Last class: Char $F = 0$.

K/F finite extension.

$K = F(\alpha)$.

$F(\alpha, \beta) = F(\alpha + c\beta)$. $c \in F$.

almost all c works.

Splitting field of $f(x) \in F[x]$. over F

if ① $f(x)$ splits completely with roots $\alpha_1 \dots \alpha_n$.

② $K = F(\alpha_1, \dots \alpha_n)$

Prop: ① $\forall f$. Splitting field exists

② $F \subset L \subset K$, K is splitting field of $f(x)$ over F. then also splitting field over L.

③ K/F finite extension.

There exist $\tilde{K}/K$ a splitting field.

Pf: (Existence) Keep adding roots to split $f(x)$ completely and define $K = F(\alpha_1 \cdots \alpha_n)$

Example: $w = e^{\frac{2\pi i}{3}}$. $f(x) = x^3 - 2$.

$\mathbb{Q}(w, \sqrt[3]{2}) \to$ This is the splitting field of $f(x)$ over $\mathbb{Q}$

$|$

$\mathbb{Q}(w) \to$ This is not.

$|$

$\mathbb{Q}$

Most important Thm of splitting field.

Thm: If K/F is a splitting field of $f(x) \in F[x]$, and $g(x) \in F[x]$ is irreducible with one root $\alpha \in K$, then $g(x)$ splits completely in K.

Prop: (Uniqueness of splitting field)

① $K_1 \subset L$, $K_2 \subset L$. $F \subset K_i$. $f(x) \in F[x]$, Assume K_1 and K_2 are both splitting field of $f(x)$

Then $K_1 = K_2$

② If K_1, K_2 are both splitting field of $f(x) \in F[x]$, then

$K_1 \cong K_2$

Pf: ① $K_1 = K_2 = F(\alpha_1 \cdots \alpha_n)$

② choose $K_1 = F[\alpha_1]$. $K_2 = F[\alpha_2]$.

α_1, α_2. α_1 has irreducible polynomial $g(x)$

choose L/K_2 such that $g(x)$ splits completely with one root $\tilde{\alpha}$.

$$\begin{tikzcd}
 & L \arrow[d, dash] \arrow[dr, dash] & \\
K_1 \cong & \tilde{K} \arrow[d, dash] & K_2 \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

choose $\tilde{K} = F[\tilde{\alpha}]$.

Then $K_1 \cong \tilde{K}$. $\tilde{K}$ is also a splitting field of $f(x)$

so $\tilde{K} = K_2$. from ①.

Galois group. $G(K/F)$

$$G(K/F) = \{ g : K \to K \text{ isomorphism} \mid g|_F = id_F . \}$$

$K = \mathbb{Q}[\sqrt{2}, i] \Big/ \mathbb{Q}[\sqrt{2}] = F$

$G(K/F) = \{ id, \ \sigma : a \mapsto \bar{a} \}$.

$$G(K/\mathbb{Q}) = \left\{ \begin{array}{ll} id, & \sigma_1 : \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \end{array} \\ \sigma_2 : \begin{array}{l} i \mapsto -i \\ \sqrt{2} \mapsto \sqrt{2}. \end{array} & \sigma_3 : \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{array} \end{array} \right\}$$

How to specify an element σ in $G(K/F)$?

If $K = F[\alpha]$, we only need to know $\sigma(\alpha)$.

$\sigma(\sum a_i \alpha^i) = a_i \sum \sigma(\alpha)^i$

Prop: $\alpha \in K$, α is a root of $f(x)$
then $\sigma(\alpha)$ is a root of $f(x)$.

① Splitting field $K = F(\alpha)$.

then $\sigma(\alpha) = \alpha_i$.

$(\alpha_1 \ldots \alpha_n)$ are the roots
of irreducible polynomial of
$f(x)$

Two aspects. a) α_i determines σ uniquely.
b) For each α_i, there exists
σ_i such that $\sigma_i(\alpha) = \alpha_i$

In other words $|G(K/F)| = n = [K:F]$

Example: $K = \mathbb{Q}(\sqrt{3}+\sqrt{5}) / \mathbb{Q}$.

$$G(K/\mathbb{Q}) = \left\{ \begin{array}{l} \sigma_1 : \sqrt{3}+\sqrt{5} \longmapsto \sqrt{3}+\sqrt{5} \\ \sigma_2 : \sqrt{3}+\sqrt{5} \longmapsto \sqrt{3}-\sqrt{5} \\ \sigma_3 : \sqrt{3}+\sqrt{5} \longmapsto -\sqrt{3}+\sqrt{5} \\ \sigma_4 : \sqrt{3}+\sqrt{5} \longmapsto -\sqrt{3}-\sqrt{5} \end{array} \right\}$$

(2) In the case that K/F is not a splitting field, then $|G(K/F)| < [K:F]$

In fact $|G(K/F)| \,\Big|\, [K:F]$

Example: $K = \mathbb{Q}[\sqrt[3]{2}]$.

then $G(K/F) = \{1\}$.

because any root of x^3-2 other than $\sqrt[3]{2}$ is not in K.

Fixed fields. H is a finite subgroup of $\text{Aut}(K)$

$$H \subset \text{Aut}(K)$$

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \ \forall \sigma \in H\}.$$

① H finite. $\beta \in K$. $\{\beta_1, \ldots, \beta_r\}$ is the H-orbit of β.

then the irreducible polynomial of β over K^H is

$$(x - \beta_1) \cdots (x - \beta_r).$$

② $[K : K^H]$ is finite.

and $[K : K^H] = |H|$.

Pf: ① $\beta_1 + \cdots \beta_r \in K^H$ because $\sigma \in H$ only change the order of $\beta_1, \ldots \beta_r$

Galois extension K/F

TFAE: (1) K/F is a splitting field.

(2) $G(K/F) = [K:F]$

(3) $F = K^H$ for some H finite in $\mathrm{Aut}(K)$

(1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3), and K/F satisfies this proposition is called Galois extension.

Galois correspondance: K/F Galois

$$\left\{ \begin{array}{l} L \text{ intermediate field} \\ \text{between } K/F. \\ \text{i.e. } F \subset L \subset K \end{array} \right\} \overset{1:1.}{\longleftrightarrow} \left\{ \begin{array}{l} H. \\ \text{Sub groups} \\ \text{of } K/F \end{array} \right\}$$

$$L \longrightarrow \mathrm{Gal}(K/L).$$

$$K^H \longleftarrow H$$

Example (will be explained in the last class)

$K = \mathbb{Q}(\omega, \sqrt[3]{2})$. (splitting field of $f(x) = x^3 - 2$)

$$\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\sqrt[3]{2}\omega) & \mathbb{Q}(\sqrt[3]{2}\omega^2) & \mathbb{Q}(\omega) \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[u, dash, "3"'] \arrow[ur, dash, "3"] \arrow[urr, dash, "2"'] & &
\end{tikzcd}$$

$G(K/\mathbb{Q}) \cong S_3 = \langle \sigma, \tau \rangle$. $\sigma^3 = \tau^2 = 1$

$\tau\sigma\tau = \sigma^2$.

$$\begin{tikzcd}
 & \{1\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "3"] & & \\
\langle \tau \rangle & \langle \sigma\tau \rangle & \langle \sigma^2\tau \rangle & \langle \sigma \rangle \\
 & S_3 \arrow[ul, dash, "3"] \arrow[u, dash, "3"'] \arrow[ur, dash, "3"] \arrow[urr, dash, "2"'] & &
\end{tikzcd}$$