# Lecture 13.2

Last time:

- $K/F$ is Galois if and only if it is finite and $K^{\mathrm{Aut}(K/F)} = F$.

- We are aiming to prove the Fundamental Theorem of Galois Theory, which says that for a Galois extension $K/F$, the Galois correspondence is bijective.

---

**Lemma** Let $G$ be a finite group consisting of automorphisms of some field $K$. Then

$$[K : K^G] \leq |G|.$$

**Pf:** Let $G = \{\sigma_1, \ldots, \sigma_m\}$ with $\sigma_1 = id$.

We claim that any $\alpha_1, \ldots, \alpha_n \in K$ with $n > m$ are linearly dependent over $K^G$.

Consider the linear system

$$(*) \begin{cases} \sigma_1(\alpha_1)x_1 + \ldots + \sigma_1(\alpha_n)x_n = 0 \\ \vdots \\ \sigma_m(\alpha_1)x_1 + \ldots + \sigma_m(\alpha_n)x_n = 0. \end{cases}$$

Since $n > m$, linear algebra tells us this system has a nontrivial solution

$$\beta = (\beta_1, \ldots, \beta_n) \in K^n.$$

If we can find a solution in $(K^G)^n$,

we'll be done.

Assume:

(i) $\beta$ has the minimal number of nonzero coordinates among all nontrivial solutions to (*).

(ii) $\beta_1 = 1$.

Suppose $\beta \notin (K^G)^n$. Then there is some

$\sigma \in G$ with $\sigma(\beta_j) \neq \beta_j$ for some $j$.

Since $G = \{\sigma \in G : \sigma(\beta_j) = \beta_j\} = G_{\beta_j}$, the

Since $\sigma U = \{\sigma a_1, \ldots, \sigma a_m\} = U$, the linear system $(*)$ is unchanged by acting by $\sigma$:

$$(*)\begin{cases} \sigma a_1(\alpha_1)x_1 + \ldots + \sigma a_1(\alpha_n)x_n = 0 \\ \vdots \\ \sigma a_m(\alpha_1)x_1 + \ldots + \sigma a_m(\alpha_n)x_n = 0. \end{cases}$$

Then $\sigma(\beta) = (\sigma(\beta_1), \ldots, \sigma(\beta_n))$ is a solution to $(*)$ and therefore so is $\sigma(\beta) - \beta$.

Since $\sigma(\beta_j) \neq \beta_j$, this is a nontrivial solution to $(*)$, but $\sigma(\beta_1) - \beta_1 = \sigma(1) - 1 = 0$ so $\sigma(\beta) - \beta$ has fewer nonzero coordinates than

$\beta$, a contradiction.

Therefore $\sigma(\beta) = \beta$ for every $\sigma \in G$ so

$\beta \in (K^G)^n$. $\square$

Now it's time to prove the big theorem.

**Theorem (Fundamental Theorem of Galois Theory)**

Let $K/F$ be a Galois extension. Then

(1) The Galois correspondence between subfields of $K/F$ and subgroups of $\mathrm{Gal}(K/F)$ is an inclusion-reversing bijection.

(2) If $H \subseteq G \subseteq \mathrm{Gal}(K/F)$ are subgroups,

then $[G : H] = [K^H : K^G]$.

(3) For each subgroup $H \subseteq \mathrm{Gal}(K/F)$, there is a bijection

$$\left\{ \begin{array}{c} \text{conjugate subgroups} \\ H' \subseteq \mathrm{Gal}(K/F) \text{ of } H \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subfields} \\ E \cong K^H \end{array} \right\}.$$

(4) The Galois correspondence determines a bijection between normal subgroups $N \trianglelefteq \mathrm{Aut}(K/F)$ and normal subfields $K^N/F$. For any such $N$,

$$\mathrm{Gal}(K^N/F) \cong \mathrm{Gal}(K/F)/N.$$

$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K/E)/N$.

Pf: (1) By Exercise 1 in Lecture 13.1, for any subfield $F \subseteq E \subseteq K$, $K/E$ is Galois, so by our characterization of Galois extensions, $K^{\mathrm{Aut}(K/E)} = E$.

On the other hand, take $H \subseteq \mathrm{Aut}(K/F)$ and consider the subgroup $\mathrm{Aut}(K/K^H)$. Every element of $H$ fixes $K^H$, so

$H \subseteq \mathrm{Aut}(K/K^H)$.

But $K/K^H$ is Galois so by the Lemma,

$$|\mathrm{Aut}(K/K^H)| = [K : K^H] \leq |H|.$$

Hence $H = \mathrm{Aut}(K/K^H)$.

(2) Take $H \subseteq G \subseteq \mathrm{Aut}(K/F)$. Then (1) shows $|H| = [K : K^H]$ and $|G| = [K : K^G]$.

By the tower law,

$$[G : H] = \frac{|G|}{|H|} = \frac{[K : K^G]}{[K : K^H]} = [K^H : K^G].$$

(3) Fix $H \leq \mathrm{Aut}(K/F)$ and take $\sigma \in \mathrm{Aut}(K/F)$.

Then $\sigma H \sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in H\}$ is another subgroup of $\mathrm{Aut}(K/F)$, so it corresponds

to a unique subfield $E$ of $K/F$.

We claim $E = \sigma(K^H)$; since $\sigma$ is an automorphism of $K$, this will give us $K^H \cong E$.

Notice that for any $\alpha \in K$,

$$\alpha \in K^H \iff \tau(\alpha) = \alpha \text{ for all } \tau \in H$$

$$\iff \sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma(\alpha) \text{ for all } \tau \in H$$

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

This shows $E = \sigma(K^H)$.

(4) We need to show that

$N \subseteq Aut(K/F)$ is normal $\iff$ $K^N/F$ is a normal extension.

First assume $K^N/F$ is normal and take $\sigma \in Aut(K/F)$ and $\alpha \in K^N$ with minimal polynomial $p_\alpha \in F[x]$.

Then $p_\alpha$ splits over $K^N$ so $\sigma(\alpha)$, which is another root of $p_\alpha$, lies in $K^N$.

This shows $\sigma(K^N) \subseteq K^N$ but both are finite extensions of $F$, so $\sigma(K^N) = K^N$.

By (3), $\sigma N \sigma^{-1} = N$ for every $\sigma \in Aut(K/F)$, so $N$ is normal.

Conversely, if $N$ is normal, then (3) says

$$\sigma(K^N) = K^N \quad \text{for every} \quad \sigma \in \mathrm{Aut}(K/F).$$

That is, every $F$-automorphism of $K$ restricts to an $F$-automorphism of $K^N$.

Define

$$\varphi : \mathrm{Aut}(K/F) \longrightarrow \mathrm{Aut}(K^N/F)$$

$$\sigma \longmapsto \sigma|_{K^N}.$$

This is a group homomorphism with

$$\ker(\varphi) = \{\sigma : \sigma|_{K^N} = \mathrm{id}\}$$

$= \mathrm{Aut}(K/K^N) = N.$

$\uparrow$

by (1)

If $\alpha \in (K^N)^{\mathrm{im}(\varphi)}$ then $\alpha \in K^{\mathrm{Aut}(K/F)} = F$,

so $(K^N)^{\mathrm{im}(\varphi)} = F$ and therefore

$K^N/F$ is Galois and in particular

normal.

Finally, $|\mathrm{Aut}(K^N/F)| = [K^N : F]$

$= [K^N : (K^N)^{\mathrm{im}(\varphi)}]$

$\leq |\mathrm{im}(\varphi)|$ by the Lemma.

So $\mathrm{Aut}(K^N/F) = \mathrm{im}(\varphi)$ and the First

Isomorphism Theorem for groups,

$$\mathrm{Aut}(K^N/F) \cong \mathrm{Aut}(K/F)/N. \quad \square$$

Next time: applications.