $G = \text{Aut}_K F$. Then:

1. $F' = 1$ and $K' = G$
2. $1' = F$
3. $L \subset M \Rightarrow M' < L'$
4. $H < J \Rightarrow J' \subset H'$
5. $L \subset L''$ and $H < H''$ where $L'' = (L')'$ and $H'' = (H')'$
6. $L' = L'''$ and $H' = H'''$

Proof. 1,2 are direct results of the definition. Consider 3: If $L \subset M$, then for any F -automorphism that fix M , it must fix L , therefore $M' < L'$.