Lecture 13.1

Last time:

- For a simple extension $F(\alpha)/F$ and any extension K/F,

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

- A **normal closure** of K/F is a smallest extension L/K such that L/F is normal.

- For any finite extension K/F with normal closure L/K,

$$\# \left\{ \begin{array}{c} F\text{-homomorphisms} \\ K \to L \end{array} \right\} = [K : F]$$

$\{ K \to L \}$ $[K:F]$.

- In particular, if K/F is normal,

$$|Gal(K/F)| = [K:F].$$

Recall: for any field extension K/F, there is a correspondence

$$\left\{ \begin{array}{l} \text{subfields} \\ F \subseteq E \subseteq K \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{subgroups} \\ H \subseteq Aut(K/F) \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{subfields} \\ F \subseteq E \subseteq K \end{array} \right\} \longleftarrow \left\{ \begin{array}{l} \text{subgroups} \\ H \subseteq Aut(K/F) \end{array} \right\}$$

$$E \longmapsto Aut(K/E)$$

$$K^H \longmapsfrom H$$

We are going to prove that this is a bijection when K/F is Galois.

Much more is true though:

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,

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

We need some preliminary results before

proving the Fundamental Theorem.

Theorem Let K/F be any field extension. Then the following are equivalent:

(1) K/F is Galois (= finite, separable and normal).

(2) $K = K_f$ for some separable $f \in F[x]$.

(3) K/F is finite and $K^{\mathrm{Aut}(K/F)} = F$.

Compare this to a similar theorem in Lecture 11.2.

Pf: (1) $\Rightarrow$ (2) As in that proof in Lecture 11.2, K/F normal implies $K = K_f$ for some $f \in F[x]$. Moreover, if $f = g_1 \cdots g_r$ for irreducible $g_j \in F[x]$, then each g_j is separable, so either f is too, or we can replace f by its largest separable factor.

(2) $\Rightarrow$ (3) We know $[K:F] < (\deg f)!$ so K/F is finite. On the other hand, since K/F is normal, the Corollary

from the end of Lecture 12.1 shows

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

Claim: $\mathrm{Aut}(K/K^{\mathrm{Aut}(K/F)}) = \mathrm{Aut}(K/F)$.

We already know (by the correspondence)

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

but by definition, every element of $\mathrm{Aut}(K/F)$ fixes $K^{\mathrm{Aut}(K/F)}$, so these groups are equal.

Now by the tower law,

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

which implies $[K^{Aut(K/F)} : F] = 1$ and so

$K^{Aut(K/F)} = F$.

(3) $\Rightarrow$ (1) Take $\alpha \in K$ with minimal polynomial $p_\alpha(x) \in F[x]$.

Let $\alpha, \alpha_2, \ldots, \alpha_n$ be the roots of $p_\alpha(x)$ in K and put

$$f(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n) \in K[x].$$

For any $\sigma \in Aut(K/F)$ and α_j, $1 \le j \le n$, $\sigma(\alpha_j)$ is again a root of $p_\alpha(x)$ in K, hence a root of $f(x)$.

This shows that $f(x) \in K^{Aut(K/F)}[x] = F[x]$,

so $p_\alpha(x) \mid f(x)$.

But every factor $x - a_j$ in $f(x)$ is also a factor in $p_\alpha(x)$ (in some splitting field) so $f(x) \mid p_\alpha(x)$, forcing $f(x) = p_\alpha(x)$.

Hence $p_\alpha(x)$ splits in K, implying K/F is normal.

Of course, the roots of a minimal polynomial are always distinct so K/F is also separable, hence Galois. □

Corollary Let K/F be a finite extension. Then K/F is Galois if and only if K is the splitting field of a separable polynomial $f(x) \in F[x]$.

Corollary Let $F \subseteq E \subseteq K$ be a tower of fields. If K/F is Galois, then so is K/E.

Exercise 1: Prove it!

One last tool:

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

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

Next time: a proof of the lemma and

the Fundamental Theorem.