Lecture 10.2

Last time:

- An F-homomorphism $\varphi: K \to L$ is a ring homomorphism such that $\varphi(x) = x$ for all $x \in F$.

- $\mathrm{Aut}(K/F) = \{F\text{-automorphisms } \sigma: K \to K\}$ is a group under composition.

- If $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ has automorphism group $\mathrm{Aut}(K/\mathbb{Q}) = \{id, \sigma, \tau, \tau\sigma\}$ with $|\sigma| = |\tau| = 2$, we can solve the polynomial

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$$

$f(x) = (x-r_1)(x-r_2)(x-r_3)(x-r_4)$

by radicals using the subgroup structure of $\mathrm{Aut}(K/\mathbb{Q})$.

The main theme of Galois theory is:

subfields of K/F correspond to subgroups of $\mathrm{Aut}(K/F)$.

$\boxed{\text{Lemma}}$ Let $L/K/F$ be a tower of field extensions. Then $\mathrm{Aut}(L/K)$ is a subgroup of $\mathrm{Aut}(L/F)$.

Pf: A K-automorphism $\sigma \in \mathrm{Aut}(L/K)$ also fixes every element of $F \subseteq K$, so $\sigma \in Aut(L/F)$. The group operation is still just composition, so $Aut(L/K) \subseteq Aut(L/F)$ is a subgroup. $\square$

Def For a subgroup $H \subseteq Aut(K/F)$, the **fixed field** of H is

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Lemma K^H is a subextension of K/F.

Pf: Take $\alpha, \beta \in K^H$ and $\sigma \in H$. Then

- $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta) = \alpha+\beta \in K^H$

- $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta \in K^H$

- $\sigma(-\alpha) = \sigma(-\alpha) + \sigma(\alpha) - \sigma(\alpha)$

$$= \sigma(-\alpha + \alpha) - \alpha$$

$$= \sigma(0) - \alpha = 0 - \alpha \in K^H$$

- if $\alpha \neq 0$ then

$\sigma(\alpha) = \alpha \neq 0$

$$\sigma(\alpha^{-1}) = \sigma(\alpha^{-1})\sigma(\alpha)\sigma(\alpha)^{-1}$$

$$= \sigma(\alpha^{-1}\alpha)\,\alpha^{-1}$$

$$= \sigma(1)\,\alpha^{-1} = \alpha^{-1} \in K^H.$$

So K^H is a subfield and $F \subseteq K^H$

is clear since $H \subseteq \mathrm{Aut}(K/F)$. $\square$

Exercise 1: Let K/F be a field extension. Show that if $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K/F)$, then $K^{H_2} \subseteq K^{H_1}$.

This, along with the first **Lemma** above, shows that there is an <u>inclusion-reversing correspondence</u>

$$\left\{ \begin{matrix} \text{subextensions} \\ F \subseteq E \subseteq K \end{matrix} \right\} \begin{matrix} \longrightarrow \\ \longleftarrow \end{matrix} \left\{ \begin{matrix} \text{subgroups} \\ H \subseteq \mathrm{Aut}(K/F) \end{matrix} \right\}$$

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

$$K^H \longleftarrow\!\!\shortmid \; H$$

Q: Is this correspondence bijective?

A: No!

$\boxed{\text{Ex}}$ 1 Let $K = \mathbb{Q}(\sqrt[3]{2}, i)$. We saw in Lecture 10.1 that the subfield $\mathbb{Q}(\sqrt[3]{2}) \subsetneq K$ has automorphism group

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}.$$

But $K^{\{id\}} = K$, so the correspondence is not bijective.

② Let $K = \mathbb{Q}(\sqrt{5}, -\sqrt{5}, i, -i) = \mathbb{Q}(\sqrt{5}, i)$ from Lecture 10.1. We compute

$$\mathrm{Aut}(K/\mathbb{Q}) = \{ id, \sigma, \tau, \tau\sigma \}$$

where $\sigma : \sqrt{5} \longmapsto -\sqrt{5}$ and $\tau : i \longmapsto -i$.

In this case, the correspondence between subfields and subgroups is bijective:

$$\begin{tikzcd}[column sep=small]
 & K = \mathbb{Q}(\sqrt{5}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{5}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}[column sep=small]
 & \{ id \} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \tau \rangle \arrow[dr, dash] & \langle \sigma \rangle \arrow[d, dash] & \langle \tau\sigma \rangle \arrow[dl, dash] \\
 & \mathrm{Aut}(K/\mathbb{Q}) &
\end{tikzcd}$$

If you haven't already, go prove that

$$\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Notice that in this case,

$$|\mathrm{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}] = 4.$$

3 Let $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_5 = e^{2\pi i/5}$.

We already know $[K:\mathbb{Q}] = 4$.

Let's compute $\mathrm{Aut}(K/\mathbb{Q})$.

For any $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$,

$$\sigma(\zeta)^5 = \sigma(\zeta^5) = \sigma(1) = 1$$

so $\sigma(\zeta) = \zeta^j$ for some $0 \le j \le 4$.

By a similar computation $\zeta = \sigma(\zeta^k)$ for some $0 \le k \le 4$.

This shows once again that Aut$(K/\mathbb{Q})$ acts on roots of polynomials that split in K.

Notice that

$$\zeta^{jk} = \sigma(\zeta)^k = \sigma(\zeta^k) = \zeta$$

so $jk = 5n + 1$ for some $n \in \mathbb{Z}$.

What's going on? It looks like each

what's going on: If ...

$\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ is determined by $j \in \mathbb{Z}/5\mathbb{Z}$

with the extra condition that $jk = 1$

for some $k \in \mathbb{Z}/5\mathbb{Z}$.

Define a group homomorphism

$$\varphi : \mathrm{Aut}(K/\mathbb{Q}) \longrightarrow (\mathbb{Z}/5\mathbb{Z})^\times$$

$$\sigma \longmapsto j \quad \text{where } \sigma(\zeta) = \zeta^j.$$

We claim φ is an isomorphism:

- if $\varphi(\sigma) = 1 \in (\mathbb{Z}/5\mathbb{Z})^\times$ then

$\sigma(\zeta) = \zeta$ but since

$K = \mathrm{Span}\{1, \zeta, \zeta^2, \zeta^3\}$

$K = \mathrm{span}_{\mathbb{Q}}\{1, \zeta, \zeta^2, \zeta^3\}$

this implies $\sigma = id$;

- every $\sigma(\zeta) = \zeta^i$ defines an automorphism, so φ is onto.

This shows $|\mathrm{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$.

Here, the subgroup structure is simpler:

$$
\begin{array}{ccc}
\{1\} & \qquad\qquad & \{id\} \\
| & & | \\
\langle 4 \rangle & & \langle \sigma : \zeta \mapsto \zeta^4 \rangle \\
| & & | \\
(\mathbb{Z}/5\mathbb{Z})^\times & & \mathrm{Aut}(K/\mathbb{Q})
\end{array}
$$

One can check in this case that the subgroup-subfield correspondence is bijective, so the only subfield is $K^{\langle \sigma \rangle}$ where $\sigma: \varphi \mapsto \varphi^4$:

$$\begin{array}{c} K = \mathbb{Q}(\varphi) \\ | \\ K^{\langle \sigma \rangle} = \mathbb{Q}(\varphi + \varphi^4) \\ | \\ \mathbb{Q} \end{array}$$

Exercise 2: Compute $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. Then draw the subfield and subgroup diagrams. Are they in bijection?

Next time: splitting fields.