Lecture 12.1

Last time:

- K/F is normal $\iff$ $K = K_f$ for some $f \in F[x]$.

- K/F is separable $\iff$ every $\alpha \in K$ has $p_\alpha(x) \in F[x]$ with no repeated roots.

- K/F is Galois if it is finite, normal and separable.

Galois Theory

Note: when K/F is Galois, we will

write $\mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$.

Recall that for certain K/F, we can find or bound $[K:F]$:

- Simple extensions: $[F(\alpha):F] = \deg p_\alpha$
- Splitting fields: $[K_f : F] < (\deg f)!$

Prop Let $F(\alpha)/F$ be a simple extension with α algebraic over F. Then for any field extension K/F, there is a bijection

$$\left\{ \begin{array}{c} F\text{-homomorphisms} \\ \varphi : F(\alpha) \to K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{roots of } p_\alpha(x) \\ \text{in } K \end{array} \right\}.$$

Pf: For an F-homomorphism $\varphi : F(\alpha) \to K$

(1): For an F-homomorphism $\varphi: F(\alpha) \to K$,

let $\beta = \varphi(\alpha)$. If

$$p_\alpha(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$$

then

$$p_\alpha(\beta) = a_0 + a_1 \varphi(\alpha) + \dots + a_n \varphi(\alpha)^n$$

$$= \varphi(a_0 + a_1 \alpha + \dots + a_n \alpha^n)$$

$$= \varphi(0) = 0.$$

So β is a root of $p_\alpha(x)$.

On the other hand, if $\beta \in K$ is a root of

$p_\alpha(x)$, we need to construct a map

$\varphi: F(\alpha) \to K$.

We know $F(\alpha) = \text{Span}\{1, \alpha, \dots, \alpha^{n-1}\}$ where

$n = \deg p_\alpha$, so define

$$\varphi : F(\alpha) \longrightarrow K$$

$$\sum_{j=0}^{n-1} c_j \alpha^j \longmapsto \sum_{j=0}^{n-1} c_j \beta^j.$$

Exercise 1 : Check φ is an F-homomorphism.

Now let's show

$$\left\{ \begin{array}{c} F\text{-homomorphisms} \\ \varphi : F(\alpha) \to K \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{roots of } p_\alpha(x) \\ \text{in } K \end{array} \right\}$$

$$\varphi \longmapsto \beta = \varphi(\alpha)$$

$$(\varphi : \alpha \mapsto \beta) \longmapsto \beta$$

is a bijection.

Clearly sending β to $\varphi : \alpha \mapsto \beta$ defined above and then extracting $\varphi(\alpha)$ recovers β as a root of p_α.

On the other hand, any F-homomorphism $\varphi : F(\alpha) \to K$ is completely determined by where it sends α, so the other composition $\varphi \mapsto \varphi(\alpha) \mapsto (\alpha \mapsto \varphi(\alpha))$ is also the identity. $\square$

Corollary For a simple algebraic extension $F(\alpha)/F$,

$|\mathrm{Aut}(F(\alpha)/F)| = \#\{\text{roots of } p_\alpha \text{ in } F(\alpha)\}$.

Pf: Apply the Proposition with $K = F(\alpha)$. □

Ex ① In Lecture 10.2, we showed that $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{F}_5^\times \cong \mathbb{Z}/4\mathbb{Z}$.

Explicitly, we exhibited the bijection from the Proposition as

$$\left\{\begin{array}{c}\text{roots of} \\ x^4+x^3+x^2+x+1\end{array}\right\} \longleftrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$$

$$\zeta_5^{\,j} \longleftrightarrow \left(\sigma^j : \zeta_5 \mapsto \zeta_5^{\,j}\right).$$

(2) Non-splitting fields make counting roots more difficult.

Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[3]{2})$.

We saw in Lecture 10.1 that

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

which corresponds to the single root $\sqrt[3]{2}$ of $x^3 - 2$ in K.

A splitting field for $x^3 - 2$ is

$$L = K(\zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3), \quad \zeta_3 = e^{2\pi i/3}.$$

Now $L/\mathbb{Q}$ is not visibly a simple

extension, but L/K is, so

$$|\mathrm{Aut}(L/K)| = \#\{\text{roots of } \underbrace{x^2+x+1}_{P_{3,3}(x)} \text{ in } L\} = 2.$$

Therefore $\mathrm{Aut}(L/K)$ is an order 2 subgroup of $\mathrm{Aut}(L/\mathbb{Q})$ — can you see which $\mathbb{Q}$-automorphism generates it?

Let's see if we can determine $|\mathrm{Aut}(L/\mathbb{Q})|$.

Any $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ restricts to a map

$$\sigma|_K : K \longrightarrow L \quad \text{and since } K = \mathbb{Q}(\sqrt[3]{2})$$

$$\begin{array}{ccc} K & \longrightarrow & L \\ \cap & \nearrow_{\sigma} & \\ L & & \end{array}$$

is simple, we can apply the Proposition

to get

$$\#\{\varphi : K \to L\} = \#\{\text{roots of } x^3 - 2 \text{ in } L\} = 3.$$

So $|\mathrm{Aut}(L/\mathbb{Q})| \geq 3$ but we also know

$|\mathrm{Aut}(L/\mathbb{Q})| \leq 3! = 6$ since L is a splitting field.

Since it has an order 2 subgroup, $\mathrm{Aut}(L/\mathbb{Q})$ must have order 4 or 6.

Exercise 2: Show $|\mathrm{Aut}(L/\mathbb{Q})| = 6$. Is this group isomorphic to $\mathbb{Z}/6\mathbb{Z}$ or S_3?

What makes this example work is that $L/\mathbb{Q}$ is a normal extension containing the non-normal extension $K/\mathbb{Q}$ as a subfield.

Def For any field extension K/F, a normal closure of K/F is an extension L/K such that L/F is normal and no subextension $K \subseteq L' \subsetneq L$ is normal over F.

Notice that if K/F is normal to begin

with, it is its own normal closure.

Theorem If $F \subseteq K \subseteq \mathbb{C}$ is a finite extension, there exists a unique normal closure L/K which is also finite.

Pf: Use splitting fields. $\square$

For the next theorem, assume again that everything is a subfield of $\mathbb{C}$.

Theorem Let K/F be a finite extension with $[K:F] = n$ and normal closure L/K. Then

$$\#\left\{\begin{matrix}F\text{-homomorphisms} \\ K \to L\end{matrix}\right\} = n.$$

Pf: Induct on n — the base case with $n = 1$ is trivial (but make sure you understand it).

Take $\alpha \in K \setminus F$ with minimal polynomial p_α, say of order m.

Then $m = [F(\alpha) : F] \leq [K : F] = n$ by the tower law.

If $K = F(\alpha)$, the Proposition earlier says

$$\#\{F(\alpha) \to L\} = \#\{\text{roots of } p_\alpha \text{ in } L\} = m = n.$$

Otherwise, $m < n$ and we can use induction.

Since p_α is irreducible over $F \subseteq \mathbb{C}$, it is separable, so it has exactly m roots in L.

Write

$$n = [L : F] = [L : F(\alpha)][F(\alpha) : F] = km.$$

By induction,

$$\left\{ \begin{array}{c} F(\alpha)\text{-automorphisms} \\ K \longrightarrow L \end{array} \right\} = \{\sigma_1, \ldots, \sigma_k\}$$

while there are (at least) m F-homomorphisms

$$\tau_1, \ldots, \tau_m : L \longrightarrow L$$

sending α to each of the m roots of p_α in L.

We claim $\{\tau_\ell \sigma_j \mid 1 \le j \le k,\ 1 \le \ell \le m\}$ is the complete set of F-homomorphisms $K \to L$.

First, they are F-homomorphisms since each σ_j and τ_ℓ is an F-homomorphism.

Next, they are distinct since they send α to different elements of L.

Finally, let $\varphi : K \to L$ be any F-homomorphism. Then $\varphi(\alpha)$ is a root of p_α, so for one of the τ_ℓ, $\tau_\ell^{-1}\varphi : K \to L$ is equal

to one of the $\sigma_j : K \to L$.

Hence $\varphi = \tau_\ell \circ \sigma_j$. □

Corollary If K/F is a finite normal extension of subfields of $\mathbb{C}$,

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

Pf: Apply the Theorem with $L = K$. □

Next time: The Galois correspondence.