TENSOR
Pure and Applied Mathematics Journal

April 2023 | Vol. 4 | No. 1 Halaman 1–12
p-ISSN: 2723-0325 e-ISSN: 2723-0333

BASIC PROPERTIES OF GALOIS CORRESPONDENCE

Novita Dahoklory[1]*, Henry W. M. Patty [1]

[1] Algebra and Analysis Division, Department of Mathematics, Faculty of Mathematics and Natural Sciences, Pattimura University, Jl. Ir. M. Putuhena, Ambon. Indonesia
Email: novitadahoklory93@gmail.com

Manuscript submitted : March 2023
Accepted for publication : April 2023
doi : https://doi.org/10.30598/tensorvol4iss1pp1-12

Abstract:

Let K, F be fields where $F \subseteq K$. The field K is called an extension field over K denoted by K/F. In this research, we assume K/F to be a Galois extension with its Galois group $G = Gal(K/F)$. Using the properties of K/F as a Galois extension, we will show that there is a one-one correspondence between the set of all intermediate subfields of K/F and the set of all subgroups in G. Furthermore, we will give some basic properties related to Galois correspondence.

2010 Mathematical Subject Classification : 11R32, 13B05
Keywords: Extension field, Galois field, Galois group, Galois correspondence

1. Introduction

Let F, K be fields. The field K is called an extension field of K if $F \subseteq K$ (denoted by K/F) [3]. Therefore, K can be viewed as a vector space over F. Suppose B is a basis of K. Therefore, the number of elements in B is called the dimension of K denoted by $[K\colon F]$. In particular, if $[K\colon F] < \infty$ then K/F is called a finite extension field [1].

Moreover, we form the set of all automorphisms of K defined by

$$Aut(K/F) = \{\sigma\colon K \to K \ automorphism | \sigma(x) = x \ (\forall x \in F)\}.$$

The set $Aut(K/F)$ is a group under the composition operation [1]. The order of $Aut(K/F)$ is the number of elements consisted in $Aut(K/F)$ denoted by $|Aut(K/F)|$. In particular, an extension field K/F is called Galois extension if $|Aut(K/F)| = [K\colon F]$. Moreover if K/F is a Galois extension $Aut(K/F)$ is commonly written as $Gal(K/F)$ and is called Galois group of K/F.

Suppose K/F be a Galois extension with its Galois group $G = Gal(K/F)$. Let E be an intermediate field in K/F that is $F \subseteq E \subseteq K$. Therefore, we can form two extension fields E/F and K/E. It shows that K/E is also a Galois extension [2]. However, E/F is not always a Galois extension. For example, let K/F with an intermediate field E where $K = \mathbb{Q}(\sqrt[4]{3}, i)$, $F = \mathbb{Q}$, and $E = \mathbb{Q}(\sqrt[4]{3})$, we know that K/E is Galois while E/F is not a Galois extension.

In this paper, we will assume K/F be a Galois extension with its Galois group $G = Gal(K/F)$. We will show that there is a one-one correspondence between the set of all intermediate subfields of K/F and the set of all subgroups in G. Moreover, we will discuss basic properties related to Galois correspondence. Furthermore, we will give a condition for E/F to be a Galois extension using the Galois correspondence. The correspondence of Galois group has been developed especially in Hopf algebra and in [3],[4],[5],[6].

We refer to [7],[8],[9],[10] for some basic theories including groups in particular automorphism group and vector spaces. For extension fields in particular Galois extension fields, this research is based on [11],[12] .

2. SOME RESULTS

2.1. Finite Extension Fields

In this part we will discuss extension fields in particular finite extension fields. We will also give some properties of finite extension fields. We first study the role of an extension field as a vector space.

Definition 1[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

i. $\mathbb{R}$ is an extension field of $\mathbb{Q}$.

ii. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is an extension field of $\mathbb{Q}$.

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

Let K/F be an extension field. We know that K can be viewed as a vector space over F and has a basis where the dimension of K over F is denoted by $[K: F]$. Next, we will give the definition of a finite extension field.

Definition 3 [1]
Let K/F is an extension field. The field K is called a **finite extension of** F if $[K: F] < \infty$.

In other words, the extension field K/F is called finite if the number of the basis of K is finite. Next, we will give an example of a finite extension field.

Example 4

i. Let $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ be an extension field. Every $x \in \mathbb{Q}(\sqrt{2})$ can be expressed by
$$x = a + b\sqrt{2}$$
for some $a, b \in \mathbb{Q}$. So, 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, $B = \{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Hence, $[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2$.

ii. Given $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ an extension field where every element in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written as
$$y = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
for some $a, b, c, d \in \mathbb{Q}$. Note that $C = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Hence, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}): \mathbb{Q}] = 4$

Therefore, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ are finite extensions.

Next, we will assume that an extension field K/F as a finite extension field.

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[1]
If K, E, F are fields where $F \subseteq E \subseteq K$ then $[K: F] = [K: E]. [E: F]$.

Proof

Suppose $[K:E]=m$ and $[E:F]=n$ where $m,n\in\mathbb{N}$. Next, we will show that $[K:F]=[K:E].[E:F]=mn$. Let $B=\{v_1,v_2,\dots,v_m\}$ and $C=\{v_1,v_2,\dots,v_m\}$ be a basis for K/E and E/F, respectively. It is clear that K is a vector space over E so that any $x\in K$ can be expressed as

$$x=\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_mv_m.$$

for $\alpha_1,\alpha_2,\dots,\alpha_m\in E$. Note that E is a vector space over F, we get

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

for $i=1,2,\dots,m$. We have

$$\begin{aligned}x&=(\beta_{11}w_1+\beta_{12}w_2+\cdots+\beta_{1n}w_n)v_1+\cdots+(\beta_{m1}w_1+\beta_{m2}w_2+\cdots+\beta_{mn}w_n)v_m\\&=\beta_{11}v_1w_1+\beta_{12}v_1w_2+\cdots+\beta_{1n}v_1w_n+\cdots+\beta_{m1}v_mw_1+\beta_{m2}v_mw_2+\cdots+\beta_{mn}v_mw_n.\end{aligned}$$

Write $B=\{v_iw_j|i=1,2,\dots,m,\ j=1,2,\dots,n\}$. Thus, K is generated by B. Moreover, we will show that B is linearly independent. Suppose that

$$c_{11}v_1w_1+c_{12}v_1w_2+\cdots+c_{1n}v_2w_n+\cdots+c_{m1}v_mw_1+c_{m2}v_mw_2+\cdots+c_{mn}v_mw_n=0.$$

We have

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

Since $\{v_1,v_2,\dots,v_m\}$ is linearly independent, we obtain $c_{i1}w_1+c_{i2}w_2+\cdots+c_{in}w_n=0$ for $i=1,2,\dots,m$. Also, since $\{w_1,w_2,\dots,w_n\}$ is linearly independent, it implies $c_{i1}=c_{i2}=\cdots=c_{in}=0$. Thus, $c_{ij}=0$ for $i=1,2,\dots,m$ and $j=1,2,\dots,n$. Therefore, B is a basis of K over F. Hence, $B=\{v_iw_j|i=1,2,\dots,m,\ j=1,2,\dots,n\}$ and $[K:F]=mn$. ■

2.2. Galois Extension Fields

In this part , we will explain Galois extension fields. First, we will describe the automorphism group from an extension field K/F.

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

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

$Aut(K/F)$ is a group under the operation of composition and is called **the automorphism group of K/F** [5].

Next, we will give an example of $Aut(K/F)$ of an extension field K/F.

Example 6

Suppose an extension field K/F where $K=\mathbb{Q}(\sqrt{2}),F=\mathbb{Q}$ with its basis $B=\{1,\sqrt{2}\}$. We can form an automorphism of K defined by

$$\rho:B\to\mathbb{Q}(\sqrt{2}).$$

The function will then be extended to

$$\begin{gathered}\rho':\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2})\\a+b\sqrt{2}\mapsto a\rho(1)+b\rho(\sqrt{2})\end{gathered}$$

for all $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. Since $\sigma\in Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, we have

$$\sigma(1)=1\ \text{ so that }\ \sigma(a)=\sigma(1.a)=a.\sigma(1)=a.1=a$$

for every $a\in\mathbb{Q}$. Note that,

$$0=\sigma(1)=\sigma\left(\left(\sqrt{2}\right)^2-2\right)=\sigma(\sqrt{2})^2-2.$$

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

$$\begin{gathered}\sigma_1:B\to\mathbb{Q}(\sqrt{2})\\1\mapsto1\\\sqrt{2}\mapsto\sqrt{2}\end{gathered}$$

and

$$\begin{gathered}\sigma_2:B\to\mathbb{Q}(\sqrt{2})\\1\mapsto1\\\sqrt{2}\mapsto-\sqrt{2}.\end{gathered}$$

Then, those two functions are extended to

$$\sigma_1{}': \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a.1 + b.\sqrt{2} \mapsto a.\sigma_1(1) + b.\sigma_1(\sqrt{2})$$

and

$$\sigma_2: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a.1 + b.\sqrt{2} \mapsto a.\sigma_1(1) + b.\sigma_1(-\sqrt{2})$$

Therefore, $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1{}', \sigma_2{}'\} = \{id, \sigma_2\}$.

Next, we will give a property of automorphism group of an extension field K/F.

Proposition 7[5]
If $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is the set of automorphisms of K then $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ 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 $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is the set of automorphisms of K. We will prove that $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is linearly independent using the induction method on k elements of the given set.

i. For $k = 1$. We take any σ_i for $i = 1,2, \dots, n$ where $\alpha_i\sigma_i = 0$. It means $(\alpha_1\sigma_1)(x) = \alpha_1(\sigma_1(x)) = 0$. Note that K is a field and σ_i is an automorphism, then we have $\sigma_1(x) \neq 0$ for every nonzero $x \in K$. Therefore, $\alpha_i = 0$.

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

iii. We will prove that also holds for $k + 1$. Suppose that

$$\alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_{k+1}\sigma_{k+1} = 0$$

where $\alpha_1, \alpha_2, \dots, \alpha_{k+1} \in F$. So, for every $x \in K$

$$(\alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_{k+1}\sigma_{k+1})(x) = 0.$$

Thus,

$$\alpha_1\sigma_1(x) + \alpha_2\sigma_2(x) + \cdots + \alpha_{k+1}\sigma_{k+1}(x) = 0. \qquad (1)$$

Because $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ are distinct, there is a nonzero $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$. Using equation (1), we obtain

$$\Leftrightarrow \alpha_1\sigma_1(xy) + \alpha_2\sigma_2(xy) + \cdots + \alpha_{k+1}\sigma_{k+1}(xy) = 0$$
$$\Leftrightarrow \alpha_1\sigma_1(x)\sigma_1(y) + \alpha_2\sigma_2(x)\sigma_2(y) + \cdots + \alpha_{k+1}\sigma_{k+1}(x)\sigma_{k+1}(y) = 0 \qquad (2)$$

From (1), we obtain

$$\alpha_1\sigma_1(x) = -\alpha_2\sigma_2(x) - \cdots - \alpha_{k+1}\sigma_{k+1}(x) \qquad (3)$$

Then, we substitute (iii) to (ii)

$$\Leftrightarrow (-\alpha_2\sigma_2(x) - \alpha_3\sigma_3(x) - \cdots - \alpha_{k+1}\sigma_{k+1}(x))\sigma_1(y) + \alpha_2\sigma_2(x)\sigma_2(y) + \cdots + \alpha_{k+1}\sigma_{k+1}(x)\sigma_{k+1}(y) = 0$$
$$\Leftrightarrow -\alpha_2\sigma_2(x)\sigma_1(y) - \alpha_3\sigma_3(x)\sigma_1(y) \dots - \alpha_{k+1}\sigma_{k+1}(x)\sigma_1(y) + \alpha_2\sigma_2(x)\sigma_2(y) + \cdots + \alpha_{k+1}\sigma_{k+1}(x)\sigma_{k+1}(y) = 0$$
$$\Leftrightarrow -\alpha_2\sigma_2(x)\sigma_1(y) - \alpha_3\sigma_3(x)\sigma_1(y) - \cdots - \alpha_{k+1}\sigma_{k+1}(x)\sigma_1(y) + \alpha_2\sigma_2(x)\sigma_2(y) + \alpha_3\sigma_3(x)\sigma_3(y) + \cdots + \alpha_{k+1}\sigma_{k+1}(x)\sigma_{k+1}(y) = 0$$
$$\Leftrightarrow \alpha_2\sigma_2(x)(\sigma_2(y) - \sigma_1(y)) + \alpha_3\sigma_3(x)(\sigma_3(y) - \sigma_1(y)) \dots + \alpha_{k+1}\sigma_{k+1}(x)(\sigma_{k+1}(y) - \sigma_1(y)) = 0$$
$$\Leftrightarrow \alpha_2(\sigma_2(y) - \sigma_1(y))\sigma_2(x) + \alpha_3(\sigma_3(y) - \sigma_1(y))\sigma_3(x) + \cdots + \alpha_{k+1}(\sigma_{k+1}(y) - \sigma_1(y))\sigma_{k+1}(x) = 0$$
$$\Leftrightarrow (\alpha_2(\sigma_2(y) - \sigma_1(y))\sigma_2 + \alpha_3(\sigma_3(y) - \sigma_1(y))\sigma_3 \dots + \alpha_{k+1}(\sigma_{k+1}(y) - \sigma_1(y))\sigma_{k+1})\ (x) = 0$$

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

$$\Leftrightarrow \alpha_1\sigma_1(x) + \alpha_3\sigma_3(x) \dots + \alpha_{k+1}\sigma_{k+1}(x) = 0$$
$$\Leftrightarrow (\alpha_1\sigma_1 + \alpha_3\sigma_3 + \cdots + \alpha_{k+1}\sigma_{k+1})(x) = 0.$$

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, $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is linearly independent over F. ■

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

Proposition 8 [1]
If K/F is an extension field then $|Aut(K/F)| \leq [K: F]$.

Proof
Write $G = Aut(K/F)$. Suppose $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ so that $|G| = n$. Let $[K: F] = n$ and the basis of K/F is $B = \{v_1, v_2, \dots, v_d\}$ for some $d \in \mathbb{N}$. We will prove that $n \leq d$ using a method of contradiction. Suppose $n > d$. We form a linear equation system i.e.

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

Note that there are more variables than the number of equations. It implies there is a nonzero solution, $\begin{pmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{pmatrix} = \begin{pmatrix} c_1\\ c_2\\ \vdots\\ c_n\end{pmatrix}$ where $c_i \neq 0$ for some $i \in \{1,2,\dots,n\}$. Let $w \in K/F$. It means w can be expressed as

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

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

$$\begin{gathered}a_1\sigma_1(v_1)x_1 + a_1\sigma_2(v_1)x_2 + \cdots + a_1\sigma_n(v_1)x_n = 0\\ a_2\sigma_1(v_2)x_1 + a_2\sigma_2(v_2)x_2 + \cdots + a_2\sigma_n(v_2)x_n = 0\\ \vdots\\ a_d\sigma_1(v_d)x_1 + a_d\sigma_2(v_d)x_2 + \cdots + a_d\sigma_n(v_d)x_n = 0.\end{gathered}$$

Therefore,

$$\begin{aligned}&(a_1\sigma_1(v_1) + a_2\sigma_1(v_2) + \cdots + a_d\sigma_1(v_d))c_1 + (a_1\sigma_2(v_1) + a_2\sigma_2(v_2) + \cdots + a_d\sigma_2(v_d))c_2 + \cdots + (a_1\sigma_n(v_1)\\ &\qquad + a_2\sigma_n(v_2) + \cdots + a_d\sigma_n(v_d))c_n = 0\end{aligned}$$

and

$$\begin{aligned}&\sigma_1(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_1 + \sigma_2(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_2 + \cdots + \sigma_n(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_n\\ &\qquad = 0.\end{aligned}$$

So, $c_1.\sigma_1(w) + c_2.\sigma_2(w) + \cdots + c_n\sigma_n(w) = 0$ and $(c_1\sigma_1 + c_1\sigma_2 + \cdots + c_n\sigma_n)(w) = 0$. It holds for every $w \in K/F$. It implies that $\alpha_1\sigma_1 + \alpha_2\sigma_2 + \cdots + \alpha_n\sigma_d = 0$. Note that there is $c_i \neq 0$ for some $i = 1,2,\dots,n$. Hence, $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is linearly independent. It implies contradiction with **Proposition 7**. Hence, $n \leq d$ that is $|G| \leq [K: F]$. ■

Definition 9[2]
Let K/F be a finite extension field. K is called **Galois extension over** F if $|Aut(K/F)| = [K: F]$.

It is common to write the automorphism $Aut(K/F)$ as $\boldsymbol{Gal(K/F)}$ when K/F is a Galois extension. Next, we will give an example of a Galois extension and a non-Galois extension in these following examples.

Example 10
Suppose an extension field K/F where $K = \mathbb{Q}(\sqrt[4]{3}, i), F = \mathbb{Q}$ where

$$\mathbb{Q}(\sqrt[4]{3}, i) = \{a + b\sqrt[4]{3} + C.\sqrt{3} + d.\sqrt[4]{27} + e.i + f.\sqrt[4]{3}i + g.\sqrt{3}i + h.\sqrt[4]{27}i\ |a,b,c,d,e,f,g,h \in \mathbb{Q}\}.$$

Therefore, $B = \{1, \sqrt[4]{3}, \sqrt{3}, \sqrt[4]{27}, i, \sqrt[4]{3}i, \sqrt{3}i, \sqrt[4]{27}i\}$ is a basis of K. Therefore, $[K: F] = 8$. Next, we will use the same way from **Example 6** to find all automorphisms of K. Take any $\sigma \in Aut(K/F)$. Using the properties of $Aut(K/F)$, we have these possibilities

$$\sigma(3^{1/4}) = 3^{1/4}, \sigma(3^{1/4}) = 3^{1/4}i, \sigma(3^{1/4}) = -3^{1/4}i, \sigma(3^{1/4}) = -3^{1/4}$$

and

$$\sigma(i) = \mathrm{i} \text{ or } \sigma(\mathrm{i}) = -i.$$

Then, we form $\sigma, \tau \in Aut(K/F)$ where $\sigma(3^{1/4}) = 3^{1/4}i$ and $\tau(i) = -i$. Note that $\sigma^4 = \tau^2 = id$ and $\tau^{-1} = \sigma^{-1}\tau\sigma$. It can be computed that

$$\begin{aligned} Aut(K/F) &= \langle \sigma, \tau | \sigma^4 = \tau^2 = id, \tau^{-1} = \sigma^{-1}\tau\sigma \rangle \\ &= \{id, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}. \end{aligned}$$

Therefore, $Aut(K/F)$ is the dihedral group D_8 so that $|Aut(K/F)| = 8$. Thus, K/F is a Galois extension with its Galois group $G = Gal(K/F) = D_8$.

Example 11

Suppose an extension field $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$ where

$$\mathbb{Q}(\sqrt[4]{3}) = \{a.1 + b.\sqrt[4]{3} + c.\sqrt[4]{9} + b.\sqrt[4]{27}\}.$$

So, $\{1, \sqrt[4]{3}, \sqrt[4]{9}, \sqrt[4]{27}\}$ is a basis of $\mathbb{Q}(\sqrt[4]{3}) = \{a.1 + b.\sqrt[4]{3} + c.\sqrt{3} + b.\sqrt[4]{27}\}$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. We construct all automorphisms in $\mathbb{Q}(\sqrt[4]{3})$ defined by

$$\rho : B \to \mathbb{Q}(\sqrt[4]{3}).$$

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

$$0 = \sigma(0) = \sigma((\sqrt[4]{3})^4 - 3) = \sigma((\sqrt[3]{2}))^4 - \sigma(2) = \sigma(\sqrt[4]{3})^4 - 3.$$

So,

$$\sigma(\sqrt[4]{3})^4 = 3.$$

We know that the roots of $x^4 - 3 = 0$ are $\sqrt[4]{3}, -\sqrt[4]{3}, \sqrt[4]{3}i,$ and$-\sqrt[4]{3}i$. Note that $\sqrt[4]{3}i, -\sqrt[4]{3}i. \notin \mathbb{Q}(\sqrt[4]{3})$ so that $\sigma(\sqrt[4]{3}) = \sqrt[4]{3}$ or $\sigma(\sqrt[4]{3}) = -\sqrt[4]{3}$.

Since $\sqrt[4]{9} = (\sqrt[4]{3})^2$ and $\sqrt[4]{27} = (\sqrt[4]{3})^3$, we have $\sigma(\sqrt[4]{9})$ and $\sigma(\sqrt[4]{27})$ are depending on $\sigma(\sqrt[4]{3})$. Hence, there are only two automorphisms in $Aut(\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q})$ defined by

$$\begin{aligned} \sigma_1 : B &\to \mathbb{Q}(\sqrt[3]{2}) \\ 1 &\mapsto 1 \\ \sqrt[4]{3} &\mapsto \sqrt[4]{3} \\ \sqrt[4]{9} &\mapsto 9 \\ \sqrt[4]{27} &\mapsto \sqrt[4]{27} \end{aligned}$$

and

$$\begin{aligned} \sigma_2 : B &\to \mathbb{Q}(\sqrt[3]{2}) \\ 1 &\mapsto 1 \\ \sqrt[4]{3} &\mapsto -\sqrt[4]{3} \\ \sqrt[4]{9} &\mapsto 9 \\ \sqrt[4]{27} &\mapsto -\sqrt[4]{27} \end{aligned}$$

In conclusion, we obtain $|Aut(\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q})| = 2$ while $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. Hence, $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$ is not a Galois extension.

Next, we assume that K/F is a Galois extension field with its Galois group $G = Gal(K/F)$. Moreover, we will give some properties of K/F related to its Galois group. We will first discuss the fixed field of an extension field.

Let K/F be a Galois extension with its Galois group $G = Gal(K/F)$. We form a subset of K defined by

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

Note that $\forall a, b \in K^G$ dan $\sigma \in G$, 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^G is a subfield in K and is called **the fixed field of K/F** [5].

Next, we will give an example on finding the fixed field of a Galois extension using **Example 4.**

Example 12
Let $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ be a Galois extension where its Galois group $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma_2{}'\}$. We obtain,

$$\begin{gathered} id: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} \mapsto a + b\sqrt{2} \end{gathered}$$

and

$$\begin{gathered} \sigma_2{}': \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} \mapsto a - b\sqrt{2} \end{gathered}$$

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

Lemma 13[5]
Let K/F be a Galois extension field with its Galois group $G = Gal(K/F)$. If $S \subseteq G$ then K^S is an intermediate subfield of K/F i.e. $F \subseteq K^S \subseteq K$
Proof
Note that for every $a, b \in K^S$ dan $\sigma \in S$, we have

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

and

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

Thus, K^S is a subfield in K containing F.

Moreover, for every $S \subseteq G$, we called K^Sas **the fixed field of** $\boldsymbol{S}$. ■

Let K/F be a Galois extension with its Galois group $G = Gal(K/F)$ where

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

is the fixed field of K/F. It is obvious that $F \subseteq K^G$. Furthermore, we will give the properties of K/F related to its fixed field K^G.

Theorem 14 [2]
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 8**, we have $d \geq n$. Next, we will prove that $d \leq n$, using a method of contradiction.
Suppose $d > n$. Thus, there exist $n + 1$ elements $v_1, v_2, \dots, v_{n+1}$ which are linearly independent over F. Then, we construct the following system of the equations

$$\begin{gathered} \sigma_1(v_1)x_1 + \sigma_1(v_2)x_2 + \cdots + \sigma_1(v_{n+1})x_{n+1} = 0 \\ \sigma_2(v_1)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_2(v_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(v_1)x_1 + \sigma_2(v_2)x_2 + \cdots + \sigma_n(v_{n+1})x_{n+1} = 0. \end{gathered}$$

Note that there are more variables than the number of equations. It implies there is a non-trivial solution, $(x_1\ x_2\ \vdots\ x_{n+1}\ ) = (\alpha_1\ \alpha_2\ \vdots\ \alpha_{n+1}\ )$ where $\alpha_i \neq 0$ for some $i \in \{1,2, \dots, n + 1\}$. Among all non-trivial solutions, we choose r as the least number of non-zero elements. Moreover, $r \neq 1$ because $\sigma_1(v_1)\alpha_1 = 0$ implies $\sigma_1(v_1) = 0$ and $v_1 = 0$.

i. We will prove that there exists a non-trivial solution where α_i are in F for any $i \in \{1,2, \dots, n + 1\}$.
Suppose $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is a non-trivial solution with r non-zero elements where $\alpha_1, \alpha_2, \dots, \alpha_r \neq 0$. We

obtain a new non-trivial solution by multiplying the given solution with $\frac{1}{\alpha_r}$ which is $\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_r\\ 0\\ \vdots\\ 0\end{pmatrix} = \begin{pmatrix}\alpha_1/\alpha_r\\ \alpha_2/\alpha_r\\ \vdots\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}$. Thus,

$$\beta_1\sigma_i(v_1) + \beta_2\sigma_i(v_2) + \cdots + 1.\sigma_i(v_{n+1}) = 0 \qquad (4)$$

For $i = 1,2,\dots,n$. Now, we will show that β_i are in F for any $i \in \{1,2,\dots,n+1\}$ using a method of contradiction. Suppose there exists $\beta_i \notin F$, say β_1. We know that $F = K^G$ so that β_1 is not an element of the fixed field. In other words, there exists $\sigma_k \in G$ where $\sigma_k(\beta_1) \neq \beta_1$. So, $\sigma_k(\beta_1) - \beta_1 \neq 0$. 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 $j = 1,2,\dots,n$. Applying σ_k to the expressions of (4)

$$\Leftrightarrow \sigma_k(\beta_1\sigma_j(v_1) + \beta_2\sigma_j(v_2) + \cdots + 1.\sigma_j(v_r)) = 0$$
$$\Leftrightarrow \sigma_k(\beta_1).\sigma_k\sigma_j(v_1) + \sigma_k(\beta_2).\sigma_k\sigma_j(v_2) + \cdots + \sigma_k\sigma_j(v_r) = 0$$

for $j = 1,2,\dots,n$ so that from $\sigma_i = \sigma_k\sigma_j$. We obtain

$$\sigma_k(\beta_1).\sigma_i(v_1) + \sigma_k(\beta_2).\sigma_i(v_2) + \cdots + \sigma_i(v_r) = 0. \qquad (5)$$

Subtracting (4) and (5), we have

$$(\beta_1 - \sigma_k(\beta_1)\sigma_i(v_1) + (\beta_2 - \sigma_k(\beta_2)\sigma_i(v_2) + \cdots + (\beta_{r-1} - \sigma_k(\beta_{r-1})\sigma_i(v_{r-1}) + 0 = 0$$

which is 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 minimal number. Hence, $\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_r\\ 0\\ \vdots\\ 0\end{pmatrix}$ is a non-trivial where all $\beta_i \in F$ for any $i = 1,2,\dots,n$.

ii. Using (i), we obtain a nonzero solution with all elements in F. So, using the first equation in the system, we obtain

$$\Leftrightarrow \sigma_1(v_1)\beta_1 + \sigma_1(v_2)\beta_2 + \cdots + \sigma_1(v_r)\beta_r = 0$$
$$\Leftrightarrow \sigma_1(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_r) = 0.$$

Because σ_1 is an automorphism, we obtain $\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_r v_r = 0$ where $\beta_1, \beta_2, \dots, \beta_r$ are nonzero elements in K. It is contrary to $v_1, v_2, \dots, v_{n+1}$ which are linearly independent over F.

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

Theorem 15[2]

An extension K/F is a Galois extension field with its Galois group $G = Gal(K/F)$ if and only if $K^G = F$.

Proof

($\Longrightarrow$) Suppose K is a Galois extension over F where $[K:F] = |Aut(K/F)|$. Next, we will show that $K^G = F$. Based on the previous Lemma know that K^G is a subfield of K and $F \subseteq K^G \subseteq K$.

Using **Lemma 5,** we have

$$[K:F] = [K:K^G] = [K:F]/[K^G:F].$$

It implies $[K^G:F] = 1$. Hence, $K^G = F$.

($\Longleftarrow$)Let $K^G = F$. Based on Theorem 14, we have $[K:F] = [K:K^G] = |Aut(K/F)|$. Thus, K/F is Galois. ■

Let $\boldsymbol{K/F}$ be a Galois extension and $\boldsymbol{E}$ is an intermediate field in $\boldsymbol{K/F}$ i.e. $\boldsymbol{F \subseteq E \subseteq K}$. Note that, we can form an extension field $\boldsymbol{K/E}$ and $\boldsymbol{E/F}$. In this section , we will show that $\boldsymbol{K/E}$ is always Galois.

Lemma 16[12]
Let $\boldsymbol{K/F}$ be a Galois extension with its Galois group $\boldsymbol{G = Gal(K/F)}$. If $\boldsymbol{E}$ is an intermediate field in $\boldsymbol{K/F}$ where $\boldsymbol{F \subseteq E \subseteq K}$ then $\boldsymbol{K/E}$ is Galois with Galois group $\boldsymbol{H = Gal(K/E)}$.
Proof.
Let $\boldsymbol{K/F}$ be a Galois extension where $\boldsymbol{G = Gal(K/F)}$. We will show that $\boldsymbol{K/E}$ is Galois i.e. $[\boldsymbol{K}:\boldsymbol{E}] = |\boldsymbol{Aut(K/E)}|$.
Suppose $\boldsymbol{H \subseteq G}$ where $\boldsymbol{E}$ is the fixed field of $\boldsymbol{H}$ i.e. $\boldsymbol{E = K^H}$. First, we will prove that $\boldsymbol{H \subseteq Aut(K/E)}$. Next, we will prove that $\boldsymbol{H = Aut(K/E)}$. Take any $\boldsymbol{h \in H}$. Because $\boldsymbol{E}$ is the fixed field of $\boldsymbol{H}$, we obtain

$$h(x) = x$$

for every $\boldsymbol{x \in E}$. Thus, $\boldsymbol{h}$ fixes all element in $\boldsymbol{E}$ so that $\boldsymbol{h \in Aut(K/E)}$ and $\boldsymbol{H \subseteq Aut(K/E)}$. Thus, $\boldsymbol{H} \leq |\boldsymbol{Aut(K/E)}|$. Based on **Proposition 8** and **Theorem 14**, we obtain

$$|\boldsymbol{H}| \leq |\boldsymbol{Aut(K/E)}| \leq [\boldsymbol{K}:\boldsymbol{E}] = [\boldsymbol{K}:\boldsymbol{K^H}] = |\boldsymbol{H}|.$$

Hence, $|\boldsymbol{Aut(K/E)}| = [\boldsymbol{K}:\boldsymbol{E}]$. Therefore, $\boldsymbol{K/E}$ is Galois. ■

Let $\boldsymbol{K/F}$ be a Galois extension and $\boldsymbol{E}$ is an intermediate field in $\boldsymbol{K/F}$ i.e. $\boldsymbol{F \subseteq E \subseteq K}$. Note that, we can form an extension field $\boldsymbol{K/E}$ and $\boldsymbol{E/F}$. However, the extension field $\boldsymbol{E/F}$ is not always Galois. Using Example 10 and Example 11, for $\boldsymbol{K} = \mathbb{Q}(\boldsymbol{3^{1/4}, i})$, $\boldsymbol{F} = \mathbb{Q}$, and $\boldsymbol{E} = \mathbb{Q}(\boldsymbol{3^{1/4}})$, we know that $\boldsymbol{K/E}$ is Galois but $\boldsymbol{E/F}$ is not a Galois extension.

2.3. Galois Correspondence

Let $\boldsymbol{K/F}$ be a Galois extension with its Galois group $\boldsymbol{G = Gal(K/F)}$. In this part, we will discuss about Galois correspondence between the set of all subgroups in $\boldsymbol{G}$ and the set of all intermediate field $\boldsymbol{E}$ of $\boldsymbol{K/F}$ i.e. $\boldsymbol{F \subseteq E \subseteq K}$. We will also give a condition for $\boldsymbol{E/F}$ to be a Galois extension using Galois correspondence.

Let K/F be a Galois extension field with its Galois group $G = Gal(K/F)$. We know that for every subgroup H in G, we can form a subfield K^H. 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. Next, we will show that there is a one-one correspondence between $\mathcal{H}$ and $\mathcal{F}$ that is ρ is bijective.

Theorem 17[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

$$\rho: \mathcal{H} \to \mathcal{F}$$
$$H \mapsto K^H.$$

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 ρ is bijective.

i. Suppose E is an intermediate field. From **Lemma 16**, 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, ρ 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 16**. Based on **Theorem 14**, we obtain, $H_1 = Aut(K/K^{H_1})$ 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. Therefore, $H_1 \subseteq Aut(K/K^{H_2}) = H_2$. Therefore, $H_1 = H_2$. Hence, ρ is injective. ■

Let K/F be an extension field. If K is a Galois extension then there is an one-one correspondence between intermediate subfield E of K/F and subgroups H of G defined by

$$\begin{aligned} \rho: \mathcal{H} &\to \mathcal{F} \\ H &\mapsto K^H. \end{aligned}$$

It implies H is corresponding to its fixed field K^H i.e. $H = Aut(K/K^H)$. Moreover, we will construct the inverse of $\rho: \mathcal{H} \to \mathcal{F}$ that is $\varphi: \mathcal{F} \to \mathcal{H}$. Note that for every intermediate subfield E, we obtain $E = \rho(H) = K^H$ for some $H \in \mathcal{H}$. Next, we will determine the subgroup H. Based on **Lemma 16** and **Theorem 14,** we have these following conditions

i. K/E is Galois with its Galois group $Aut(K/E)$;
ii. E is the fixed field of $Aut(K/E)$ i.e. $E = K^{Aut(K/E)}$.

Thus, $E = K^{Aut(K/E)}$ and $E = \rho(H) = K^H$. Using the fact that ρ is bijective, we have $H = Aut(K/E)$. Therefore, we also can construct φ defined by

$$\begin{aligned} \varphi: \mathcal{F} &\to \mathcal{H} \\ E &\mapsto Aut(K/E). \end{aligned}$$

Next, we will give some properties related to Galois correspondence.

Theorem 18[2]
Let $\boldsymbol{K/F}$ be a Galois extension with its Galois group $\boldsymbol{G = Gal(K/F)}$ and $\boldsymbol{\sigma \in G}$. If $\boldsymbol{E}$ is correspondent to $\boldsymbol{H}$ then $\boldsymbol{\sigma(E)}$ is correspondent to $\boldsymbol{\sigma H \sigma^{-1}}$.
Proof.
Suppose an intermediate field E of K/F and subgroups H of G. We obtain,

$$\begin{aligned} \varphi: \mathcal{F} &\to \mathcal{H} \\ E &\mapsto Gal(K/E) = H. \end{aligned}$$

Next, we will show that $\boldsymbol{\sigma(E)}$ is mapped to $\boldsymbol{\sigma H \sigma^{-1}}$.

i. First, we will show that $\sigma H \sigma^{-1} \subseteq Gal(K/\sigma(E))$. Let $h \in H$ and $\alpha \in E$, we have
$$\sigma h \sigma^{-1}(\sigma(\alpha)) = \sigma h(\alpha) = \sigma(\alpha).$$
Therefore, $\sigma h \sigma^{-1}$ fixes all elements in $\sigma(E)$. So, $\sigma h \sigma^{-1} \in Gal(K/\sigma(E))$ so that $\sigma H \sigma^{-1} \subseteq Gal(K/\sigma(E))$.

ii. Note that the restriction of σ to E where
$$\sigma_{|E}: E \to \sigma(E)$$
is an isomorphism. Therefore, we have $\boldsymbol{[E/F] = [\sigma(E)/F]}$. We have,
$$\begin{aligned} \boldsymbol{[K:E]} &= \boldsymbol{[K:F]/[E:F]} \\ &= \boldsymbol{[K:F]/[\sigma(E):F]} \\ &= \boldsymbol{[K:\sigma(E)]} \end{aligned}$$
Based on Lemma 16, we have $\boldsymbol{K/E}$ and $\boldsymbol{K/\sigma(E)}$ are Galois so that
$$\boldsymbol{|H| = |Aut(K/E)| = [K:E] = [K:\sigma(E)] = |Aut(K/\sigma(E))|}$$
From group properties, we also get
$$|H| = |\sigma H \sigma^{-1}|.$$
Therefore, we have $|\sigma H \sigma^{-1}| = |Aut(K/\sigma(E))|$.

From (i) and (ii), we have $\sigma H \sigma^{-1} \subseteq Gal(K/\sigma(E))$ and $|\sigma H \sigma^{-1}| = |Aut(K/\sigma(E))|$. Hence, $\sigma H \sigma^{-1} = Gal(K/\sigma(E))$. ■

Theorem 19[12]
Suppose K/F be a Galois group and E is an indeterminate field of K/F with its Galois group $H = Aut(K/E)$. If H is a normal subgroup in G then E/F is a Galois extension with its Galois group $Gal(E/F)$.
Proof.
Suppose H is normal.
Take any $\sigma \in Gal(K/F)$. Since H is normal, we have $\sigma H \sigma^{-1} = H$. Based on **Theorem 18**, we get $\varphi(E) = H$ and $\rho(\sigma(E)) = \sigma H \sigma^{-1} = H$. Because φ is bijective, it implies $E = \sigma(E)$. Note that $\sigma(x) \in E$ for all $x \in E$ so that

$$\sigma_{|E}: E \to E$$

and $\sigma_{|E} \in Aut(E/F)$. Therefore, we can form a group homomorphism

$$\begin{aligned} \psi: Gal(K/F) &\to Aut(E/F) \\ \sigma &\mapsto \sigma_{|E}. \end{aligned}$$

i. First we will show that $Gal(K/E) = Ker(\psi)$. For any $g \in Gal(K/E)$, we have $g(x) = x$ for every $x \in E$. Therefore, $g_{|E} = id$ and $f \in Ker(\psi)$.
Moreover, take $f \in Ker(\psi)$. It means $\psi(f) = f_{|E} = id$. So, $f(x) = x$ for every $x \in E$ and $f \in Gal(K/E)$. Hence, $Aut(K/E) = Ker(\psi)$.

ii. Next, we will prove that E/F is Galois that is $Aut(E/F) = [E\colon F]$
Using the homomorphism theorem, we have
$$Gal(K/F)/Gal(K/E) \cong im(\psi).$$
So,
$$\begin{array}{llll}
\Leftrightarrow & |im(\psi)| & \leq & Aut(E/F) \\
\Leftrightarrow & |Gal(K/F)/Gal(K/E)| & \leq & Aut(E/F) \\
\Leftrightarrow & \frac{|Gal(K/F)|}{|Gal(K/E)|} & \leq & Aut(E/F) \\
\Leftrightarrow & \frac{[K\colon F]}{[K\colon E]} & \leq & Aut(E/F) \\
\Leftrightarrow & \frac{[K\colon F]}{[K\colon E]} & \leq & Aut(E/F) \\
\Leftrightarrow & [E\colon F] & \leq & Aut(E/F).
\end{array}$$
Based on **Proposition 8**, $Aut(E/F) \leq [E\colon F]$. Therefore, $Aut(E/F) = [E\colon F]$. Hence, E/F is Galois extension with its Galois group $Gal(E/F)$. ■

Here, we will give an application on finding Galois extension E/F related to Galois correspondence using **Example 10.**

Example 20
Based on **Example 10**, we obtain a Galois extension Suppose an extension field K/F where $K = \mathbb{Q}(\sqrt[4]{3}, i), F = \mathbb{Q}$ and its Galois $G = Gal(K/F) = D_8$ where
$$\begin{aligned} Gal(K/F) &= \langle \sigma, \tau | \sigma^4 = \tau^2 = id, \tau^{-1} = \sigma^{-1}\tau\sigma \rangle \\ &= \{id, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}. \end{aligned}$$
Using the previous Theorem, we can obtain a Galois E/F by computing the normal subgroups in G. Note that the proper normal subgroups in G are
$$\begin{aligned} H_1 &=< \sigma >= \{id, \sigma, \sigma^2, \sigma^3\} \\ H_2 &=< \tau, \sigma^2 >= \{id, \tau, \sigma^2, \tau\sigma^2\} \\ H_3 &=< \tau\sigma, \sigma^2 >= \{id, \tau\sigma, \sigma^2, \tau\sigma^3\} \\ H_4 &=< \sigma^2 >= \{id, \sigma^2\}. \end{aligned}$$
Using the Galois correspondence, we can compute the Galois extensions by finding indeterminate subfields $E_1, E_2, E_3,$ and E_4 of K/F where its Galois group is $H_1, H_2, H_3,$ and H_4. Thus, based on the correspondence, we have
$$\begin{aligned} \rho\colon \mathcal{H} &\to \mathcal{F} \\ H &\mapsto K^H. \end{aligned}$$
So, $E_i = K^{H_i}$ for all $i = 1,2,3,4$. Note that for $H_1 =< \sigma >$, we get $\sigma(i) = i$ so that $\sigma^2(i) = i$ and $\sigma^3(i) = i$. Thus, every element in H_1 fixes all element in $\mathbb{Q}$ and i. Hence, the fixed field of H_1 i.e. $K^{H_1} = \mathbb{Q}(i)$. Note also for $H_2 =< \tau, \sigma^2 >$, $\tau(\sqrt{3}i) = \sqrt{3}i$ and $\sigma^2(\sqrt{3}i) = \sqrt{3}i$. Therefore, $\tau\sigma^2(\sqrt{3}i) = \sqrt{3}i$ so that every element in H_2 fixes $\mathbb{Q}$ and $\sqrt{3}i$. It implies, $K^{H_2} = \mathbb{Q}(\sqrt{3}i)$. Using the same way, we obtain $K^{H_3} = \mathbb{Q}(\sqrt{3})$ and $K^{H_4} = \mathbb{Q}(\sqrt{3}, i)$.
Therefore, we obtain Galois extension $\mathbb{Q}(i)/\mathbb{Q})$, $\mathbb{Q}(\sqrt{3}i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, and $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$.

3. Conclusion

Let K/F be Galois extension field with its Galois group $G = Gal(K/F)$. Suppose E be an intermediate field of K/E that is $F \subseteq E \subseteq K$.

1. There is an one-one correspondence between the set of all intermediate subfield of K/F and the set of all subgroup in G defined by

$$\begin{aligned} \rho: \mathcal{H} &\to \mathcal{F} \\ H &\mapsto K^H \end{aligned}$$

for all subgroups H in G where K^H is the fixed field of H.

2. K/E is a Galois extension with its Galois group $H = Gal(K/E)$.
3. E/F is a Galois if and only if $H = Gal(K/E)$ is a normal subgroup in G.

References

[1] Lidl, R., & Niederreiter, H. (1986). *Introduction to Finite Fields and Their Applications*. Cambridge: Cambridge University Press.

[2] Morandi, P. (1999). *Fields and Galois Theory*. New York: Springer.

[3] Crespo, T., Rio, A., & Velam, M. (2016). On the Galois Correspondence Theorem in Separable Hopf Galois Theory. Publicacions Matemàtiques, 60(1).

[4] Childs, L., N. (2018). Skew braces and the Galois correspondence for Hopf Galois structures. Journal of Algebra, vol. 511, p. 270-291.

[5] Stewart, I. (2016). Field Automorphisms. Galois Theory, 165–170.

[6] Conrad, K. (2013). Galois Theory At Work : Concrete Examples. Retrieved from the University of Connecticut website: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisappn.pdf

[7] Dummit, D.S. & Foote, R.N. (1999) Abstract Algebra. Canada: John Wiley and Sons.

[8] Vijay, K. K. & Bhamri, S. K. (2000). *A Course in Abstract Algebra*-Vikas Publishing House Pvt Limited.

[9] Malik, D. S., Mordeson, J. N., & Sen, M.K. (2007). Fundamentals of Abstract Algebra. The McGraw-Hill Companies, Inc.

[10] Roman, S. (2005). *Advanced Linear Algebra*. New York: Springer.

[11] Conrad, K. (2015). Galois groups as permutation groups. Retrieved from the University of Connecticut website: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf

[12] Conrad, K. (2010). The Galois Correspondence. Retrieved from the University of Connecticut website: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorr.pdf