Fundamental Theorem of Galois Theory

October 2, 2020

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

Remark. If $\sigma \in Aut_K F$, 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 $\sigma \in AutF$ 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 filed of K, $f(x) \in \mathbf{K[x]}$. If $u \in F$ is a root of $f(x)$ and $\sigma \in Aut_K F$ then $\sigma(u)$ is also a root of $f(x)$.*

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

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

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

With Theorem1, 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 $|Aut_K K(u)| \leq m$. It's easy to see that $\forall \sigma, \delta \in Aut_K K(u)$, if $\sigma \neq \delta$, then $\sigma(u) \neq \delta(u)$, otherwise σ and δ has the same effect on $\{1, u, u^2, ..., u^{n-1}\}$, 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 **Theorem1** 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 $Aut_K F$ Then:*

1. $H^{'} = \{v \in F | \sigma(v) = v, \forall \sigma \in H\}$

2. $E^{'} = \{\sigma \in Aut_K F | \sigma(u) = u, \forall u \in E\}$

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 $E^{'} = Aut_E F$. Specifically, we have:

$$F^{'} = Aut_F F = \{1_F\}, K^{'} = Aut_K F$$

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

Definition 3. *Let F be an extension field of K, $Aut_K F$ the Galois group of F over K, if the fixed field of $Aut_K F$ 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, $K_0 = Aut_K F^{'}$. Then $Aut_{K_0} F = Aut_K F$, therefore F is Galois over K_0*

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

In the rest section, we will prepare and prove the fundamental theorem of Galois theroy, 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 $Aut_K F$.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=$Aut_K F$. Then:

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