# Galois Theory

Lectured by Alessio Corti
Scribed by Yu Coughlin

Autumn 2025

## Contents



## 1 Galois correspondence

Fix a field $\mathbb{Q} \subset K \subset \mathbb{C}$. For some $\alpha \in \mathbb{C}$ we will use the notation:

$$K(\alpha) := \left\{ \frac{P(\alpha)}{Q(\alpha)} \in \mathbb{C} \;\middle|\; P, Q \in K[X],\ Q(\alpha) \neq 0 \right\}.$$

$K(\alpha_1, \dots, \alpha_n)$ is defined recursively.

**Definition 1.0.1.** Such an $\alpha \in \mathbb{C}$ is **algebraic over** $K$ is there is some nonzero polynomial $P \in K[x]$ such that $P(\alpha) = 0$.

Consider $\mathbb{Q}(\sqrt{2})$, this has a simpler description than as the full quotient:

$$\mathbb{Q}(\sqrt{2}) + \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

If we choose something transcendental (non-algebraic) like $\mathbb{Q}(\pi)$, then we must use the full quotient definition, and in this case we have $\mathbb{Q}(\pi) \cong Q(X)$ the field of fractions of $\mathbb{Q}[X]$.

**Definition 1.0.2.** For some $f \in K[x]$ with distinct complex roots $a_1, \dots, a_n \in \mathbb{C}$, the **splitting field** of $f$ is $L = K(\alpha_1, \dots, \alpha_n)$.

Let $K = \mathbb{Q}$ and $f = x^3 - 2$. The roots of $f$ in $\mathbb{C}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where $\omega$ is $(1 - i\sqrt{3})/2$. So the splitting field is $L = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ which can be simplified to just $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. What are the intermediate fields between $\mathbb{Q}$ and $L$?

$$\begin{tikzcd}
 & & L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) & & \\
\mathbb{Q}(\sqrt[2]{3}) \arrow[urr] & \mathbb{Q}(\omega\sqrt[2]{3}) \arrow[ur] & & \mathbb{Q}(\omega^2\sqrt[2]{3}) \arrow[ul] & \\
 & & & & \mathbb{Q}(i\sqrt{3}) \arrow[uull] \\
 & & \mathbb{Q} \arrow[uull] \arrow[uul] \arrow[uur] \arrow[urr] & &
\end{tikzcd}$$

Lots of fields you might guess, like $\mathbb{Q}(i\sqrt{3}\sqrt[2]{3})$ and $\mathbb{Q}(\sqrt[2]{3} + i\sqrt{3})$ happen to already be in this diagram. But we cannot yet prove this is everything. The length of the arrows is a clue, they relate to the dimension as $\mathbb{Q}$-vector spaces and subgroups in the Galois correspondence.

**Theorem 1.0.3** (Fundamental theorem of Galois theory)**.** The **Galois group** of a field extension $K \subset L$ is

$$G = \mathrm{Gal}(L/K) = \left\{ \varphi : L \xrightarrow{\sim} L \;\middle|\; \varphi|_K = \mathrm{id}_K \right\}$$

and the eponymous Galois correspondence:

$$\begin{aligned} \{K \subset F \subset L\} &\xleftrightarrow{\sim} \{H \leq G\} \\ F &\longmapsto F^\dagger := \{g \in G \mid g|_F = \mathrm{id}_F\} = G_F \\ H^* := \{\alpha \in L \mid H\alpha = \alpha\} &\longleftarrow H \end{aligned} .$$

If one knows the Galois group is a supgroup of the permutation of all the roots, then for the case $L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, there is seemingly no way to distinguish the roots, so we expect $G = S_3$, which is luckily true.
Fields are complicated and hard, there are two operations that "cavort" via a weird distributivity law, and proving the classification of subfields of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ already feels pretty impossible. Galois theory allows us to move information from the easy theory of finite groups into the world of field extensions.