

Last class: $\text{Char } F = 0$.

K/F finite extension.

$$K = \bar{F}(\alpha).$$

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

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.

then exist \bar{K}/K

a splitting field.

Pf: (Existence) Keep adding roots to
split $f(x)$ completely and
define $K = F(d_1, \dots, d_n)$

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

$\mathbb{Q}(w, \sqrt[3]{2}) \rightarrow$ This is the splitting
field of
 $\mathbb{Q}(w) \rightarrow$ This is not. field of
 \mathbb{Q} $f(x)$ over \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

$$K_1 \cong K_2$$

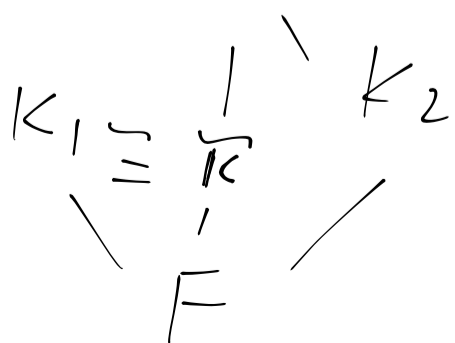
Pf: ① $K_1 = K_2 = F(\alpha_1 \dots \alpha_n)$

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

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



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 $G(K/F)$

$$G(K/F) = \left\{ g: K \rightarrow K \text{ isomorphisms} \mid g|_F = \text{id}_F \right\}$$

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

\downarrow
 F

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

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

How to specify an element σ in

$$G(K/F)?$$

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

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

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

$(\alpha_1, \dots, \alpha_n)$ all 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: $K = \mathbb{Q}(\sqrt{3} + \sqrt{5}) / \mathbb{Q}$.

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

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

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

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

$$K^{H-1} = \left\{ \alpha \in K \mid \sigma(\alpha) = \alpha \right. \\ \left. \forall \sigma \in H \right\}$$

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

then the irreducible polynomial of
 β over K^{H-1} is

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

② $[K : K^{H-1}]$ is finite.

$$\text{and } [K : K^{H-1}] = |H|$$

Pf: ① $\beta_1, \dots, \beta_r \in K^{H-1}$ because $\sigma \in H$ only change
the order of β_1, \dots, β_r

Galois extension K/F

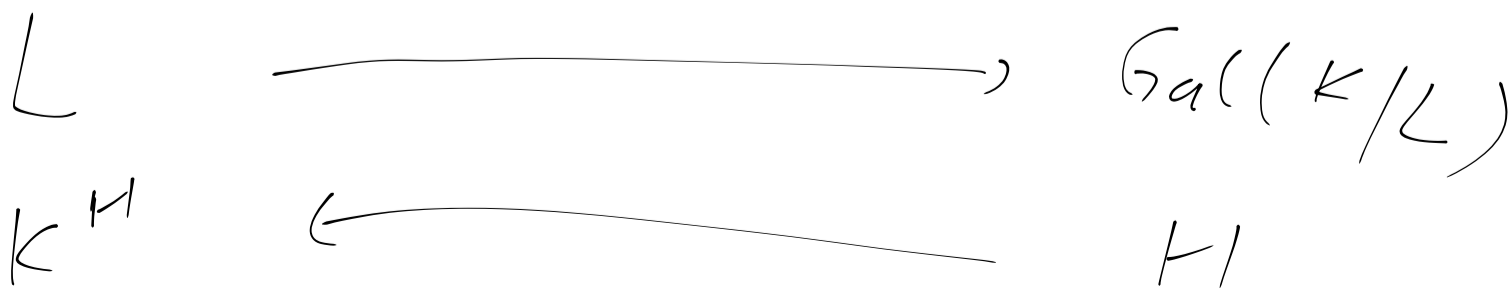
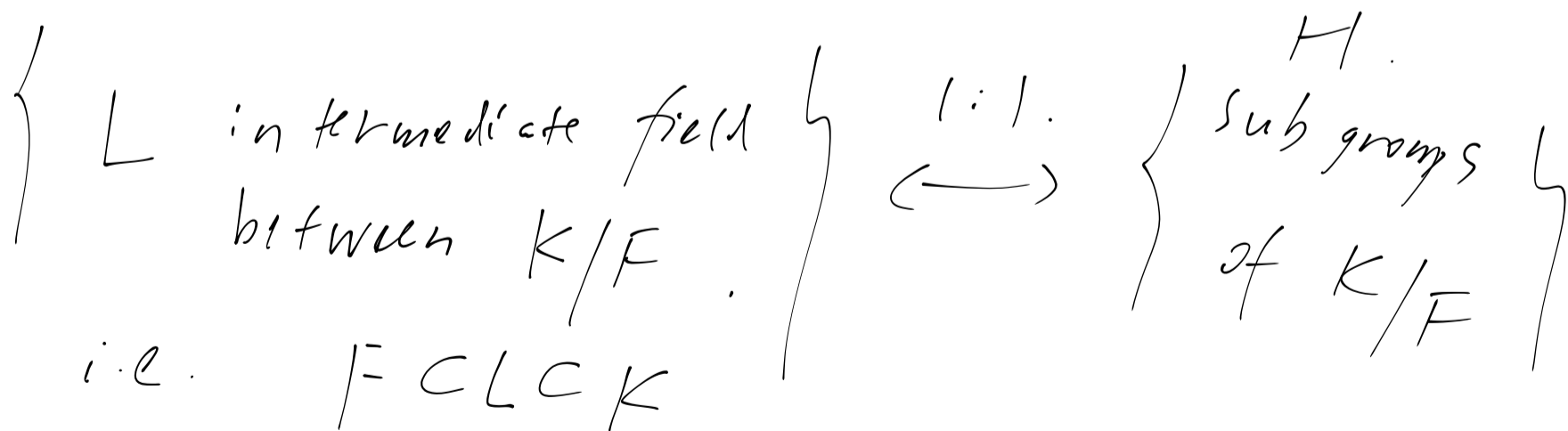
IFAE: (1) K/F is a splitting field.

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

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

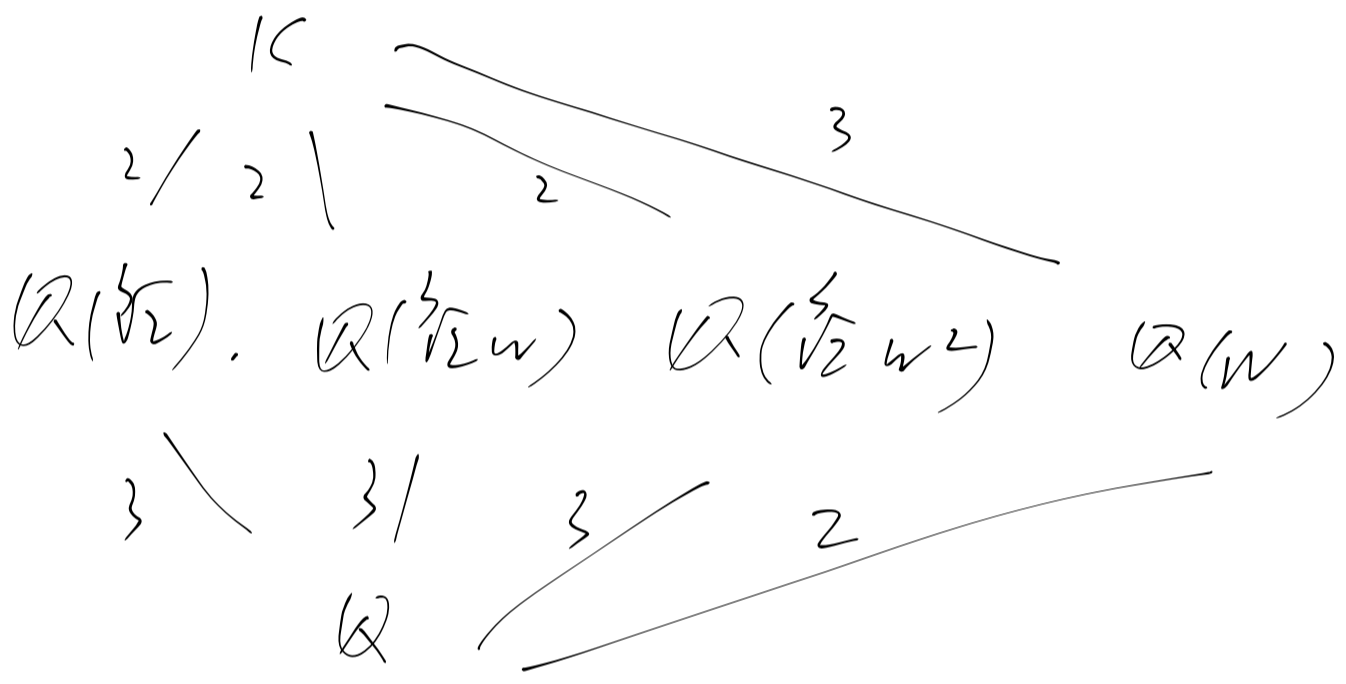
(1) \Leftrightarrow (2) \Leftrightarrow (3), and K/F satisfies this proposition is called Galois extension.

Galois correspondence: K/F Galois



Example (will be explained in the last class)

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



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

