Galois Group Correspondence On Extension Fields Over $\mathbb{Q}$

Novita Dahoklory$^{1, a)}$, Henry W. M. Patty$^{1,b)}$

$^1$Department of Mathematics, Pattimura University

$^{a)}$Corresponding author: novitadahoklory93@gmail.com

$^{b)}$henrywmpatty81@gmail.com

Abstract. Let $K/F$ be an extension field where $[K:F]$ denotes dimension of $K$ as a vector space over $F$. Let $Aut(K/F)$ be the group of all automorphism of $K$ that fixes $F$ where the order of $Aut(K/F)$ is denoted by $|Aut(K/F)|$. Particularly, an extension field is called a Galois extension if $|Aut(K/F)| = [K:F]$. Moreover, we will give some examples of properties of extension field $K/F$ which is a Galois extension. Using the properties of Galois extension, we will show that there is an one-one correspondence between the set of all intermediate fields in $K$ and the set of all subgroups in $Aut(K/F)$. Furthermore, we will give some examples of Galois group correspondence using an extension field over $\mathbb{Q}$.

Keywords: Extension fields, Galois extension, Galois correspondence

2020 Mathematical Subject Classification: 11T71, 94B05, 94B25, 97D60

INTRODUCTION

Suppose $F$ and $K$ be fields where $F \subseteq K$. The field $K$ is called an extension field of $F$ and is denoted by $K/F$. We know that $K$ can be viewed as a vector space over $F$. Thus, $K$ have a basis where the dimension of $K$ is denoted by $[K:F]$. Moreover, we form a set of all automorphisms of $K$ that fixes $F$ that is $Aut(K/F) = \{ \sigma : K \to K \text{ automorphism} | \sigma(x) = x, \text{for all } x \in F \}$

Note that $Aut(K/F)$ is a group under the operation of composition in $Aut(K/F)$. The group $Aut(K/F)$ is called automorphism group of $K/F$. The number of elements in $Aut(K/F)$ is called order of $Aut(K/F)$ and is written as $|Aut(K/F)|$. In particular, an extension field $K/F$ is called a Galois extension if $|Aut(K/F)| = [K:F]$.

Let $K/F$ be an extension field with its automorphism group $G = Aut(K/F)$. An intermediate field $E$ of $K/F$ is a subfield in $K$ containing $F$ that is $F \subseteq E \subseteq K$. Let $H$ be a subgroup in $G$. Then, we form a set in $K$ defined by $K^H = \{ x \in K | \sigma(x) = x \text{ for every } \sigma \in H \}$. In other words, $K^H$ is the set of all elements in $K$ which are mapped into itself by every $\sigma \in H$. The set $K^H$ is a subfield in $K$ containing $F$ and is called fixed field of $S$. Thus, for every subgroup in $G$, we can form an intermediate subfield in $K$ defined by $K^H$. Furthermore, suppose $\mathcal{H}$ is the set of all subgroups in $G$, and $\mathcal{F}$ is the set of all intermediate field of $K/F$. We can form a function between $\mathcal{H}$ and $\mathcal{F}$ defined by $\rho : \mathcal{H} \to \mathcal{F}$ $H \mapsto K^H$ for all $H \in \mathcal{H}$. Using this correspondence, we can compute all subfields of $K/F$. For example, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is an extension field where its automorphism group is $G = \{ id, \sigma \}$ where $\sigma(1) = 1$ and $\sigma(\sqrt{2}) = -\sqrt{2}$. Note that, the set

DOI: https://doi.org/10.30598/PattimuraSci.2023.KNMXXI.17-28
of all subgroups in $G$ is $H_1 = \{id\}$ and $H_2 = G$ itself. Using the function, we obtain $\mathbb{Q}(\sqrt{2})^{H_1} = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})^{H_2} = \mathbb{Q}$. Thus, the intermediate subfields of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$.

Throughout this research, we will show that if $K/F$ is a Galois extension then there is a one-one correspondence between the set of all subfields in $K$ which contains $F$ and the set of all subgroups in $Aut(K/F)$ (i.e. $\mathcal{F}$ and $\mathcal{H}$). We called this correspondence as Galois correspondence. Furthermore, we will give an example related to Galois group correspondence especially extension fields over $\mathbb{Q}$.

**SOME RESULTS**

In this part, we will discuss about an extension field $K/F$ with its properties related to its role as a vector space over $F$. Next, we will also explain the automorphism group of an extension field $K/F$ and give some examples on finding all automorphisms of $K/F$. Moreover, we will discuss about Galois extension with its properties. Using the properties of Galois extension, we will also discuss Galois correspondence.

**Definition 1**
Let $F$ and $K$ be fields where $F \subseteq K$. The field $K$ is called an extension field of $F$ (denoted by $K/F$).

**Example 2**
- $\mathbb{R}$ is an extension field of $\mathbb{Q}$.
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is an extension field of $\mathbb{Q}$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\}$ is an extension field of $\mathbb{Q}$.

Let $K/F$ is an extension field. We know that $K$ can be viewed as a vector space over $F$. Thus, $K$ has a basis $B$ over $F$ where the number of elements in $B$ is called dimension of $K$ denoted by $[K:F]$.

**Definition 3**
Let $K/F$ is an extension field. If $[K:F] < \infty$ then $K$ is called a finite extension of $F$.

Next, we will give an example of the dimension of a finite extension field.

**Example 4**
- Given $\mathbb{Q}$ with its extension $\mathbb{Q}(\sqrt{2})$. Every $x \in \mathbb{Q}(\sqrt{2})$ can be expressed by $x = a + b\sqrt{2}$.

Therefore, $x$ can be written as a linear combination of $\{1, \sqrt{2}\}$. It is clear that $\{1, \sqrt{2}\}$ is linearly independent over $\mathbb{Q}$. So, $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Hence, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$.

- Let $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ be an extension field. Note that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\}$.

Therefore, basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}] = 4$.

Suppose $K/F$ is an extension field and $E$ is a subfield in $K$ containing $F$ i.e. $F \subseteq E \subseteq K$. Thus, we obtain extension fields $K/E$ and $E/F$. We will give a property of $[K:E]$ and $[E:F]$ in the following Lemma.

**Lemma 5**
If $K, E, F$ are fields where $F \subseteq E \subseteq K$ then $[K:F] = [K:E][E:F]$.

**Proof**
Let $[K:E] = m$ and $[E:F] = n$. We will show that $[K:F] = [K:E][E:F] = mn$. Suppose that $\{v_1, v_2, ..., v_m\}$ and $\{w_1, w_2, ..., w_n\}$ be basis for $K/E$ and $E/F$, respectively. Take any $x \in K$. Since $K$ is a vector space over $E$, $x$ can be expressed as

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m,$$

for $\alpha_1, \alpha_2, ..., \alpha_m \in E$. Note that $E$ is a vector space over $F$, we obtain
Given an extension field 

\[ \alpha_i = \beta_{i1}w_1 + \beta_{i2}w_2 + \cdots + \beta_{in}w_n \]

for \( i = 1, 2, \ldots, m \). Then,

\[
x = (\beta_{11}w_1 + \beta_{12}w_2 + \cdots + \beta_{1n}w_n)v_1 + \cdots + (\beta_{m1}w_1 + \beta_{m2}w_2 + \cdots + \beta_{mn}w_n)v_m
\]

\[
= \beta_{11}v_1w_1 + \beta_{12}v_1w_2 + \cdots + \beta_{1n}v_1w_n + \cdots + \beta_{m1}v_mw_1 + \beta_{m2}v_mw_2 + \cdots + \beta_{mn}v_mw_n.
\]

Thus, \( K \) is generated by \( B = \{ v_iw_j | i = 1, 2, \ldots, m, j = 1, 2, \ldots, n \} \). Now, we will show that \( B \) is linearly independent.

Suppose that

\[
c_1v_1w_1 + c_2v_2w_2 + \cdots + c_nv_nw_n = 0
\]

So,

\[
(c_{11}w_1 + c_{12}w_2 + \cdots + c_{1n}w_n)v_1 + \cdots + (c_{m1}w_1 + c_{m2}w_2 + \cdots + c_{mn}w_n)v_m = 0.
\]

Since \( \{v_1, v_2, \ldots, v_n\} \) is linearly independent, we obtain \( c_{11}v_1 + c_{12}v_2 + \cdots + c_{1n}v_n = 0 \) for \( i = 1, 2, \ldots, m \). Also, since \( \{w_1, w_2, \ldots, w_n\} \) is linearly independent, it means \( c_{11} = c_{12} = \cdots = c_{1n} = 0 \). Thus, \( c_{ij} = 0 \) for \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, n \). We have \( B \) is a basis of \( K \) over \( F \). Hence, \( B = \{ v_iw_j | i = 1, 2, \ldots, m, j = 1, 2, \ldots, n \} \) and \( [K:F] = mn \).

Next, we will discuss automorphism group of an extension field. Moreover, we will give some properties related to the automorphism group.

Let \( K/F \) be an extension field. We form the set of all automorphism of \( K \) which is defined by

\[ \text{Aut}(K/F) = \{ \sigma : K \rightarrow K \text{ automorphism} | \sigma(x) = x, \text{ for all } x \in F \}. \]

\( \text{Aut}(K/F) \) is a group under the operation of composition and is called the automorphism group of \( K/F \).

Next, we will give some examples of \( \text{Aut}(K/F) \) of extension field \( K/F \).

**Example 6**

Suppose an extension field \( \mathbb{Q}(\sqrt{2})/\mathbb{Q} \) with its basis \( B = \{ 1, \sqrt{2} \} \). It is known that each automorphism can be defined by a function

\[ \rho : B \rightarrow \mathbb{Q}(\sqrt{2}). \]

The function will then be extended to \( \rho' : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}) \). Because \( \sigma \) is an element in \( \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \), we have \( \sigma(1) = 1 \) and \( \sigma(a) = \sigma(1.a) = a. \sigma(1) = a \cdot 1 = a \) for every \( a \in \mathbb{Q} \). Note that,

\[ 0 = \sigma(0) = \sigma((\sqrt{2})^2 - 2) = \sigma(\sqrt{2})^2 - 2. \]

So, \( \sigma(\sqrt{2})^2 = 2 \) and \( \sigma(\sqrt{2}) = \sqrt{2} \) or \( -\sqrt{2} \). So, we get two automorphisms of \( \mathbb{Q}(\sqrt{2}) \) which is defined by

\[ \sigma_1 : B \rightarrow \mathbb{Q}(\sqrt{2}) \]

\[ 1 \mapsto 1 \]

\[ \sqrt{2} \mapsto \sqrt{2} \]

and

\[ \sigma_2 : B \rightarrow \mathbb{Q}(\sqrt{2}) \]

\[ 1 \mapsto 1 \]

\[ \sqrt{2} \mapsto -\sqrt{2} \]

Then, those two functions are extended to

\[ \sigma_1' : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}) \]

\[ a. 1 + b. \sqrt{2} \mapsto a. \sigma_1(1) + b. \sigma_1(\sqrt{2}) \]

and

\[ \sigma_2' : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}) \]

\[ a. 1 + b. \sqrt{2} \mapsto a. \sigma_2(1) + b. \sigma_2(\sqrt{2}) \]

Therefore, \( \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{ \sigma_1', \sigma_2' \} = \{ id, \sigma_2' \} \). Thus, we have extension field \( \mathbb{Q}(\sqrt{2})/\mathbb{Q} \) with its automorphism group \( G = \text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{ id, \sigma_2' \} \).

**Example 7**

Given an extension field \( \mathbb{Q}(\sqrt{3})/\mathbb{Q} \) where
Suppose an extension field \( Q(\sqrt{2}) \) is a basis of \( Q(\sqrt{2}) \) over \( Q \). We will use the same way from Example 6 to find all automorphisms of \( Q(\sqrt{2}) \). We construct all automorphisms in \( Q(\sqrt{2}) \) from bijective function which is defined by

\[ \rho: B \rightarrow Q(\sqrt{2}). \]

We obtain \( \sigma(1) = 1 \) and \( \sigma(a) = \sigma(1,a) = a \). \( \sigma(1) = a \) for every \( a \in Q \). So,

\[ 0 = \sigma(0) = \sigma((\sqrt{2})^3 - 2) = \sigma((\sqrt{2})^3) - \sigma(2) = \sigma((\sqrt{2})^3 - 2). \]

So,

\[ \sigma((\sqrt{2})^3) = 2. \]

We know that the roots of \( x^3 - 2 = 0 \) are \( \sqrt{2} e^{\frac{2\pi i}{3}}, \sqrt{2} e^{\frac{4\pi i}{3}}, \) and \( \sqrt{2} \). Note that \( \sqrt{2} e^{\frac{2\pi i}{3}}, \sqrt{2} e^{\frac{4\pi i}{3}} \in Q(\sqrt{2}) \), so \( \sigma(\sqrt{2}) = \sqrt{2} \). Using the same way, we will also only have \( \sigma(\sqrt{4}) = \sqrt{4} \). Hence, we can only form one automorphism defined by

\[ \sigma_1: B \rightarrow Q(\sqrt{2}) \]

\[ \sqrt{2} \mapsto \sqrt{2} \]

\[ \frac{\sqrt{2}}{2} \mapsto \frac{\sqrt{2}}{2} \]

Then, we extend \( \sigma_1 \) to \( \sigma_1' \) defined by

\[ \sigma_1': Q(\sqrt{2}) \rightarrow Q(\sqrt{2}) \]

\[ a, b, c, \sqrt{2}, \sqrt{3}, \sqrt{6} \mapsto a, b, \sigma_1(1) + b, \sigma_1(\sqrt{2}) + c, \sigma_1(\sqrt{3})(\sqrt{6}) \]

Thus, \( \sigma_1' \) is the identity function of \( Q(\sqrt{2}) \). In conclusion, we obtain \( Aut(Q(\sqrt{2})/Q) = \{ \sigma_1' \} = \{ id \} \).

Example 8
Suppose an extension field \( Q(\sqrt{2}, \sqrt{3})/Q \) with its basis \( B = \{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \} \). It is known that each automorphism can be defined by a function

\[ \sigma: B \rightarrow Q(\sqrt{2}, \sqrt{3}). \]

The function will then be extended to \( \sigma': Q(\sqrt{2}) \rightarrow Q(\sqrt{2}) \). Because \( \sigma \in Aut(Q(\sqrt{2})/Q) \), we have \( \sigma(1) = 1 \) because \( \sigma(a) = a \) for every \( a \in Q \). Note that,

\[ 0 = \sigma(0) = \sigma((\sqrt{2})^2 - 2) = \sigma((\sqrt{2})^2 - 2), \]

\[ 0 = \sigma(0) = \sigma((\sqrt{3})^2 - 3) = \sigma((\sqrt{3})^2 - 3) \]

So, \( \sigma((\sqrt{2})^2 = 2 \) and \( \sigma(\sqrt{2}) = \sqrt{2} \) or \( -\sqrt{2} \). Also, \( \sigma((\sqrt{3})^2 = 3 \) so that \( \sigma(\sqrt{3}) = 3 \) or \( -\sqrt{3} \). Note that \( \sigma(\sqrt{6}) = \sigma((\sqrt{2})\sigma(\sqrt{3}) \). It means \( \sigma(\sqrt{6}) \) depends on \( \sigma(3) \) and \( \sigma(\sqrt{3}) \). So, we get four automorphisms of \( Q(\sqrt{2}) \) which is defined by

\[ \sigma_1: B \rightarrow Q(\sqrt{2}, \sqrt{3}) \]

\[ \sigma_2: B \rightarrow Q(\sqrt{2}, \sqrt{3}) \]

\[ \sigma_3: B \rightarrow Q(\sqrt{2}, \sqrt{3}) \]

\[ \sigma_4: B \rightarrow Q(\sqrt{2}, \sqrt{3}) \]

\[ 1 \mapsto 1 \]

\[ \sqrt{2} \mapsto \sqrt{2} \]

\[ \sqrt{3} \mapsto \sqrt{3} \]

\[ \sqrt{6} \mapsto \sqrt{6} \]

\[ 1 \mapsto 1 \]

\[ \sqrt{2} \mapsto -\sqrt{2} \]

\[ \sqrt{3} \mapsto -\sqrt{3} \]

\[ \sqrt{6} \mapsto -\sqrt{6} \]

\[ 1 \mapsto 1 \]

\[ \sqrt{2} \mapsto \sqrt{2} \]

\[ \sqrt{3} \mapsto \sqrt{3} \]

\[ \sqrt{6} \mapsto \sqrt{6} \]

Next, we extend those four automorphisms to \( Q(\sqrt{2}, \sqrt{3}) \) defined by

\[ \sigma_i': Q(\sqrt{2}, \sqrt{3}) \rightarrow Q(\sqrt{2}, \sqrt{3}) \]

\[ a, b, \sqrt{2} + c, \sqrt{3} + d, \sqrt{6} \mapsto a, \sigma_i(1) + b, \sigma_i(\sqrt{2}) + c, \sigma_i(\sqrt{3}) + d, \sigma_i(\sqrt{6}) \]

Thus, \( Aut(Q(\sqrt{2}, \sqrt{3})/Q) = \{ \sigma_1', \sigma_2', \sigma_3', \sigma_4' \} \). Note that \( \sigma_1' = id \) and \( \sigma_4' = \sigma_2' \sigma_3' \). Hence, \( Aut(Q(\sqrt{2}, \sqrt{3})/Q) = \{ id, \sigma_2', \sigma_3', \sigma_2'\sigma_3' \} \).
Next, we will give a property of $Aut(K/F)$ in this following lemma.

**Proposition 9** [5]

If $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is the set of automorphisms of $K$ then $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is linearly independent (i.e. if $\alpha_1 \sigma_1 + \alpha_2 \sigma_2 + \cdots + \alpha_n \sigma_n = 0$ then $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$).

**Proof.**

Suppose that $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is the set of automorphisms of $K$. We will prove that $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is linearly independent using induction method on $k$ elements of the given set.

i. For $k = 1$. We take any $\sigma_i$ for $i = 1, 2, \ldots, n$ where $\alpha_i \sigma_i = 0$. It means $(\alpha_i \sigma_i)(x) = \alpha_i(\sigma_i(x)) = 0$. Note that $\sigma_i$ is a field and $\sigma_i$ is an automorphism, then we have $\sigma_i(x) \neq 0$ for every nonzero $x \in K$. Therefore, $\alpha_i = 0$.

ii. It holds for $k$ where $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ is linearly independent.

iii. We will prove that also holds for $k + 1$. Suppose that $\alpha_1 \sigma_1 + \alpha_2 \sigma_2 + \cdots + \alpha_k \sigma_k + 1 = 0$ where $\alpha_1, \alpha_2, \ldots, \alpha_k + 1 \in F$. So, for every $x \in K$

\[
(\alpha_1 \sigma_1 + \alpha_2 \sigma_2 + \cdots + \alpha_k \sigma_k + 1)(x) = 0.
\]

Thus,

\[
\alpha_1 \sigma_1(x) + \alpha_2 \sigma_2(x) + \cdots + \alpha_k \sigma_k(x) + \alpha_{k+1} \sigma_{k+1}(x) = 0.
\]

Because $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ are distinct, there is a nonzero $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$. Using equation (i), we obtain

\[
\iff \alpha_1 \sigma_1(xy) + \alpha_2 \sigma_2(xy) + \cdots + \alpha_k \sigma_k(xy) + \alpha_{k+1} \sigma_{k+1}(xy) = 0
\]

From (i), we obtain

\[
\alpha_1 \sigma_1(x) = -\alpha_2 \sigma_2(x) - \cdots - \alpha_{k+1} \sigma_{k+1}(x)
\]

Then, we substitute (iii) into (ii)

\[
\iff (\alpha_2 \sigma_2(x) - \alpha_3 \sigma_3(x) - \cdots - \alpha_{k+1} \sigma_{k+1}(x)) \sigma_1(y) + \alpha_2 \sigma_2(x) \sigma_2(y) + \cdots + \alpha_k \sigma_k(x) \sigma_k(y) + \alpha_{k+1} \sigma_{k+1}(x) \sigma_{k+1}(y) = 0
\]

Using the assumption for $k$, we obtain

\[
\alpha_2(\sigma_2(y) - \sigma_1(y)) = \alpha_2(\sigma_2(y) - \sigma_1(y)) = \cdots = \alpha_{k+1}(\sigma_{k+1}(y) - \sigma_1(y)) = 0.
\]

Note that $\alpha_2(\sigma_2(y) - \sigma_1(y)) = 0$ and $(y) \neq \sigma_1(y)$, so we have $\alpha_2 = 0$. Moreover, using (i) and $\alpha_2 = 0$, we also have

\[
\iff \alpha_1 \sigma_1(x) + \alpha_3 \sigma_3(x) + \cdots + \alpha_{k+1} \sigma_{k+1}(x) = 0
\]

Therefore, $\alpha_1 \sigma_1 + \alpha_3 \sigma_3 + \cdots + \alpha_{k+1} \sigma_{k+1} = 0$. Again, using the assumption for $n = k$, it implies that that $\alpha_1 = \alpha_3 = \cdots = \alpha_{k+1} = 0$. Hence, $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is linearly independent over $F$.

Moreover, we will give the relation between $|Aut(K/F)|$ and $[K:F]$ in the proposition below.

**Proposition 10** [5]

If $K/F$ is an extension field then $|Aut(K/F)| \leq [K:F]$.
Proof
Write $G = \text{Aut}(K/F)$. Suppose $G = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ so that $|G| = n$. Let $[K:F] = n$ and the basis of $K/F$ is $B = \{v_1, v_2, ..., v_d\}$ for some $d \in \mathbb{N}$. We will prove that $n \leq d$ using method of contradiction.

Suppose $n > d$. We form a linear equation system i.e.

$$
\begin{align*}
\sigma_1(v_1)x_1 + \sigma_2(v_1)x_2 + \cdots + \sigma_n(v_1)x_n &= 0 \\
\sigma_1(v_2)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_n(v_2)x_n &= 0 \\
\vdots \\
\sigma_1(v_d)x_1 + \sigma_2(v_d)x_2 + \cdots + \sigma_n(v_d)x_n &= 0.
\end{align*}
$$

Note that there are more variables than the number of equations. It implies there is a nonzero solution, $(x_1, x_2, \ldots, x_n)$ where $c_i \neq 0$ for some $i \in \{1, 2, \ldots, n\}$. Let $w \in K/F$. It means $w$ can be expressed as

$$w = a_1v_1 + a_2v_2 + \cdots + a_dv_d$$

where $a_1, a_2, \ldots, a_d \in F$. Then, we multiply $a_i$ to the system of equations. Thus,

$$a_1\sigma_1(v_1)x_1 + a_1\sigma_2(v_1)x_2 + \cdots + a_1\sigma_n(v_1)x_n = 0$$

$$a_2\sigma_1(v_2)x_1 + a_2\sigma_2(v_2)x_2 + \cdots + a_2\sigma_n(v_2)x_n = 0$$

$$\vdots$$

$$a_d\sigma_1(v_d)x_1 + a_d\sigma_2(v_d)x_2 + \cdots + a_d\sigma_n(v_d)x_n = 0.$$

Therefore,

$$(a_1\sigma_1(v_1) + a_2\sigma_1(v_2) + \cdots + a_d\sigma_1(v_d))c_1 + (a_1\sigma_2(v_1) + a_2\sigma_2(v_2) + \cdots + a_d\sigma_2(v_d))c_2 + \cdots + (a_1\sigma_n(v_1) + a_2\sigma_n(v_2) + \cdots + a_d\sigma_n(v_d))c_n = 0$$

and

$$\sigma_1(a_1v_1 + a_2v_2 + \cdots + a_dv_d.c_1 + a_1v_1 + a_2v_2 + \cdots + a_dv_d.c_2 + \cdots + a_1v_1 + a_2v_2 + \cdots + a_dv_d.c_n = 0.$$

So, $c_1, \sigma_1(w) + c_2, \sigma_2(w) + \cdots + c_n\sigma_n(w) = 0$ and $(c_1, c_2, \ldots, c_n)(w) = 0$. It holds for every $w \in K/F$. It implies that $\sigma_1 + \sigma_2 + \cdots + \sigma_d = 0$. Note that there is $c_i \neq 0$ for some $i = 1, 2, \ldots, n$. Hence, $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is linearly independent. It implies contradiction with Proposition 7. Hence, $n \leq d$ that is $|G| \leq [K:F]$. \[\square\]

Based on Proposition 10, we have $|\text{Aut}(K/F)| \leq [K:F]$. However, the equality does not always hold to all extension fields. We will give an example to describe it.

Example 11
Given an extension field $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. From Example 4, we know that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} + c\sqrt{2} \mid a, b, c \in \mathbb{Q}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. So, $\{1, \sqrt{2}, \sqrt{2}^2\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. We also have $\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id\}$. Thus, $[\mathbb{Q}(\sqrt{2})/\mathbb{Q}] = 3$ and $|\text{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 1$.

Based on the example above, it then motivates the definition of Galois extension. We will give the definition of Galois extension on the following definition.

Definition 12[5]
Let $K/F$ be a finite extension field. $K$ is called Galois extension over $F$ if $|\text{Aut}(K/F)| = [K:F]$.

It’s common to write the automorphism $\text{Aut}(K/F)$ as $\text{Gal}(K/F)$ when $K$ is a Galois extension and is called Galois group of $K/F$. Next, we will give example of a Galois extension and a non-Galois extension in the following example.
Example 13
i. Using Example 6, we have $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension. Because the basis of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is $\{1, \sqrt{2}\}$. We obtain $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma_2\}$. Thus, $|Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2$. Hence, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension field over $\mathbb{Q}$.

ii. Based on Example 7, we know that $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is not a Galois extension because $Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id\}$ and the basis of $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is $\{1, \sqrt{3}\}$. So, $|Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{3}): \mathbb{Q}] = 2$.

Let $K/F$ be an extension field and $Aut(K/F)$ be the automorphism group of $K/F$. For every, $S \subseteq Aut(K/F)$, we form a subset of $K$ defined by

$$K^S = \{x \in K | \sigma(x) = x, \forall \sigma \in S \}.$$

Note that $\forall a, b \in K^S$ dan $\sigma \in S$, we obtain

$$\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$$

and

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)(\sigma(b))^{-1} = ab^{-1}.$$

Therefore, $K^S$ is a subfield in $K$ containing $F$ and is called the fixed field of $S$ [5]. In other words, $S$ fixed all elements in $K^S$.

Example 14
Using Example 6, we have $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We obtain $G = Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma_2\}$ where

$$id: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$$

$$a.1 + b.\sqrt{2} \mapsto a.\sigma_1(1) + b.\sigma_1(\sqrt{2})$$

and

$$\sigma_2': \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$$

$$a.1 + b.\sqrt{2} \mapsto a.\sigma_1(1) + b.\sigma_1(-\sqrt{2})$$

Thus, $id(a.1) = a$ and $\sigma_2'(a.1) = a$ where $a \in \mathbb{Q}$. Hence, $\mathbb{Q}(\sqrt{2})^G = \mathbb{Q}$.

Let $K/F$ be an extension field where it automorphism group is $G = Aut(K/F)$. Suppose $H$ is a subgroup in $H$. Next, we will give a property related to fixed field of a $H$ which is denoted by $K^H$ in this following Lemma.

Theorem 15 [5]
Let $K/F$ be an extension field where $[K:F] < \infty$. If $K^G = F$ then $[K:F] = |Aut(K/F)|$.

Proof.
Let $[K:F] = d$ and $|Aut(K/F)| = n$. Based on Proposition 10, we have $d \geq n$. Next, we will prove that $d \leq n$ using method of contradiction.

Suppose $d > n$. Thus, there exist $n + 1$ elements $v_1, v_2, \ldots, v_{n+1}$ which are linearly independent over $F$. Then, we construct the following system of equations

$$\sigma_1(v_1)x_1 + \sigma_1(v_2)x_2 + \cdots + \sigma_1(v_{n+1})x_{n+1} = 0$$

$$\sigma_2(v_1)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_2(v_{n+1})x_{n+1} = 0$$

$$\vdots$$

$$\sigma_n(v_1)x_1 + \sigma_n(v_2)x_2 + \cdots + \sigma_n(v_{n+1})x_{n+1} = 0.$$

Note that there are more variables than the number of equations. It implies there is a non-trivial solution, $\left( \begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_{n+1} \end{array} \right) = \left( \begin{array}{c} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n+1} \end{array} \right)$ where $\alpha_i \neq 0$ for some $i \in \{1,2, \ldots, n + 1\}$. Among all non-trivial solutions, we choose $r$ as the least number of nonzero elements. Moreover, $r \neq 1$ because $\sigma_i(v_1)\alpha_i = 0$ implies $\sigma_i(v_1) = 0$ and $v_1 = 0$. 

23
i. We will prove that there exists a non-trivial solution where $\alpha_i$ are in $F$ for any $i \in \{1, 2, ..., n + 1\}$. Supposing 
\[
\begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_r \\
0 \\
0
\end{pmatrix}
\] is a non-trivial solution with $r$ non-zero elements where $\alpha_1, \alpha_2, ..., \alpha_r \neq 0$. We obtain a new non-trivial solution by multiplying the given solution with $\frac{1}{\alpha_r}$, which is
\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_r \\
0 \\
0
\end{pmatrix} = \begin{pmatrix}
\alpha_1/\alpha_r \\
\alpha_2/\alpha_r \\
\vdots \\
1 \\
0 \\
0
\end{pmatrix}.
\] Thus,
\[
\beta_1 \sigma_i(v_1) + \beta_2 \sigma_i(v_2) + \cdots + 1. \sigma_i(v_{n+1}) = 0
\] (*)

For $i = 1, 2, ..., n$. Now, we will show that $\beta_i$ are in $F$ for any $i \in \{1, 2, ..., n + 1\}$ using method of contradiction. Suppose there exists $\beta_i \notin F$, say $\beta_i$. We know that $F = K^G$ so that $\beta_i$ is not an element of the fixed field. In other words, there exists $\sigma_k \in G$ where $\sigma_k(\beta_i) \neq \beta_i$. So, $\sigma_k(\beta_i) - \beta_i \neq 0$. Since $G$ is a group, it implies $\sigma_k G = G$. It means for any $\sigma_i \in G$, we obtain $\sigma_i = \sigma_k \sigma_j$ for $j = 1, 2, ..., n$. Applying $\sigma_k$ to the expressions of (*)
\[
\Leftrightarrow \sigma_k(\beta_1 \sigma_i(v_1)) = \sigma_k(\beta_2 \sigma_i(v_2)) + \cdots + 1. \sigma_i(v_{n+1}) = 0
\] for $j = 1, 2, ..., n$ so that from $\sigma_i = \sigma_k \sigma_j$. We obtain
\[\sigma_k(\beta_1 \sigma_i(v_1)) = \sigma_k(\beta_2 \sigma_i(v_2)) + \cdots + 1. \sigma_i(v_{n+1}) = 0 \] (**)

Subtracting (*) and (**), we have
\[
(\beta_1 - \sigma_k(\beta_1)) \sigma_i(v_1) + (\beta_2 - \sigma_k(\beta_2)) \sigma_i(v_2) + \cdots + (\beta_{n+1} - \sigma_k(\beta_{n+1})) \sigma_i(v_{n+1}) = 0
\] which is a non-trivial solution because $\sigma_k(\beta_1) \neq \beta_1$ and is having $r - 1$ non-zero elements, contrary to the choice of $r$ as the minimality. Hence, 
\[
\begin{pmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_r \\
0 \\
0
\end{pmatrix}
\]
 is a non-trivial where all $\beta_i \in F$ for any $i = 1, 2, ..., n$.

ii. Using (i), we obtain a nonzero solution with all elements are in $F$. So, using the first equation in the system, we obtain
\[
\sigma_i(v_1)\beta_1 + \sigma_i(v_2)\beta_2 + \cdots + \sigma_i(v_{n+1})\beta_r = 0
\]
\[
\sigma_i(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_{n+1}) = 0.
\]
Because $\sigma_i$ is an automorphism, we obtain $\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_{n+1} = 0$ where $\beta_1, \beta_2, ..., \beta_r$ are nonzero elements in $K$. It is contrary to $v_1, v_2, ..., v_{n+1}$ which are linearly independent over $F$.

Thus, we have $d \leq n$. Hence, $d = n$ i.e. $[K:F] = |Aut(K/F)|$. ■

Next, we will give a necessary and sufficient condition for $K/F$ is Galois using its fixed field.

**Corollary 16[5]**

Let $K/F$ be an extension field where $[K:F] < \infty$ with its automorphism group $G = Aut(K/F)$. The field $K/F$ is a Galois extension over $F$ if and only if $K^G = F$.

**Proof.**

$(\Rightarrow)$ We have $K$ is a Galois extension over $F$. It means $[K:F] = |Aut(K/F)|$. We will show that $K^G = F$. We know that $K^G$ is a subfield of $K$ and $F \subseteq K^G \subseteq K$. Based on **Lemma 5** and **Theorem 15**, we obtain

(\Rightarrow) We know that $K^G = F$. Using Theorem 15, we have $|K: K^G| = |K: F|$. Thus, $K$ is a Galois extension over $F$. $lacksquare$

Let $K/F$ be an extension field with its automorphism group $G = Aut(K/F)$. Using the Corollary above, we can determine that $K/F$ is a Galois extension by showing that the fixed field of its automorphism group $G$ is $F$ itself (that is $K^G = F$).

Lemma 17 [5]
Let $K/F$ be an extension field and $E$ be an intermediate field of $K/F$ that is $F \subseteq E \subseteq K$. The automorphism group $Aut(K/E)$ is a subgroup in $Aut(K/F)$.

Proof.
Let $K/F$ be an extension field and $E$ be an intermediate field of $K/F$. Write $G = Aut(K/F)$. Note that $K/E$ is an extension field. So, $H = Aut(K/E)$ is the automorphism group of $K/E$ where

\[ Aut(K/E) = \{ \sigma : K \to K \text{ automorphism } | \sigma(x) = x \text{ for all } x \in E \} \]

Moreover, let $\sigma \in H$. It means, $\sigma(x) = x$ for all $x \in E$. Because $F \subseteq E$, so $\sigma(x) = x$ for all $x \in F \subseteq E$. Thus, $\sigma \in Aut(K/F) = G$. Hence, $H$ is group and a subset in $G$. It implies that $H$ is a subgroup of $G$. $lacksquare$

Lemma 18 [5]
Let $K/F$ be Galois extension field. If $E$ is an intermediate field of $K/F$ then $K/E$ is a Galois extension.

Proof.
Let $K/F$ be Galois extension field. If $E$ is an intermediate field of $K/F$. We have, $K/E$ is an extension field with its automorphism group $H = Aut(K/E)$. Based on Corollary 16, we will prove that $K/E$ is a Galois extension by showing that $E$ is the fixed field of its automorphism group $Aut(K/E)$ i.e. $E = K^{Aut(K/E)}$. Write $G = Aut(K/F)$.

Suppose $H$ is a subgroup of $G$ where its fixed field is $E$ i.e. $E = K^H$.

i. First, we will show that $H \subseteq Aut(K/E)$. Let $\sigma \in H \subseteq G$. We know that $H$ fixes all element in $E$. So, $\sigma(x) = x$ for all $x \in E$. Using the definition of $Aut(K/E)$, we have $\sigma \in Aut(K/E)$. Thus, $H \subseteq Aut(K/E)$ and $|H| \leq |Aut(K/K^H)|$. Based on Theorem 15, we have

\[ |K: K^H| = |H|. \]

Note that $K/K^H$ is an extension field, so $|Aut(K/K^H)| \leq |K: K^H|$ based on Proposition 10. Therefore,

\[ |H| \leq |Aut(K/K^H)| \leq |K: K^H| = |H|. \]

Thus, $|H| = |Aut(K/K^H)|$. Because $|H|$ and $|Aut(K/K^H)|$ are finite and also $H \subseteq Aut(K/E)$, it implies $H = Aut(K/K^H) = Aut(K/E)$. In other words, $E$ is the fixed field of $Aut(K/E)$.

ii. We have $E$ is the fixed field of $Aut(K/E)$ from (i). It means, $E = K^{Aut(K/E)}$. Using Corollary 16, we have $K/E$ is a Galois extension with Galois group $H = Aut(K/K^H) = Aut(K/E)$. $lacksquare$

Let $K/F$ be a Galois extension field where $Aut(K/F)$ is the automorphism group of $K/F$. We know that for all subgroups in $G$, we can form an intermediate subfield in $K$. Suppose

$\mathcal{H}$ is the set of all subgroups in $G$, and

$\mathcal{F}$ is the set of all intermediate field of $K/F$.

We can form a function between $\mathcal{H}$ and $\mathcal{F}$ defined by

$\rho : \mathcal{H} \to \mathcal{F}$

$H \mapsto K^H$

for all $H \in \mathcal{H}$. In other words, $H$ is mapped to its fixed field $K^H$. Using the property of $K/F$ as a Galois extension, we will show that there is a one-one correspondence between $\mathcal{H}$ and $\mathcal{F}$ that is $\rho$ is bijective.
Theorem 19[5]
Let $K/F$ be an extension field. If $K$ is a Galois extension then there is an one-one correspondence between intermediate field $E$ of $K/F$ and subgroups $H$ of $G$ defined by
\[ \rho: \mathcal{H} \rightarrow \mathcal{F} \]
\[ H \mapsto K^H. \]

Proof
Let $K/F$ be a Galois extension field where $Aut(K/F)$ is the automorphism group of $K/F$. We will show that there is a one-one correspondence between $\mathcal{H}$ and $\mathcal{F}$ that is $\rho$ is bijective.

i. Suppose $E$ is an intermediate field. From Lemma 18, we have $K/E$ is a Galois extension with its Galois group $H = Aut(K/E)$. We know that $H$ is a subgroup in $G$. Thus, $E$ is the fixed field of $H$ that is $E = K^H = \rho(H)$. Hence, $\rho$ is surjective.

ii. Let $H_1, H_2 \in \mathcal{H}$ where $G$ where $\rho(H_1) = \rho(H_2)$ that is $K^{H_1} = K^{H_2}$. Note that $K/K^{H_1}$ and $K/K^{H_2}$ are Galois extensions by Lemma 18. So, $H_1 = Aut(K/K^{H_1})$ and $H_2 = Aut(K/K^{H_2})$. Also, note that $K^{H_1} = K^{H_2}$ so that $K^{H_1}$ is the fixed field of $H_2$. Thus, $H_2 \subseteq Aut(K/K^{H_1}) = H_1$. Analogously, $K^{H_2} = K^{H_1}$. We have, $K^{H_2}$ is the fixed field of $H_1$. Hence, $H_1 \subseteq Aut(K/K^{H_2}) = H_2$. Therefore, $H_1 = H_2$. Hence, $\rho$ is injective.

From (i) and (ii), it implies that, $\rho$ is bijective so that there is an one-one correspondence between set of all subgroups in $G$ and the set of all intermediate field of $K/F$. ■

Next, we will describe the Galois correspondence using Galois extension field $Q(\sqrt[3]{2}, \sqrt[3]{3})/Q$ in the following example.

Example 20
Using Example 8, we have $Q(\sqrt[3]{2}, \sqrt[3]{3})/Q$ is a Galois extension where its basis $B = \{1, \sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{6}\}$ and $G = Aut(Q(\sqrt[3]{2}, \sqrt[3]{3})/Q) = \{ id, \sigma_2, \sigma_3, \sigma_2 \sigma_3 \}$. Note that $Aut(Q(\sqrt[3]{2}, \sqrt[3]{3})/Q)$ is a Klein group generated by $\{\sigma_2, \sigma_3\}$. Next, we will find all intermediate fields of $Q(\sqrt[3]{2}, \sqrt[3]{3})/Q$ using the Galois correspondence. Since $G$ is a Klein group, we can compute all subgroups in $G$ which are

\[ H_1 = \{id\} \quad H_2 = \{id, \sigma_2\} \quad H_3 = \{id, \sigma_3\} \quad H_4 = \{id, \sigma_2 \sigma_3\} \quad H_5 = G. \]

Using the set of all subgroups which is $\{H_1, H_2, H_3, H_4, H_5\}$, we will find all intermediate fields of $Q(\sqrt[3]{2}, \sqrt[3]{3})/Q$ using the correspondence between

$\mathcal{H}$ is the set of all subgroups in $G$, and
\[ \mathcal{F} \]

is the set of all intermediate field of $Q(\sqrt[3]{2}, \sqrt[3]{3})/Q$ defined by
\[ \rho: \mathcal{H} \rightarrow \mathcal{F} \]
\[ H_i \mapsto K^{H_i} \]
for all $i = 1, 2, 3, 4$. Note that each automorphism in $G$ defined by

\[ id: Q(\sqrt[3]{2}, \sqrt[3]{3}) \rightarrow Q(\sqrt[3]{2}, \sqrt[3]{3}) \]
\[ a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \mapsto a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \]
\[ \sigma_2: Q(\sqrt[3]{2}, \sqrt[3]{3}) \rightarrow Q(\sqrt[3]{2}, \sqrt[3]{3}) \]
\[ a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \mapsto a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \]
\[ \sigma_3: Q(\sqrt[3]{2}, \sqrt[3]{3}) \rightarrow Q(\sqrt[3]{2}, \sqrt[3]{3}) \]
\[ a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \mapsto a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \]
\[ \sigma_2 \sigma_3: Q(\sqrt[3]{2}, \sqrt[3]{3}) \rightarrow Q(\sqrt[3]{2}, \sqrt[3]{3}) \]
\[ a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \mapsto a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \]

for every $a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} \in Q(\sqrt[3]{2}, \sqrt[3]{3})$. Therefore, the fixed of fields of each automorphism is
\[ K^{[id]} = \{ a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{3} + d.\sqrt[3]{6} | a, b, c, d \in Q \} = Q(\sqrt[3]{2}, \sqrt[3]{3}) \]
\[ K^{[\sigma_2]} = \{ a.1 + c.\sqrt[3]{3} | a, c \in Q \} = Q(\sqrt[3]{3}) \]
\[ K^{[\sigma_3]} = \{ a.1 + b.\sqrt[3]{2} | a, b \in Q \} = Q(\sqrt[3]{2}) \]
\[ K^{[\sigma_2 \sigma_3]} = \{ a.1 + d.\sqrt[3]{6} | a, d \in Q \} = Q(\sqrt[3]{6}) \].
Thus, the fixed field for each subgroups are
\[ K^{H_1} = K^{(id)} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \]
\[ K^{H_2} = K^{(id, \sigma_2')} = K^{(id)} \cap K^{[\sigma_2']} = \mathbb{Q}(\sqrt{3}) \]
\[ K^{H_3} = K^{(id, \sigma_3')} = K^{(id)} \cap K^{[\sigma_3']} = \mathbb{Q}(\sqrt{2}) \]
\[ K^{H_4} = K^{(id, \sigma_2' \sigma_3')} = K^{(id)} \cap K^{[\sigma_2' \sigma_3']} = \mathbb{Q}(\sqrt{6}) \]
\[ K^{H_5} = K^G = K^{(id)} \cap K^{[\sigma_2']} \cap K^{[\sigma_3']} \cap K^{[\sigma_2' \sigma_3']} = \mathbb{Q} \]

Therefore,
\[
\begin{align*}
\rho: \mathcal{H} & \rightarrow \mathcal{F} \\
H_1 & \mapsto \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\
H_2 & \mapsto \mathbb{Q}(\sqrt{3}) \\
H_3 & \mapsto \mathbb{Q}(2) \\
H_4 & \mapsto \mathbb{Q}(\sqrt{6}) \\
H_5 & \mapsto \mathbb{Q}.
\end{align*}
\]

Hence, the set of all intermediate fields of \( \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q} \) is \( \{ \mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{6}) \text{ and } \mathbb{Q} \} \). Furthermore, we will describe the correspondence using the diagram below.

CONCLUSION

Let \( K/F \) be an extension field with its automorphism group \( G = \text{Aut}(K/F) \).
1. The field \( K/F \) is Galois extension if and only if the fixed field of \( G \) is \( F \) itself.
2. If \( K/F \) is a Galois extension then there is one-one correspondence between the set of all intermediate subfields of \( K/F \) and the set of all subgroups in \( G \).

REFERENCES