# 5.2 Fundamental Theorem

Let $K \subseteq F$ be field extension.$G(F/K) = \{\sigma | \sigma : F \longrightarrow F$ is isomorphism such that $\sigma(k) = k$ for all $k\epsilon K\}$ is called the Galois group of $F$ over K.

Ex: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b\epsilon\mathbb{Q}\}$
$\sigma\epsilon G(\mathbb{Q}\sqrt{2}/\mathbb{Q}) \Rightarrow \sigma(\sqrt{2})\sigma(\sqrt{2}) = \sigma(2) = 2 \Rightarrow \sigma(\sqrt{2})$ is a root of $x^2 - 2 = 0$. Hence $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{2}) = \sqrt{2} \Rightarrow \sigma = 1$. Then $G(\mathbb{Q}\sqrt{2}/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.

Note: $|G(K(\alpha)\diagup K)| \leq \deg(\alpha, K)$ where $\deg(\alpha, K)$ is the degree of irreducible polynomial $f(x)\epsilon K[x]$ with $f(\alpha) = 0$.

Ex: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$
$\sigma\epsilon G((\mathbb{Q}(\sqrt[3]{2})\diagup\mathbb{Q}) \Rightarrow \sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$,where $\omega = e^{\frac{2\pi}{3}i}$ . But $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$. Hence $G((\mathbb{Q}(\sqrt[3]{2})\diagup\mathbb{Q}) = \{1\}$.

Def: Let $K \subseteq F \subseteq E$ be field extension , and $H \leq G(E/F)$.
Define $F' = \{\sigma\epsilon G(E/K) | \sigma(k) = k$ for any $k\epsilon F\}$ and $H' = \{a\epsilon E | \sigma(a) =$ for all $\sigma\epsilon H\}$.
$E$ is a Galois extension over $K$ if $G(E/K)' = K$ (denoted by $K \lhd E$).

Ex: $G((\mathbb{Q}(\sqrt[3]{2})\diagup\mathbb{Q}) = \{1\} \Rightarrow G((\mathbb{Q}(\sqrt[3]{2})\diagup\mathbb{Q})' = \mathbb{Q}(\sqrt[3]{2})$ (not a Galois extension).

Ex: $\mathbb{Q}(\sqrt{2})$ is a Galois extension over $\mathbb{Q}$. Since $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})' = \mathbb{Q}$.

*GaloisTheory*

Suppose $K \lhd E$, Then we have the following diagram:

$$\begin{array}{rcl}
E & \longleftrightarrow & < e > \\
F & \longleftrightarrow & F' \\
H' & \longleftrightarrow & H \\
\triangledown & \longleftrightarrow & \vartriangle \\
G(E/K)' = K & \longrightarrow & G(E/K)
\end{array}$$

for any field $F$ with $K \subseteq F \subseteq E$ and any $H \leq G(E/K)$.
In particular , there exists a $H$ corresponding between subfields between $K$ and $E$ , and the subgroups of $G(E/K)$.