

Advanced Algebra I

FINITE DIMENSIONAL GALOIS EXTENSION

In this section, we are going to prove the fundamental theorem for finite dimensional Galois extension.

Let F/K be an field extension, we define the Galois group of F over K , denoted $\text{Gal}_{F/K}$ or $G_{F/K}$ or $\text{Aut}_K(F)$, as

$$\text{Gal}_{F/K} := \{\sigma \mid \sigma \in \text{Aut} F, \sigma|_K = \mathbf{1}_K\}.$$

It's clear that for $\sigma \in \text{Gal}_{F/K}$ and $u \in F$ algebraic over K with minimal polynomial $p(x)$, then $\sigma(u)$ satisfies the same minimal polynomial.

On the other hand, if F/K is normal, let u, v be two elements having the same minimal polynomial $p(x)$, then we claim that there is an $\sigma \in \text{Gal}_{F/K}$ such that $\sigma(u) = v$. To see this, we fix an algebraic closure $\overline{K}$ containing F . There is an K -isomorphism $\sigma_0 : K(u) \rightarrow K(v)$ which extends to an embedding $\sigma : F \rightarrow \overline{K}$. Since F is normal over K , one has $\sigma(F) \subset F$. And hence $\sigma \in \text{Aut} F$.

Example 0.1. Consider the field $F := \mathbb{Q}(\sqrt[3]{2}, \omega)$ which is a splitting field of $x^3 - 2$ over $\mathbb{Q}$. Thus it's normal over $\mathbb{Q}$. One can check that the Galois group $\text{Gal}_{F/\mathbb{Q}}$ is generated by σ, τ that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma(\omega) = \omega$, and $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2$. It's easy to check that $\text{Gal}_{F/\mathbb{Q}} \cong S_3$.

Example 0.2. Consider the field $F := \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Then it's easy to check that $\text{Gal}_{F/\mathbb{Q}} = \{\mathbf{1}_F\}$.

There is a natural correspondence between subgroups of Galois groups and intermediate fields. To be precise, fix an extension F/K . Let $H < G := \text{Gal}_{F/K}$ be a subgroup. One can define

$$H' := \{u \in F \mid \sigma(u) = u, \forall \sigma \in H\}.$$

It's clear that this is a field. On the other hand, given an intermediate field L such that $K \subset L \subset F$, then one can define

$$L' := \{\sigma \in \text{Gal}_{F/K} \mid \sigma(u) = u, \forall u \in L\} = \{\sigma \in \text{Gal}_{F/K} \mid \sigma|_L = \mathbf{1}_L\}.$$

It's easy to check the following properties:

Proposition 0.3. Let F/K be an extension with Galois group G . Let L be an intermediate field, i.e. $K \subset L \subset F$, and $H < G$ is a subgroup.

- (1) $F' = \{\mathbf{1}_F\}$, $K' = G$, and $\{\mathbf{1}_F\}' = F$.
- (2) For any L , one has $L \subset L''$, $L' = L'''$.
- (3) For any H , one has $H < H''$, $H' = H'''$.
- (4) For any intermediate fields $L \subset M$, one has $M' < L'$.
- (5) For any subgroups $J < H$, one has $H' \subset J'$.

Proof. Most of the proof follows directly from the definition. We only sketch the proof for $L' = L'''$.

By $L \subset L''$ and (4), one has

$$(L'')' < L'.$$

On the other hand, by (5), one has

$$L' < (L')''.$$

We are done. $\square$

Proposition 0.4. *There is a one-to-one correspondence between*

$$\{L|K \subset L \subset F, L'' = L\} \leftrightarrow \{H|H < G, H'' = H\}.$$

Proof. The correspondence is given by $L \mapsto L'$ (or $H \mapsto H'$).

To show the injective, one sees that if $L'_1 = L'_2$, then $L_1 = L'_1 = L''_1 = L_2$.

For any H with $H'' = H$, we take $L = H'$, then $H = L'$. It suffices to check that $L'' = L$. This follows from the fact that $H''' = H'$. $\square$

In the proposition, one might expect that $G' = K$. However, this is not always the case (see e.g. Example 2). For extension with this property, we call it *Galois*. It turns out that this naive definition is a very delicate one which leads to some nice properties.

Definition 0.5. *An extension F/K is said to be Galois if $(\text{Gal}_{F/K})' = K$.*

Theorem 0.6 (Fundamental theorem of finite dimensional Galois extension). *Let F/K be a finite dimensional Galois extension with Galois group G , then*

(1) *There is an one-to-one correspondence between*

$$\{L|K \subset L \subset F\} \leftrightarrow \{H|H < G\}.$$

(2) *The corresponding degree are equal. That is, if $K \subset L \subset M \subset F$, then $[M : L] = [L' : M']$. And if $J < H < G$, then $[H : J] = [J' : H']$.*

(3) *An intermediate field E is Galois over K if and only if $E' \triangleleft G$. And in this case, $\text{Gal}_{E/K} \cong G/E'$.*

Proof. Step 1. $[M : L] \geq [L' : M']$.

We prove the case that $M = L(u)$ for some $u \in M$ and by induction on $[M : L]$, we are done. Suppose now that $M = L(u)$ and let $p(x)$ be the minimal polynomial of u over L . Let S be the set of roots of $p(x)$ in F . Then one has a map

$$\Phi : L' \rightarrow S,$$

$$\sigma \mapsto \sigma(u).$$

One can check that Φ induces an injective map $L'/M' \rightarrow S$. Hence one has

$$[L' : M'] = |L'/M'| \leq |S| \leq \deg(p(x)) = [M : L].$$

Step 2. $[H : J] \geq [J' : H']$.

Let $n = [H : J]$. Suppose on the contrary that there are $n+1$ elements $u_1, \dots, u_{n+1} \in J'$ linearly independent over H' .

We consider the equation $\sum_{i=1}^{n+1} u_i x_i = 0$ in F . Consider now a set of representative of H/J , denoted $\{e = \sigma_1, \dots, \sigma_n\}$. By applying σ_i to the above equation. Then one has a system of linear equations in F .

$$(*) \begin{cases} \sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + \dots + \sigma_1(u_{n+1})x_{n+1} = 0 \\ \sigma_2(u_1)x_1 + \sigma_2(u_2)x_2 + \dots + \sigma_2(u_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(u_1)x_1 + \sigma_n(u_2)x_2 + \dots + \sigma_n(u_{n+1})x_{n+1} = 0 \end{cases}$$

Pick a solution in F with smallest number of non-zero a_i 's, may assume it's $(a_1, \dots, a_s, 0, \dots, 0)$ and $a_1 = 1$.

If there is an $\tau \in H$ such that $\tau(a_2) \neq a_2$, then by applying τ to the system $(*)$, one get the same system of equations with a solution $(\tau(a_1), \tau(a_2), \dots, \tau(a_s), 0, \dots, 0)$. Hence

$$(a_1, \dots, a_s, 0, \dots, 0) - (\tau(a_1), \tau(a_2), \dots, \tau(a_s), 0, \dots, 0) = (0, a_2 - \tau(a_2), \dots, 0)$$

is a non-zero solution of smaller length. This is the required contradiction.

To find τ . We look at $u_1 a_1 + \dots + u_s a_s = 0$. Since $\{u_1, \dots, u_s\}$ is independent over H' , not all a_i is in H' . We may assume that $a_2 \notin H'$. Hence there is a $\tau \in H$ such that $\tau(a_2) \neq a_2$. We are done.

Step 3. We show that every intermediate field L , $L'' = L$. And every subgroup $H < G$, $H'' = H$.

By Step 1, one has

$$[L'' : K] = [L'' : K''] \leq [K' : L'] \leq [L : K],$$

however, one has $L \subset L''$. Thus one has $L = L''$. Similarly, one can prove that $H'' = H$ by considering $[H'' : \{1_F\}]$.

Step 4. $[M : L] = [L' : M']$ and $[H : J] = [J' : H']$.

This follows from $[M : L] = [M : K]/[L : K] = [K' : M']/[K' : L'] = [L' : M']$. And the other one is similar.

Step 5. F/K is normal and separable.

Given $u \in F$, with minimal polynomial $p(x)$ over K . As in the proof of Step 1. One has $[K(u)' : K'] \leq |S| \leq \deg(p(x)) = [K(u) : K]$. By Step 4, they are equalities. In particular, every root of $p(x)$ is in F and there is no multiple roots. Thus F is normal and separable over K .

Step 6. If $N \triangleleft G$, then N' is stable. That is, for all $\sigma \in G$, $\sigma(N') \subset N'$ (indeed $= N'$).

Since $N \triangleleft G$, for all $\sigma \in G$ and for all $\tau \in N$, one has $\sigma^{-1}\tau\sigma \in N$. Thus, $\sigma^{-1}\tau\sigma(N') = N'$. It follows that $\tau\sigma(N') = \sigma(N')$, for all $\tau \in N$. Hence $\sigma(N')$ is fixed by all N and thus $\sigma(N') \subset N'$.

Step 7. If E is a stable intermediate subfield. Then the restriction map $\text{Gal}_{F/K} \rightarrow \text{Gal}_{E/K}$ is well-defined and surjective.

Since E is stable, then $\sigma|_E \in \text{Gal}_{E/K}$ for any $\sigma \in \text{Gal}_{F/K}$. Moreover, let $\tau \in \text{Gal}_{E/K}$, by the extension theorem, there is an extension $\bar{\tau} : F \rightarrow \bar{K}$. Since F is normal over K , $\bar{\tau}$ is in fact an automorphism of F .

Step 8. If an intermediate field E is stable, then E/K is Galois.

To see this, it suffices to show that for any $u \in E - K$, there is an $\sigma \in \text{Gal}_{E/K}$ such that $\sigma(u) \neq u$. Fix any $F \ni v \neq u$ with the same minimal polynomial as u . There is a K -isomorphism $\sigma_0 : K(u) \rightarrow K(v)$ such that $\sigma_0(u) = v$. σ_0 can be extended to an embedding $\bar{\sigma} : F \rightarrow \bar{K}$, which gives an automorphism of F . The restriction $\sigma = \bar{\sigma}|_E$ gives an automorphism of E that $\sigma(u) \neq u$.

Step 9. If E/K is Galois, then E is stable.

One first notices that E/K is normal. For every $\sigma \in \text{Gal}_{F/K}$, σ gives an embedding $\sigma|_E : E \rightarrow \bar{K}$. Since E/K is normal, $\sigma|_E$ is an automorphism of E . And hence E is stable under the Galois group $\text{Gal}_{F/K}$ action.

Step 10. If E is stable, then E' is normal.

This can be checked directly. For all $\sigma \in G$ and $\tau \in E'$ and for all $u \in E$,

$$\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\tau(\sigma(u)) = \sigma^{-1}\sigma(u) = u,$$

since $\sigma(u) \in E$. Therefore, $\sigma^{-1}\tau\sigma \in E'$. □

Remark 0.7. Some of the result we proved still true in a more general setting. We list some here:

- (1) If F/K is an extension, and an intermediate field E is stable, then $E' \triangleleft \text{Gal}_{F/K}$.
- (2) Let F/K be an extension. If $N \triangleleft \text{Gal}_{F/K}$, then H' is stable.
- (3) If F/K is Galois, and E is a stable intermediate field, then E is Galois over K . (finite-dimensional assumption is unnecessary here)
- (4) An intermediate field E is algebraic and Galois over K , then E is stable.

We conclude this section with the following theorem concerning the relation between Galois extension, normal extension and splitting fields.

Theorem 0.8. Let F/K be an extension, then the following are equivalent

- (1) F is algebraic and Galois over K .
- (2) F is separable over K and F is a splitting field over K of a set S of polynomials.
- (3) F is a splitting field of separable polynomials in $K[X]$.

(4) F/K is normal and separable.

Proof. Fix $u \in F$ with minimal polynomial $p(x)$ over K . Let $\{u = u_1, \dots, u_r\}$ be distinct roots of $p(x)$ in F . For any σ , then σ permutes $\{u = u_1, \dots, u_r\}$. Thus $f(x) := \prod_{i=1}^r (x - u_i)$ is invariant under σ . Hence $f(x) \in K[x]$. It follows that $f(x) = p(x)$. This proved that (1) $\Rightarrow$ (2), (3), (4).

One notices that (2) $\Leftrightarrow$ (4). Thus it remains to show that (2) $\Rightarrow$ (3), and (3) $\Rightarrow$ (1).

For (2) $\Rightarrow$ (3), let $f(x) \in S$ and let $g(x)$ be a monic irreducible component of $f(x)$. Since $f(x)$ splits in F , it's clear that $g(x)$ is a minimal polynomial of some element in F . Moreover, since F/K is separable, $g(x)$ is separable. One sees that F is in fact a splitting field of such $g(x)$'s.

For (3) $\Rightarrow$ (1), we first note that F/K is algebraic since F is a splitting field. We shall prove that (4) $\Rightarrow$ (1). The implication (3) $\rightarrow$ (4) follows from a general fact about separable extension that an algebraic extension F/K is separable if F is generated by separable elements.

To this end, pick any $u \in F - K$, with minimal polynomial $p(x)$ of degree ≥ 2 and separable. Hence there is a different root, say v , of $p(x)$ in F . It's natural to consider the K -isomorphism $\sigma : K(u) \rightarrow K(v)$. Which can be extended to $\bar{\sigma} : F \rightarrow \bar{K}$. Since F is normal, $\bar{\sigma}$ is an automorphism of F , hence in $\text{Gal}_{F/K}$ sending u to $v \neq u$. So F/K is Galois.

□