The Galois correspondence

Theorem 1 (Fundamental Theorem of Galois Theory)**.** Let L/F be a Galois extension. There is a bijection

$$\begin{aligned}
\{\text{intermediate fields } E, \text{ with } F \subseteq E \subseteq L\} &\xleftrightarrow{\Psi} \{\text{subgroups } H \text{ of } \mathrm{Gal}(L/F)\} \\
E &\longmapsto \Psi(E) = \mathrm{Gal}(L/E) \\
\Psi^{-1}(H) = L^H &\longleftarrow H.
\end{aligned}$$

The inverse of Ψ sends any $H \leq \mathrm{Gal}(L/F)$ to $\Psi^{-1}(H) = L^H$. Moreover, this bijective correspondence enjoys the following properties:

(a) Ψ and Ψ^{-1} each reverse the order of inclusion.

(b) Ψ and Ψ^{-1} convert between degrees of extensions and indices of subgroups:

$$[\mathrm{Gal}(L/F) : H] = [L^H : F] \qquad \Longleftrightarrow \qquad [\mathrm{Gal}(L/F) : \mathrm{Gal}(L/E)] = [E : F].$$

(c) Normal subgroups correspond to intermediate fields that are Galois over F:

- If $N \trianglelefteq G$ then L^N/F is Galois.
- If E/F is Galois, then $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/F)$.

(d) If $E = L^N$ for a normal subgroup $N \trianglelefteq \mathrm{Gal}(L/F)$, then $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(L/F)/N$.

(e) If H_1, H_2 are subgroups of G with fixed subfields $E_1 = L^{H_1}$ and $E_2 = L^{H_2}$, then

- $E_1 \cap E_2 = L^{<H_1,H_2>}$ and $\mathrm{Gal}(L/E_1 \cap E_2) = \langle H_1, H_2\rangle$.
- $E_1E_2 = L^{H_1 \cap H_2}$ and $\mathrm{Gal}(L/E_1E_2) = H_1 \cap H_2$.

Here is the Fundamental Theorem of Galois Theory in action:

$$L := \text{splitting field of } x^4 - 2 \text{ over } \mathbb{Q}.$$

$$\text{Roots of } f\text{: } \alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = i\alpha_1, \quad \alpha_3 = -\alpha_1, \quad \alpha_4 = -i\alpha_1. \implies \mathrm{Gal}(L/\mathbb{Q}) \leq S_4$$

$$f \text{ is separable} \implies \mathbb{Q} \subseteq L \text{ is Galois}$$

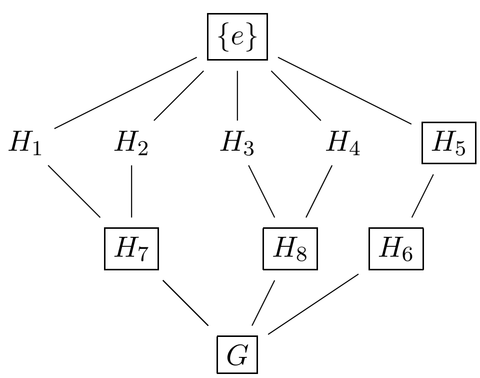
$$G = \mathrm{Gal}(L/\mathbb{Q}) = \langle (2\,4), (1\,2\,3\,4) \rangle.$$

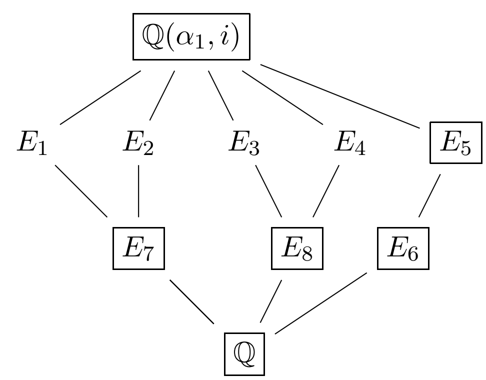
$$G \cong D_8 \text{ via } (2\,4) \mapsto \sigma \text{ reflection, } (1\,2\,3\,4) \mapsto \tau \text{ clockwise rotation by } 90\circ$$

Subgroups of G:

$\{e\}$	$G = \langle (2\,4), (1\,2\,3\,4) \rangle$
$H_1 = \langle (2\,4) \rangle$	$H_5 = \langle (1\,3)(2\,4) \rangle$
$H_2 = \langle (1\,3) \rangle$	$H_6 = \langle (1\,2\,3\,4) \rangle$
$H_3 = \langle (1\,2)(3\,4) \rangle$	$H_7 = \langle (1\,3), (2\,4) \rangle$
$H_4 = \langle (1\,4)(2\,3) \rangle$	$H_8 = \langle (1\,2)(3\,4), (1\,4)(2\,3) \rangle$

Lattices of subgroups of G and intermediate fields of $\mathbb{Q} \subseteq L$:





normal subrgroups