Recall. ① K/F splitting field.

② $|G(K/F)| = [K:F]$.

③ $F = K^H$ for some $H \subset \mathrm{Aut}(K)$.

$$\boxed{\text{For any field } K,\ \mathrm{char}\, K = 0.\quad \mathbb{Q} \subset K, \text{ and } \mathbb{Q} \subset K^H}$$

①, ②, or ③ can be used to define Galois extension.

K/F Galois.

Galois correspondance: $G = G(K/F)$

$H \subset G$ subgroup.

$F \subset L \subset K$ intermediate extension.

$$\{\text{subgroups in } G\} \longleftrightarrow \{\text{intermediate extensions}\}$$

$$H \longmapsto K^H.$$

$$G(K/L) \longleftarrow\!\!\shortmid\ L$$

Splitting field K of $f(x)$ over F; $G(K/F)$

Example 1:

$F=\mathbb{Q}$. $x^4-1 = (x^2+1)(x^2-1)$

$$=(x+i)(x-i)(x+1)(x-1)$$

$$\mathbb{Q}(-i, i, 1, -1) = \mathbb{Q}(i)$$

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

$G(\mathbb{Q}(i)/\mathbb{Q})$. $\sigma \in G(\mathbb{Q}(i)/\mathbb{Q})$

$$\sigma(a+bi) = \sigma(a) + \sigma(b)\cdot\sigma(i) \qquad a, b \in \mathbb{Q}.$$
$$= a + b\sigma(i)$$

$i^2 = 1. \Rightarrow \sigma(i)^2 = 1 \Rightarrow \sigma(i) = \pm i.$

σ is determined by $\sigma(i)$

In other words, $G(\mathbb{Q}(i)/\mathbb{Q}) \to \{i, -i\}$ is
$\sigma \mapsto \sigma(i)$

injective.

On the other hand, we know

$$\left| G(\mathbb{Q}(i)/\mathbb{Q}) \right| = [\mathbb{Q}(i):\mathbb{Q}] = 2$$

The above map is also surjective

So $G(\mathbb{Q}(i)/\mathbb{Q}) = \{ id, \sigma_0 \}$

$\sigma_0 : a+bi \mapsto a-bi$.

So $G(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

The Galois corrsspondance can be shown in the following diagram:

$$\begin{array}{ccc} \{id\} & & \mathbb{Q}(i) \\ \big|\, 2 & & \big|\, 2 \\ G = \mathbb{Z}/2\mathbb{Z} & & \mathbb{Q} \end{array}$$

Example 2:

$$G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = G.$$

$|G| = 4$. $\quad G \cong C_2 \times C_2$ or C_4.

which one?

$\sigma: \sqrt{2} \mapsto \pm\sqrt{2}$

$\quad\sqrt{3} \mapsto \pm\sqrt{3}$.

$$G \to \left\{ \begin{array}{c} (\sqrt{2}, \sqrt{3}) \\ (-\sqrt{2}, \sqrt{3}) \\ (\sqrt{2}, -\sqrt{3}) \\ (-\sqrt{2}, -\sqrt{3}) \end{array} \right\}$$

$$\sigma \longmapsto (\sigma(\sqrt{2}), \sigma(\sqrt{3}))$$

is injective.

since $|G| = 4$. the map is also surjective.

(The map also has the following interpretation.)

Look at the action of

G on the roots $(x^2-2)(x^2-3)$.

then we get a group homomorphism

$$G \longrightarrow S_2 \times S_2$$

permutation of $\{\sqrt{2}, -\sqrt{2}\}$

permutation of $\{\sqrt{3}, -\sqrt{3}\}$.

This is injective because $\sqrt{2}$, $\sqrt{3}$ are the generators for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$

since $|G| = 4$, this is an isomorphism.

$$G \cong C_2 \times C_2.$$

$$G = \{1, \sigma, \tau, \sigma\tau\}.$$

σ : $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$.

τ : $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$.

$$\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$$
$$\sqrt{3} \mapsto -\sqrt{3}$$

If we look at the fixed field.

$$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle} \supset \mathbb{Q}(\sqrt{2}).$$

$$\left(\text{because } \sigma(\sqrt{2}) = \sqrt{2} \right)$$

Claim $\quad \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle}$

Reason:

$$\begin{tikzcd}
\{id\} \arrow[r] \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash] \\
\langle \sigma \rangle \arrow[r] \arrow[d, dash, "2"] & L = \mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma \rangle} \arrow[d, dash] \\
G \arrow[rd] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
 & \mathbb{Q}.
\end{tikzcd}$$

nothing in between. on the subgroup side.

$\mathbb{Q}(\sqrt{2}) = L.$

In summary:

$$\begin{tikzcd}
& \{id\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle \sigma \rangle \arrow[dr, dash, "2"'] & \langle \tau \rangle \arrow[d, dash, "2"] & \langle \sigma\tau \rangle \arrow[dl, dash, "2"] \\
& G &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash, "2"] \\
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) &
\end{tikzcd}$$

(This diagram is the same for splitting field of $x^4+1 = (x^2-i)(x^2+i)$

$$= \left(x - \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x - \frac{-\sqrt{2}-\sqrt{2}i}{2}\right)$$
$$\left(x - \frac{\sqrt{2}-\sqrt{2}i}{2}\right)\left(x - \frac{-\sqrt{2}+\sqrt{2}i}{2}\right)$$

$\mathbb{Q}(\sqrt{2}, i)$ is the splitting field

and the same argument shows that

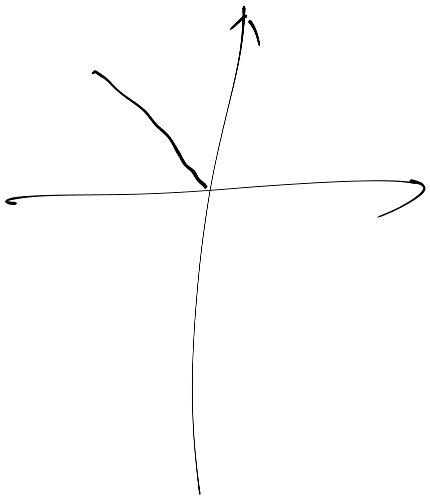
$G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$.

Example 3. Splitting field K of x^3-2

$$(x^3-2) = (x-\sqrt[3]{2})(x-\sqrt[3]{2}w)(x-\sqrt[3]{2}w^2)$$

$$w = e^{\frac{2\pi i}{3}}$$

$$= \frac{-1+\sqrt{-3}}{2}$$



$$w^2+w+1=0.$$

So $K = \mathbb{Q}(\sqrt[3]{2}, w)$.

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, dash, "\geq 2"'] \arrow[dr, dash, "\leq 3"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(w) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$3 \mid [K, \mathbb{Q}]$

$2 \mid [K, \mathbb{Q}]$

and $[K : \mathbb{Q}(\bar{w})] \leq 2$.

So $[K : \mathbb{Q}] = 6$.

Let $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\,w$, $\alpha_3 = \sqrt[3]{2}\,w^2$.

$K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

Consider the action of $G(K/\mathbb{Q})$ on the three roots $\{\alpha_1, \alpha_2, \alpha_3\}$, we obtain homomorphism

$G \longrightarrow S_3$.

① It's injective because $\alpha_1, \alpha_2, \alpha_3$ are generators.

② It's surjective because $|G| = 6$. $|S_3| = 6$.

So $G \cong S_3$.

Let $\sigma = (1\,2\,3)$ $\tau = (1\,2)$

$\sigma: \alpha_1 \mapsto \alpha_2$

$\alpha_2 \mapsto \alpha_3$

$\alpha_3 \mapsto \alpha_1$.

so $\sigma(\alpha_1) = \alpha_2$

$\sigma(w) = \sigma\left(\frac{\alpha_2}{\alpha_1}\right)$

$= \frac{\sigma(\alpha_2)}{\sigma(\alpha_1)} = \frac{\alpha_3}{\alpha_1} = w$.

$\sigma: \alpha_1 \longmapsto \alpha_1 \cdot w.$

$w \longmapsto w.$

so $\mathbb{Q}(w) \subset K^{\langle\sigma\rangle}.$

$$\begin{tikzcd}
\{id\} \arrow[r] \arrow[d, dash, "3"] & K \arrow[d, dash, "3"] \\
\langle\sigma\rangle \arrow[r] \arrow[d, dash, "2"'] & K^{\langle\sigma\rangle} \arrow[d, dash] \\
& \mathbb{Q}(w) \arrow[d, dash] \\
S_3 \arrow[r] & \mathbb{Q}
\end{tikzcd}$$

2.

No subgroup between $\langle\sigma\rangle$ and S_3. So $\mathbb{Q}(w) = K^{\langle\sigma\rangle}$

similarly $K^{\langle\tau\rangle} = \mathbb{Q}(\alpha_3)$

So

$$\begin{tikzcd}[column sep=small]
 & & \{id\} \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\langle \tau \rangle \arrow[drr, dash, "3"'] & \langle \sigma\tau \rangle \arrow[dr, dash, "3"] & \langle \sigma^2\tau \rangle \arrow[d, dash, "3"] & \langle \sigma \rangle \arrow[dl, dash, "2"] \\
 & & S_3 &
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(\sqrt[3]{2}, \omega) \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\sqrt[3]{2}\omega) \arrow[drr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{2}\omega^2) \arrow[dr, dash, "3"] & \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "3"] & \mathbb{Q}(\omega) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

This Galois extension because the subgroup $\langle \sigma \rangle$ is normal. and $G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong S_3/\langle \sigma \rangle$

Some application to find irreducible polynomial of $\beta \in K$. K/F is Galois extension.

Just need to find the orbit of

$G(K/F)$ on β.

For example $\sqrt{2}+\sqrt{3}$ in $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

the orbit is $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$.

$-\sqrt{2}+\sqrt{3}$.

So irreducible polynomial is

$$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))$$