H/W 5 posted (due Tues 2/21)

Today: Finish Section 14.2

Thm 14: Fundamental Theorem of Galois Theory:
K/F: Galois ext'n, $G := \mathrm{Gal}(K/F)$. $\exists$ bijection

$$\left\{ \begin{array}{ll} \text{intermediate fields} & K \\ F \subseteq E \subseteq K & | \\ & E \\ & | \\ & F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{ll} \text{subgroups} & 1 \\ H \leq G & | \\ & H \\ & | \\ & G \end{array} \right\}$$

given by

$$E \longmapsto \mathrm{Aut}(K/E)$$

$$\mathrm{Fix}\, H \longleftarrow H$$

"Galois correspondence".

It has the following properties ($E \leftrightarrow H$, $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$)

(1) (Inclusion reversal): $E_1 \subseteq E_2 \Leftrightarrow H_1 \geq H_2$

(2) $[K:E] = |H|$, $[E:F] = |G:H|$

$$\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \begin{array}{l} \big\} \; |H| \\ \\ \big\} \; |G:H| \end{array}$$

(3) K/E is Galois, $\mathrm{Gal}(K/E) = H$

(4) E/F is Galois $\Leftrightarrow H \trianglelefteq G$.

In this case, $\mathrm{Gal}(E/F) \cong G/H$

(5) $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$

$E_1 E_2 \leftrightarrow H_1 \cap H_2$

Pf: All done except (4)

(4) Let $\mathrm{Emb}(E/F) = \{ \tau : E \underset{\text{inj.}}{\hookrightarrow} K \mid \tau(f) = f, f \in F \}$

We'll show that $|\mathrm{Emb}(E/F)| = [E:F] \overset{(2)}{=} [G:H]$

If $\sigma \in \mathrm{Gal}(K/F)$, $\sigma|_E \in \mathrm{Emb}(E/F)$

If $\tau \in \mathrm{Emb}(E/F)$, K is a splitting field for $\tau(E)$, so Thm 13.27:

$$\begin{tikzcd} \sigma : K \arrow[r, "\sim"] & K \in G \\ \tau : E \arrow[u, dash] \arrow[r, "\sim"] & \sigma(E) \arrow[u, dash] \end{tikzcd}$$

If $\sigma, \sigma' \in G$, then $\sigma|_E = \sigma'|_E \iff$

$\sigma^{-1}\sigma' \in H (= \mathrm{Fix}\, E) \iff \sigma H = \sigma' H$

So $|\mathrm{Emb}(E/F)| = [G:H] = [E:F]$.

Now, E/F Galois $\iff |\mathrm{Aut}(E/F)| = [E:F] = |\mathrm{Emb}(E/F)|$

$\iff E = \sigma(E)$ for all $\sigma \in G$.

$\iff H = \sigma H \sigma^{-1}$ for all $\sigma \in G$ (since $\sigma(E) \leftrightarrow \sigma H \sigma^{-1}$)

$\iff H \trianglelefteq G$

When this happens, $G/H \cong \mathrm{Gal}(E/F)$ since G/H inherits its gp. structure from G $\square$

Examples:

1) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

Let $\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$ $\quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$

Then $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}) = \langle \sigma, \tau \rangle \cong K_4$

Klein 4

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\{1, \tau\} \arrow[dr, dash, "2"'] & \{1, \sigma\tau\} \arrow[d, dash, "2"] & \{1, \sigma\} \arrow[dl, dash, "2"] \\
 & K_4 &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\mathrm{Fix}\{1, \tau\} = \mathbb{Q}(\sqrt{2})$

$\mathrm{Fix}\{1, \sigma\} = \mathbb{Q}(\sqrt{3})$

$\mathrm{Fix}\{1, \sigma\tau\} = \mathbb{Q}(\sqrt{6})$

2) $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$, $\zeta = \zeta_3$

$$\sigma : \begin{cases} \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \\ \zeta \longmapsto \zeta \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \zeta \longmapsto \zeta^2 = -1-\zeta \end{cases}$$

$G = \langle \sigma, \tau \rangle \cong S_3$

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "2"] & & \\
\langle\sigma\rangle \arrow[dr, dash, "2"'] & \langle\tau\rangle \arrow[d, dash, "3"] & \langle\tau\sigma\rangle \arrow[dl, dash, "3"] & \langle\tau\sigma^2\rangle \arrow[dll, dash, "3"] \\
 & S_3 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, \zeta) \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "2"] & & \\
\mathbb{Q}(\zeta) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "3"] & \mathbb{Q}(\zeta, \sqrt[3]{2}) \arrow[dl, dash, "3"] & \mathbb{Q}(\zeta^2\sqrt[3]{2}) \arrow[dll, dash, "3"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

$$\mathrm{Fix}\langle\tau\sigma\rangle = \mathrm{Fix}\begin{cases} \sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2} \\ \zeta \longmapsto \zeta^2 \end{cases} = \mathbb{Q}(\zeta\sqrt[3]{2})$$

Since $\zeta\sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2} \cdot \zeta^2 = \zeta\sqrt[3]{2}$

Which ext'ns are Galois?

$\mathbb{Q}(\sqrt[3]{2}, \zeta)/E$ for any E above

$\mathbb{Q}(\zeta)/\mathbb{Q}$ since $\langle\sigma\rangle$ is a normal subgp. (index 2)

None of the others, since not normal subgps.

e.g. $\sigma\tau\sigma^{-1} = \tau\sigma \notin \langle\tau\rangle$

3) K = splitting field of $x^8 - 2$

$K = \mathbb{Q}(\sqrt[8]{2}, \zeta_8) = \mathbb{Q}(\sqrt[8]{2}, i)$ Let $\theta = \sqrt[8]{2}$

$[K:\mathbb{Q}] = 16$

16 automs.: $\begin{cases} \theta \mapsto \zeta^a \theta, & a = 0, 1, \ldots, 7 \\ i \mapsto \pm i \end{cases}$

$\zeta = \frac{1}{2}(1+i)\sqrt{2} = \frac{1}{2}(1+i)\theta^4$

Let $\sigma: \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto i \end{cases}$ $\tau: \begin{cases} \theta \mapsto \theta \\ i \mapsto -i \end{cases}$

$$\sigma(\rho) = \tfrac{1}{2}(1+i)\rho^4\theta^4 = -\tfrac{1}{2}(1+i)\theta^4 = -\rho = \rho^5$$

$$\tau(\rho) = \tfrac{1}{2}(1-i)\theta^4 = \overline{\rho} = \rho^7$$

$$1: \begin{cases} \theta \mapsto \theta \\ i \mapsto i \\ \rho \mapsto \rho \end{cases} \qquad \tau: \begin{cases} \theta \mapsto \theta \\ i \mapsto -i \\ \rho \mapsto \rho^7 \end{cases}$$

$$\sigma: \begin{cases} \theta \mapsto \rho\theta \\ i \mapsto i \\ \rho \mapsto \rho^5 \end{cases} \qquad \tau\sigma: \begin{cases} \theta \mapsto \rho^2\theta \\ i \mapsto -i \\ \rho \mapsto \rho^7 \end{cases}$$

$$\sigma^2: \begin{cases} \theta \mapsto \rho^6\theta \\ i \mapsto i \\ \rho \mapsto \rho \end{cases} \qquad \tau\sigma^2: \begin{cases} \theta \mapsto \rho\theta \\ i \mapsto -i \\ \rho \mapsto \rho^3 \end{cases}$$

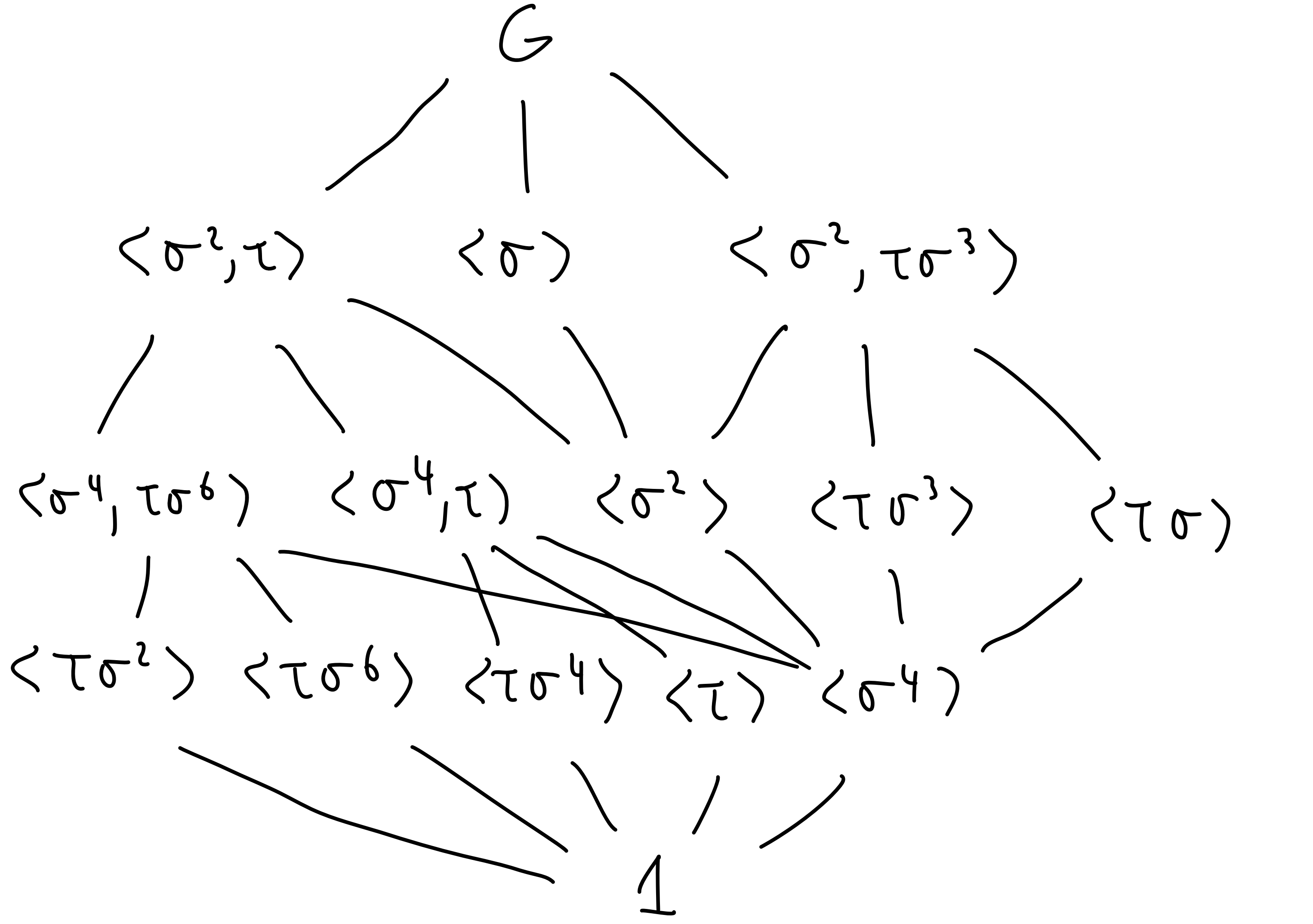
$$\sigma^3: \begin{cases} \theta \mapsto \rho^7\theta \\ i \mapsto i \\ \rho \mapsto \rho^5 \end{cases} \qquad \tau\sigma^3: \begin{cases} \theta \mapsto \rho\theta \\ i \mapsto -i \\ \rho \mapsto \rho^3 \end{cases}$$

$$\sigma\tau : \begin{cases} \theta \mapsto \rho\theta \\ i \mapsto -i \\ \rho \mapsto \rho^3 \end{cases}$$

(Note: can't have $\rho \mapsto \rho^2$)

$$G \cong \mathrm{Gal}(K/\mathbb{Q}) \cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle$$

"Quasidihedral gp."



Want to determine fixed fields of these subgroups.

$\mathrm{Fix}\langle\sigma\rangle = \mathbb{Q}(i)$ ✓

index 2 degree 2

$\mathrm{Fix}\langle\sigma^2, \tau\sigma^3\rangle = \mathbb{Q}(\zeta+\zeta^3)$

$$\sigma^2: \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases}$$

$$\tau\sigma^3: \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$\mathrm{Fix}\langle\tau\sigma^6\rangle = \mathbb{Q}(\zeta^3\theta)$

index 8 degree 8

$$\tau\sigma^6: \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$H :=$

$\mathrm{Fix}\langle\tau\sigma\rangle$ harder

index 4

$H \cong \mathbb{Z}/4\mathbb{Z}$

$\langle\sigma^4\rangle \leq H$ index 2, so normal in H

$\theta^2 \in \mathrm{Fix}\langle\sigma^4\rangle$

Let $\alpha = (1+\tau\sigma^3)\,\theta^2 = \theta^2 + \tau\sigma^3\theta^2$ summing over cosets of $H/\langle\sigma^4\rangle$

$\alpha \in \text{Fix}\,\sigma^4$ since
$$\begin{aligned}\sigma^4\alpha &= \sigma^4(1+\tau\sigma^3)\theta^2\\ &= (1+\tau\sigma^3)\,\sigma^4\theta^2\\ &= (1+\tau\sigma^3)\,\theta^2\\ &= \alpha\end{aligned}$$

$\alpha \in \text{Fix}\,\tau\sigma^3$ since
$$\begin{aligned}\tau\sigma^3\alpha &= \tau\sigma^3(1+\tau\sigma^3)\theta^2\\ &= (\tau\sigma^3 + \sigma^4)\,\theta^2\\ &= (1+\tau\sigma^3)\,\theta^2\\ &= \alpha\end{aligned}$$

$\alpha = (1+i)\sqrt[4]{2} \notin \text{Fix}\,\langle\sigma^2\rangle$

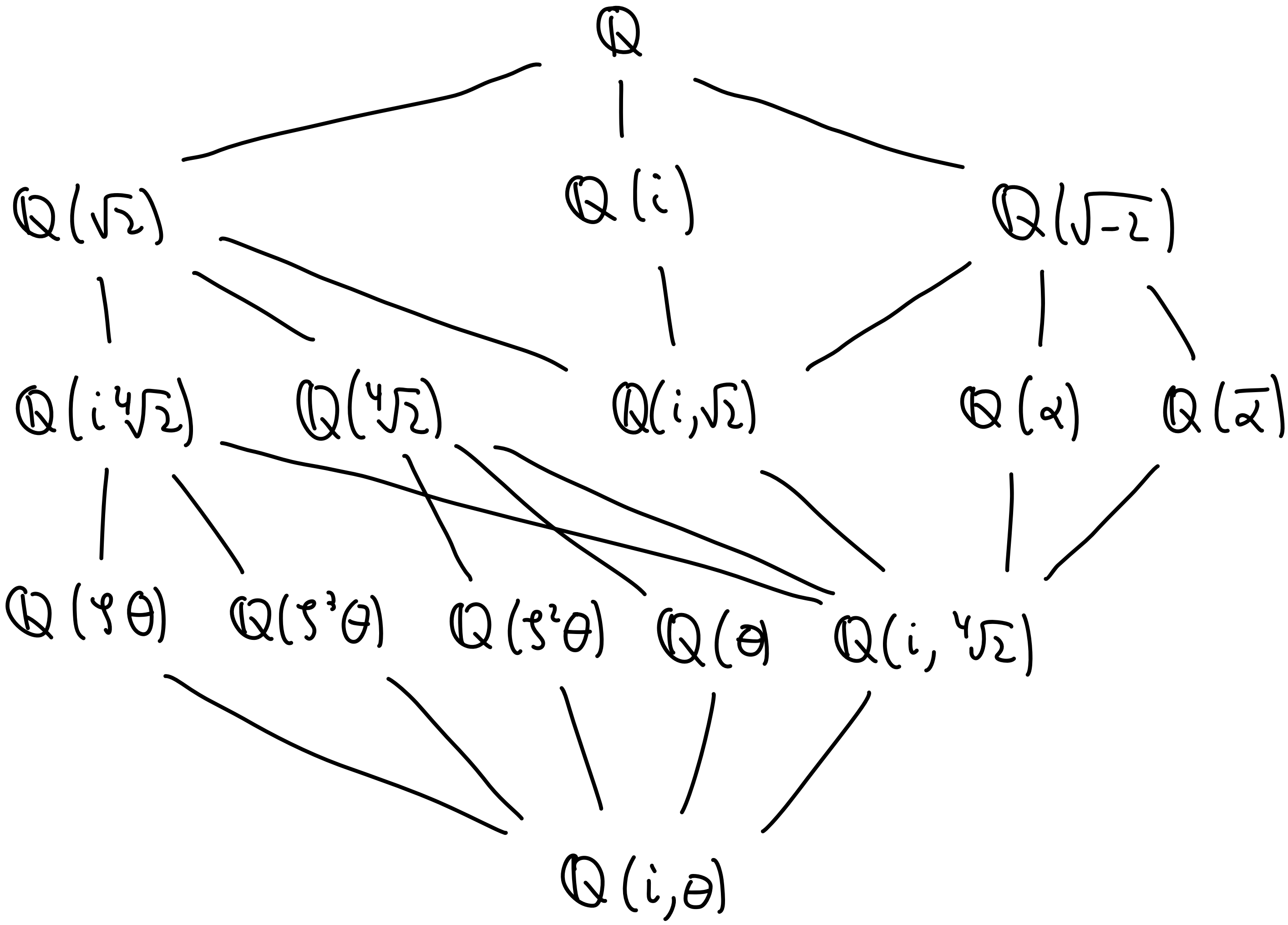
So $\text{Gal}(K/\mathbb{Q}(\alpha)) \supseteq H$ but $\text{Gal}(K/\mathbb{Q}(\alpha)) \not\supseteq \langle\sigma^2, \tau\sigma^3\rangle$

so it must equal H i.e. $\text{Fix}\,H = \mathbb{Q}(\alpha)$

$\text{Fix}\,\langle\tau\sigma\rangle = \mathbb{Q}(\tau(\alpha)) = \mathbb{Q}\big((1-i)\sqrt[4]{2}\big) = \mathbb{Q}(\bar{\alpha})$

since $\langle\tau\sigma\rangle = \tau H \tau^{-1}$, so

$\text{Fix}\,\langle\tau\sigma\rangle = \tau(\text{Fix}\,H)$



$\mathbb{Q}$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{-2})$
$\mathbb{Q}(i\sqrt[4]{2})$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(i,\sqrt{2})$
$\mathbb{Q}(\alpha)$
$\mathbb{Q}(\overline{\alpha})$
$\mathbb{Q}(\zeta\theta)$
$\mathbb{Q}(\zeta^3\theta)$
$\mathbb{Q}(\zeta^2\theta)$
$\mathbb{Q}(\theta)$
$\mathbb{Q}(i,\sqrt[4]{2})$
$\mathbb{Q}(i,\theta)$