Galois Theory

Definition: Let F/K be an extension of fields. Define $Gal(F/K) = Aut_K(F) = \{\sigma \in Aut(F) : \sigma(a) = a \quad \forall a \in K\}$. which is called the Galois group of F/K.

Example: $Gal(\mathbb{C}/\mathbb{R})$ has two elements, namely id and $z \mapsto \bar{z}$.

Note: $Aut_K(F)$ is a group under composition.

Note: If $F = K(\alpha)$ and $\beta \in F$, then we can write

$$\beta = \frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_n\alpha^n}$$ for some $a_i, b_j \in K$ and some $n \geq 0$.

If $\sigma \in Gal(F/K)$, then

$$\sigma(\beta) = \frac{a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n}{b_0 + b_1\sigma(\alpha) + \cdots + b_n\sigma(\alpha)^n}$$

so σ is determined by $\sigma(\alpha)$.

Also, if $X \subseteq F$ and $F = K(X)$, then $\sigma \in Gal(F/K)$ is just determined by $\sigma|_X$.

Theorem: If F/K is a field extension, $u \in F$, if $f(u) = 0$ for some $f(x) \in K[x]$ and if $\sigma \in Gal(F/K)$, then $f(\sigma(u)) = 0$.

Proof: $f(\sigma(u)) = \sigma(f(u)) = \sigma(0) = 0$.

For example, if $F = K(\alpha)$ is an algebraic extension, then $\sigma \in Gal(F/K)$ are determined by where they send α and they have to send α to a root of the minimal polynomial. In particular, $|Gal(F/K)| \leq [K(\alpha):K]$

Example: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, so $|Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| \leq 2$.

One map is the identity and the other is the map $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$. In particular,

$$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}_2.$$

Example: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$. If $\sigma \in Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ $\sigma(\sqrt[3]{2})$ has to be a root of x^3-2. But, $\sqrt[3]{2}$ is the only root of x^3-2 in $\mathbb{Q}(\sqrt[3]{2})$, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ i.e. $\sigma = id$, so $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$.

Theorem: Let F/K be an extension, let $H \leq Gal(F/K)$ and let $K \subseteq E \subseteq F$ be an intermediate field. Then

$$H' = \{\alpha \in F ; \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$

is an intermediate field $K \subseteq H' \subseteq F$, and

$$E^* = \{\sigma \in Gal(F/K) : \sigma(\alpha) = \alpha \ \forall \alpha \in E\}$$

is a subgroup of $Gal(F/K)$.

Proof: see notes.

Definition: An extension F/K is Galois if and only if

$$Gal(F/K)' = K.$$

Example: $\mathbb{C}/\mathbb{R}$, it is the case $Gal(\mathbb{C}/\mathbb{R})' = \mathbb{R}$.

Indeed, we have $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$.

In contrast, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. Indeed, we saw $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$. So

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})' = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.

The Fundamental Theorem of Galois Theory.

Let F/K be a finite-degree Galois extension. Then

(i) $E \to E' = \mathrm{Gal}(F/E)$

(ii) $H \to H'$

provides an inclusion-reversing bijection between subgroups of $\mathrm{Gal}(F/K)$ and intermediate fields of F/K. Furthermore, the relative degrees and indices of subgroups are related: $[E_1 : E_2] = [E_2' : E_1']$ for E_1, E_2 intermediate fields or subgroups of $\mathrm{Gal}(F/K)$.

Also, the normal subgroups of $\mathrm{Gal}(F/K)$ correspond to the intermediate fields that are also Galois extension of K.

Example: Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. If $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, then $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$ and σ is determined by the signs. In fact, all 4 possibilities happen. This is a Galois extension and $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Indeed, we can define $(n,m) \mapsto \sigma_{n,m}$ where $\sigma_{n,m}(\sqrt{2}) = (-1)^n\sqrt{2}$, $\sigma_{n,m}(\sqrt{3}) = (-1)^m\sqrt{3}$

$$
\begin{tikzcd}
 & \{id\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[rrr, leftrightarrow, bend left, "\text{FGFT}"] & & & F \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma_{1,0} \rangle \arrow[dr, dash] & \langle \sigma_{0,1} \rangle \arrow[d, dash] & \langle \sigma_{1,1} \rangle \arrow[dl, dash] \arrow[r] & \mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathrm{Gal}(F/\mathbb{Q}) & & & \mathbb{Q} &
\end{tikzcd}
$$