Fundamental Theorem of Galois Theory(1)

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, $f(x) \in \mathbf{K}[\mathbf{x}]$. 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. $1^{'} = F$
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 difinition. Consider 3: If $L \subset M$, then for any $F-automorphism$ that fix M, it must fix L, therefore $M^{'} < L^{'}$. the 4th one is the same: every element in $J^{'}$ must be fixed for under every isomorphism of J, therefore fixed by every isomorphism of H, and belongs to $H^{'}$.
As for (5), consider any $l \in L$, according to the definition of $L^{'}$, $L^{'}$ consists of those isomorphisms that fix every element of L, therefore every isomorphism fix l, which shows that $l \in L^{''}$ by definition. Therefore we have $L \subset L^{''}$. The second part could be proved in the same way.
For (6), we first notice that $L^{'} < (L^{'})^{''} = L^{'''}$ by the second part of (5). And $L \subset L^{''} \Rightarrow (L^{''})^{'} < L^{'}$ by (5) and (3). Therefore we have $L^{'} = L^{'''}$. The second part follows in the same way.

REMARK. F is galois over K iff $(Aut_K F)^{'} = K$, which means $K^{''} = K$. Therefore we have: F is galoic over any intermediate field E iff $E = E^{''}$.

Let X be an intermediate field or subgroup of the Galois group. X is called **closed** if $X^{''} = X$. And we have F is Galois over K iff K is closed.

Theorem 4. *If* F *is an extension field of* K*, then there is a one-to-one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group, given by* $\mathrm{E} \mapsto \mathrm{E}^{'} = \mathrm{Aut_E F}$.

Proof. Let A be the set of all closed intermediate fields of F and B be the set of all closed subgroups of Galois group. Define f as follows:

$$f : \mathrm{A} \to \mathrm{B}, \mathrm{E} \mapsto \mathrm{E}^{'}$$

Notice that for any map image $\mathrm{E}^{'}$, we have $\mathrm{E}^{'''} = \mathrm{E}^{'}$, which means $\mathrm{E}^{'}$ is closed. Therefore this map is well-defined.
Let g be defined as follows:

$$g : \mathrm{B} \to \mathrm{A}, \mathrm{H} \mapsto \mathrm{H}^{'}$$

Then for any $\mathrm{E} \in \mathrm{A}$, we have:$gf(\mathrm{E}) = g(\mathrm{E}^{'}) = \mathrm{E}^{''} = \mathrm{E}$ as E is closed, thus $gf = 1_{\mathrm{A}}$. Similarly, we have $fg = 1_{\mathrm{B}}$, which means f and g are bijective, it's done.

Lemma 5. Let F be an extension field of K and L, M intermediate fields with $L \subset M$. If $[M : L]$ is finite, then $[L^{'} : M^{'}] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K F| \leq [F : K]$.

Proof. We will prove this assertion by induction on $n = [M : L]$. When $n = 1$, it's done with $M = L$. Suppose for any $i < n$ this theorem is true, then choose one element $u \in M, u \notin L$. Since $[M : L]$ is finite, we have u is algebraic over L. Let $f(x) \in L[x]$ be the minimal polynomial of u, and k the degree of $f(x)$. Therefore we have:$[L(u) : L] = k$ and $[M : L(u)] = n/k$. If $\mathbf{k < n}$, we have $[M : L(u)] > 1$ and $[L^{'} : M^{'}] = [L^{'} : L(u)^{'}] \times [L(u)^{'} : M^{'}] \leq k \times (n/k) = n$ by induction.

Otherwise if $k = n$, which means $M = L(u)$.To prove this , we will construct an injective map from **the set of all left cosets of $\mathbf{M^{'}}$ in $\mathbf{L^{'}}$** to the set T of all **distinct roots**

of $f(x) \in L[x]$, whence $\mid S \mid \leq \mid T \mid$ and $\mid T \mid \leq n$.

Let $\tau M^{'}$ be a left coset of $M^{'}$ in $L^{'}$. We define g as follows:

$$g : S \to T, \tau M^{'} \mapsto \tau(u)$$

We will show this map is well-defined. First, $\tau \in L^{'}$, which means τ fix every element in L, therefore $\tau(u)$ is also a root of f by theorem 1. This means the map we defined maps the object to a right place. Second, if $\tau M^{'} = \sigma M^{'}$, then $\sigma^{-1}\tau \in M^{'}$, notice that $u \in M$, we have: $\sigma^{-1}\tau(u) = u \Rightarrow \tau(u) = \sigma(u)$, which means $g(\tau M^{'}) = g(\sigma M^{'})$. Therefore the image has no relationship with the representative object of the cosets, this map is also well defined.

In the last, we will show that g is also injective. If $g(\sigma M^{'}) = g(\tau M^{'})$, then $\sigma(u) = \tau(u)$, and $\tau^{-1}\sigma(u) = u$, which means $\tau^{-1}\sigma$ fix u. Notice that $L(u)$ is generated by $1, u, ..., u^{n-1}$. We also conclude that $\tau^{-1}\sigma$ fix this basis and further more, it fix $\mathbf{L(u) = M}$. Therefore $\tau^{-1}\sigma \in M^{'}$ and $\tau M^{'} = \sigma M^{'}$. This means g is injective, and $\mid S \mid \leq \mid T \mid \leq n$, which is $[L^{'} : M^{'}] \leq [M : L]$.

The following lemma is an analogue of **Lemma 5** for subgroups of the Galois group.

Lemma 6. Let F be an extension field of K and let H, J be subgroups of the Galois group $\mathrm{Aut_K F}$ with $H < J$.If $[J : H]$ is finite, then $[H^{'} : J^{'}] \leq [J : H]$

Proof.