TENSOR Pure and Applied Mathematics Journal
September 2022 | Vol. 3 | No. 2 Halaman 85–92
p-ISSN: 2723-0325 e-ISSN: 2723-0333

Extension Fields Which Are Galois Extensions

Novita Dahoklory[1*], Henry W. M. Patty[2]
[1,2] 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, henrywmpatty81@gmail.com

Manuscript submitted : October 2022;
Accepted for publication : November 2022.

Abstract: Let K/F be an extension field where $[K{:}F]$ is the dimension of K as a vector space over F. Let $Aut(K/F)$ be the automorphism group of K/F where its order is denoted by $|Aut(K/F)|$. In this research, we will show that $|Aut(K/F)| \leq [K{:}F]$. Moreover, K/F is called a Galois extension if the equality holds that is $|Aut(K/F)| = [K{:}F]$. We will also discuss about the fixed field of K/F. Furthermore, we will give a necessary and sufficient condition for an extension field K/F to be a Galois extension using the property of its fixed field.

2010 Mathematical Subject Classification : 11R32, 13B05
Keywords: Extension field, automorphism group, Galois extension, fixed field

1. Introduction

Let 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. Moreover, we know that K can be viewed as a vector space over F. Thus, K have a basis where the dimension of K is written by $[K{:}F]$. Furthermore, we form a set of all automorphisms of K and we denote it by $Aut(K/F)$ which 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 $|Aut(K/F)|$.

The relation between the dimension of K/F and the order of $Aut(K/F)$ ($[K{:}F]$ and $|Aut(K/F)|$) was discussed in several researches. In [5], the author shows that $|Aut(K/F)| \leq [K{:}F]$. However, the equality between $Aut(K/F)$ and $[K{:}F]$ does not always hold. For example, the extension field $Q(\sqrt[3]{2})/Q$ has $Aut(Q(\sqrt[3]{2})/Q) = \{id\}$ and the basis of $(\sqrt[3]{2})/Q$ is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ so that $|Aut(K/F)| \neq [K{:}F]$. Then, it motivates the definition of a Galois extension which is an extension field K/F where $|Aut(K/F)| = [K{:}F]$.

Furthermore, let K/F be an extension field with its automorphism group $G = Aut(K/F)$. Then, we form a set in K defined by

$$K^G = \{x \in K | \sigma(x) = x \ for\ every\ \sigma \in G\}.$$

In other words, K^G is the set of all elements in K which are mapped into itself by every $\sigma \in G$. The set K^G is a subfield in K where $F \subseteq K^G$ and is called fixed field of K.

Throughout this research, we will give some properties of an extension field and its automorphisms group. Next, we will also give a necessary and sufficient condition for K/F to be a Galois extension using the properties of its fixed field.

We refer to [1, 2, 5, 6] for some basic theories including groups in particular automorphism group and vector spaces. For extension fields and its properties also Galois extension fields, this research is based on [3,5] .

2. SOME RESULTS

2.1. Extension Field and Its Automorphism Group

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. Furthermore, we will also discuss some properties of the automorphism group of K/F.

Definition 1. [3] 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. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\}$ 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 $[K: F]$. Particularly, if $[K: F] < \infty$ then K is called **a finite extension of *F*** [3]. Next, we will give an example of the dimension of a finite extension field.

Example 3

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, $[\mathbb{Q}(\sqrt{2}): \mathbb{Q}] = 2$.

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/F and E/F. We will give a property of $[K: F]$ and $[E: F]$ in the following Lemma.

Lemma 4. [3] 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 $\{v_1, v_2, \dots, v_m\}$ and $\{w_1, w_2, \dots, w_n\}$ 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 $\alpha_1, \alpha_2, \dots, \alpha_m \in E$. Note that E is a vector space over F, we obtain

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

for $i = 1,2, \dots, m$. Then,

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

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

$$c_{11} v_1 w_1 + c_{12} v_1 w_2 + \cdots + c_{1n} v_2 w_n + \cdots + c_{m1} v_m w_1 + c_{m2} v_m w_2 + \cdots + c_{mn} v_m w_n = 0$$

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 $\{v_1, v_2, \dots, v_m\}$ 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 means $c_{i1} = c_{i2} = \cdots = c_{in} = 0$. Thus, $c_{ij} = 0$ for $i = 1,2, \dots, m$

and $j = 1,2, \dots, n$. We have B is a basis of K over F. Hence, $B = \{v_i w_j | i = 1,2, \dots, m,\ j = 1,2, \dots, n\}$ and $[K: F] = mn$. ■

Furthermore, for every extension field K/F, we form the set of all automorphism of K which is defined by

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

$Aut(K/F)$ is a group under the operation of composition. We will give some examples of $Aut(K/F)$ from an extension field K/F.

Example 5

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

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

The function will then be extended to $\rho': \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$. Because σ is an element in $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, we have $\sigma(1) = 1$ and $\sigma(a) = \sigma(1.a) = a.\sigma(1) = a.1 = a$ 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

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

and

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

Then, those two functions are extended to

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

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

Example 6

Given an extension field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ where

$$\mathbb{Q}(\sqrt[3]{2}) = \{a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{4}\}.$$

So, $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. We will use the same way from **Example 5** to find all automorphisms of $\mathbb{Q}(\sqrt[3]{2})$. We construct all automorphisms in $\mathbb{Q}(\sqrt[3]{2})$ from bijective function which is defined by

$$\rho: B \to \mathbb{Q}(\sqrt[3]{2}).$$

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

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

So,

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

We know that the roots of $x^3 - 2 = 0$ are $\sqrt[3]{2}\ e^{\frac{1}{3}.2\pi i}\sqrt[3]{2}, \sqrt[3]{2}\ e^{\frac{2}{3}.2\pi i}$,and$\sqrt[3]{2}$. Note that $\sqrt[3]{2}\ e^{\frac{1}{3}.2\pi i}\sqrt[3]{2}, \sqrt[3]{2}\ e^{\frac{2}{3}.2\pi i} \notin \mathbb{Q}(\sqrt[3]{2})$, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Using the same way, we will also only have $\sigma(\sqrt[3]{4}) = \sqrt[3]{4}$. Hence, we can only form one automorphism defined by

$$\sigma_1: B \to \mathbb{Q}(\sqrt[3]{2})$$
$$1 \mapsto 1$$
$$\sqrt[3]{2} \mapsto \sqrt[3]{2}$$
$$\sqrt[3]{4} \mapsto \sqrt[3]{4}$$

Then, we extend σ_1 to σ_1' defined by

$$\sigma_1{}': \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$$
$$a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{4} \mapsto a.\sigma_1(1) + b.\sigma_1(\sqrt[3]{2}) + c.\sigma_1(\sqrt[3]{4})$$
$$a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{4} \mapsto a.1 + b.\sqrt[3]{2}\, c + \sqrt[3]{4}.$$

Thus, $\sigma_1{}'$ is the identity function of $\mathbb{Q}(\sqrt[3]{2})$. In conclusion, we obtain $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\sigma_1{}'\} = \{id\}$.

Next, we will give a property of $Aut(K/F)$ in the following lemma.

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

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 (i), we obtain
$$\Leftrightarrow \alpha_1\sigma_1(xy) + \alpha_2\sigma_2(xy) + \cdots + \alpha_{k+1}\sigma_{k+1}(xy) = 0$$
$$\Leftrightarrow \alpha_1\sigma_1(x)\sigma_1(y) + \alpha_2\sigma_2(x)\sigma_2(y) + \cdots + \alpha_{k+1}\sigma_{k+1}(x)\sigma_{k+1}(y) = 0 \quad \text{(ii)}$$
From (i), we obtain
$$\alpha_1\sigma_1(x) = -\alpha_2\sigma_2(x) - \cdots - \alpha_{k+1}\sigma_{k+1}(x) \qquad \text{(iii)}$$

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. ■

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

Proposition 8 [5]
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 $d \in N$. 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, $(x_1\ x_2\ \vdots\ x_n\ ) = (c_1\ c_2\ \vdots\ c_n\ )$ 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,

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

and

$$\sigma_1(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_1 + \sigma_2(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_2 + \cdots + \sigma_n(a_1v_1 + a_2v_2 + \cdots + a_dv_d).c_n = 0.$$

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 dependent. It implies contradiction with **Proposition 7**. Hence, $n \leq d$ that is $|G| \leq [K:F]$. ■

Based on **Proposition 8**, we have $|Aut(K/F)| \leq [K:F]$. However, equality does not always hold for all extension fields. We will give an example to describe it.

Example 9
Given an extension field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. From Example 4, we know that $\mathbb{Q}(\sqrt[3]{2}) = \{a.1 + b.\sqrt[3]{2} + c.\sqrt[3]{4}\}$ So, $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. We also have $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$. Thus, $[\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}] = 3$ and $|Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.

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 10. [5] Let K/F be a finite extension field. K is called **Galois extension over** F if $|Aut(K/F)| = [K:F]$.

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

Example 11

i. Using Example 5, 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 6, we know that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ **is not a Galois extension** because $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$ and the basis of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\{1, \sqrt[3]{2}\}$. So, $|Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| \neq [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 2$.

2.2. Fixed Field of An Extension Field

In this part, we will discuss about fixed field of an extension field K/F. Then, we give a necessary and sufficient condition for an extension field to be a Galois extension using the property of fixed of K/F.

Let K/F be an extension field and $G = Aut(K/F)$. 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 **fixed field of** K/F [5].

Example 12

i. Using Example 5, we have $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. We obtain $G = Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma_2'\}$ where

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

and

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

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

ii. Based on Example 6, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is an extension field with its automorphism group $G = Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$. Note that for every $x \in \mathbb{Q}(\sqrt[3]{2})$, we obtain $id(x) = x$. Therefore, $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2})$.

Theorem 13. [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 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 $v_1, v_2, \ldots, v_{n+1}$ 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 $i \in \{1,2,\ldots,n+1\}$. 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 solutions where α_i are in F for any $i \in \{1,2,\ldots,n+1\}$.

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 $\alpha_1, \alpha_2, \ldots, \alpha_r \neq 0$. 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,

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

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 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 (*)

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

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

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

Subtracting (*) and (**), we have

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

which is non-trivial solution because $\sigma_k(\beta_1) \neq \beta_1$ and is having $r-1$ non-zeo 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 are in F. So, using the first equation in the system, we obtain

$$\Leftrightarrow \sigma_1(v_1)\beta_1 + \sigma_1(v_2)\beta_2 + \cdots + \sigma_1(v_r)\beta_r = 0$$
$$\Leftrightarrow \sigma_1(\beta_1v_1 + \beta_2v_2 + \cdots + \beta_rv_r) = 0.$$

Because $\sigma_1$is an automorphism, we obtain $\beta_1v_1 + \beta_2v_2 + \cdots + \beta_rv_r = 0$ 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. $[K:F] = |Aut(K/F)|$. ■

Corollary 14. [5] Let K/F be an extension field where $[K:F] < \infty$. K is a Galois extension over F if and only if $K^G = F$.

Proof

(⇒) 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 4 and Theorem 13, we obtain

$$|Aut(K/F)| = [K:K^G] = [K:F]/[K^G:F].$$

Because $[K:F] = |Aut(K/F)|$. It implies $[K^G:F] = 1$. Hence, $K^G = F$.

(⇐) We know that $K^G = F$. Using Theorem 13, we have $[K:F] = |Aut(K/F)|$. Thus, K is a Galois extension over F. ■

3. Conclusion

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

References

[1] Dummit. (1999). Abstract Algebra Dummit and Foote.pdf.

[2] Khanna. (2000). Vijay K. Khanna, S.K. Bhamri - *A Course in Abstract Algebra*-Vikas (2013).pdf.

[3] Lidl, R., & Niederreiter, H. (1986). Introduction to finite fields and their applications. Cambridge: Cambridge University Press.

[4] Malik, D. S., & Mordeson, J. N. (2007). MTH 581-582 Introduction to Abstract Algebra. *America*, *February*.

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

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