3 Galois theory

3.1 Normal extensions

Def: • L/K

Then $f \in K[T]$ splits over L if

$f = u \prod (T - a_i)$ in $L[T]$.

• $\{f_i\}_{i \in I} \subset K[T]$

A splitting field of $\{f_i\}$ over K is

a field extension L/K such that

– f_i splits over L for every $i \in I$;

– L is generated over K by the roots of all the f_i.

Rem: If $\{f_1 - f_n\} \subset K[T]$ is finite, then L/K is a splitting field of $\{f_1 - f_n\}$ iff. it is a splitting field of $f_1 \cdots f_n$.

Ex: $f = T^3 - 2 \in \mathbb{Q}[T]$, $\zeta_3 = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ (third root of unity)

$\rightsquigarrow f = \prod_{i=1}^{3} (T - \zeta_3^i \cdot \sqrt[3]{2})$

in $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3^i \sqrt[3]{2} \mid i = 1,2,3)$

$\Rightarrow L/K$ is a splitting field of $f/\mathbb{Q}$

but: $\mathbb{Q}(\sqrt[3]{2})$ is not since $f = (T - \sqrt[3]{2})\underbrace{(T^2 + \sqrt[3]{2} + \sqrt[3]{4})}_{\text{irreducible in } \mathbb{Q}(\sqrt[3]{2})}$

$$\begin{array}{c} \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ \mathbb{Q} \end{array}$$

Prop 1: $\bar{K}$ alg. cl. of K

$\{f_i\}_{i\in I} \subset K[T]$, $n_i := \deg f_i$

$$f_i = v_i \cdot \prod_{k=1}^{n_i} (T - a_{i,k}) \in \bar{K}[T]$$

Then $K(a_{i,k})_{\substack{i\in I \\ k=1 - n_i}}$ is a splitting field of $\{f_i\}$ over K.

$$\begin{tikzcd} L \arrow[r, "\sigma"] \arrow[dr, dash] & \bar{K} \arrow[d, dash] \\ & K \end{tikzcd}$$

If L/K is another splitting field of $\{f_i\}$ over K and $\sigma: L \to \bar{K}$ a field homomorphism that fixes K, then $\sigma(L) = K(a_{i,k})$.

In particular, any two splitting fields of $\{f_i\}$ over K are isomorphic.

proof: • $K(a_{i,k})$ gen. by roots $a_{i,k}$ of f_i and

$f_i = v_i \prod (T - a_{i,k})$ in $K(a_{i,k})[T]$

$\Rightarrow K(a_{i,k})$ is a splitting field of $\{f_i\}$ over K.

• Let L/K be another splitting field,

and $f_i = v_i \prod (T - b_{i,k}) \in L[T]$.

$$\begin{tikzcd} L \arrow[rr, "\sigma"] & & \overline{K} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

Since

$$u_i \prod_{k=1}^{n_i} (T - a_{i,k}) = f_i = \sigma(f_i) = \sigma(u_i) \prod_{k=1}^{n_i} (T - \sigma(b_{i,k})),$$

and $\overline{K}[T]$ is a UFD, we have $\{\sigma(b_{i,k})\} = \{a_{i,k}\}$. Thus the image of $\sigma : L = K(b_{i,k}) \longrightarrow \overline{K}$ is $K(a_{i,k})$.

- Given a splitting field L of $\{f_i\}$ over K, there exists a K-linear hom. $\sigma : L \longrightarrow \overline{K}$ by Lemma 2.2.7. Thus $L \simeq K(a_{i,k})$.

$\square$

<u>Def</u>: A field extension L/K is <u>normal</u> if it is algebraic and if every irreducible $f \in K[T]$ with a root $a \in L$ splits over L.

<u>Ex</u>: (1) K/K is normal.

(2) L/K of degree 2. If $f \in K[T]$ is irreducible with root $a \in L$, then

$$\deg f = \dim_K \left(K[T]/(f) \right) \le \dim_K L = 2,$$

and $T-a$ divides f.

Thus $f = u(T-a)$ $(\deg f = 1)$

or $f = u(T-a)\cdot(T-b)$ for some $b \in L$

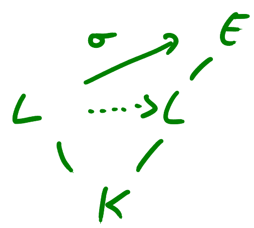
In each case, f splits over L.

Thus L/K is normal.

Thm 2: L/K alg., E/L arbitrary

Equiv: (1) L/K normal.

(2) L is a splitting field of some $\{f_i\} \subset K[T]$.



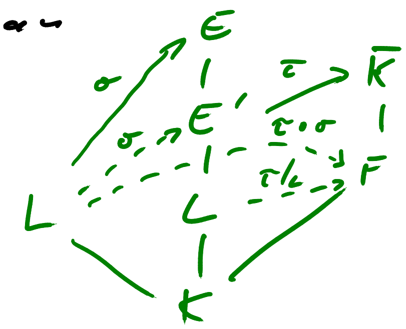
(3) Every K-linear hom. $\sigma : L \to E$ has image $\sigma(L) = L$.

proof: (1) $\Rightarrow$ (2): Consider $\{f_a\}_{a \in L}$ where $f_a = \mathrm{mipo}_a$ is the min. pol. of a over K. Then f_a splits over L by (1), and $L = K(a \mid a \in L)$; thus (2).

(2) $\Rightarrow$ (3): Let L be the splitting field of $\{f_i\} \subset K[T]$, and consider a K-linear $\sigma : L \to E$. Since L/K is algebraic, $\mathrm{im}(\sigma) \subset E' = \{a \in E \mid a \text{ alg. over } K\}$

$$= \bigcup_{\substack{K \subset F \subset E \\ F/K \text{ alg.}}} F.$$

Since E'/K is algebraic, there is a K-linear hom. $\tau : E' \longrightarrow \bar{K}$ by Lemma 2.2.7 where $\bar{K}$ is an alg. cl. of K.



By Prop. 1, $\bar{K}$ contains a unique splitting field F of $\{f_i\}$ over K.

$$\Rightarrow \quad \tau(\sigma(L)) = F = \tau(L)$$

$$\underset{(\tau \text{ injective})}{\Rightarrow} \quad \sigma(L) = L.$$

<u>(3) ⟹ (1):</u> • Let $f \in K[T]$ be irreducible and $a \in L$ a root of f; <u>want</u>: f splits over L.

• Let $b \in \bar{L}$ be another root of f. Then we have K-linear hom.

$$\begin{tikzcd} L \arrow[r, dashed, "\sigma_L"] & \bar{K} \cong \bar{L} \\ K(a) \arrow[u, dash] \arrow[ur, "\sigma"] & \\ K \arrow[u, dash] \arrow[uur, dash] & \end{tikzcd}$$

$$\sigma: K(a) \xrightarrow{\sim} K[T]/(f) \xrightarrow{\sim} K(b) \hookrightarrow \bar{L}$$
$$a \longmapsto [T] \longmapsto b$$

which extends to a homomorphism $\sigma_L : L \longrightarrow \bar{K} \cong \bar{L}$ by Lemma 2.2.7.

• By (3) applied to $E = \bar{L}$, we have $\sigma_L(L) = L$

$$\Rightarrow \quad b = \sigma_L(a) \in L$$

Thus L contains all roots of f, and f splits over L. □

<u>Cor 3:</u> $K \subset E \subset L$

If L/K is normal, then L/E is normal.

$$\begin{array}{ccc} & L & \\ \text{normal} & | & \text{normal} \\ & E & \\ & | & \\ & K & \end{array}$$

<u>proof</u>: Any E-linear hom. $\sigma: L \to \bar{L}$ is K-linear. Since L/K is normal, $\sigma(L) = L$ by Thm. 2. Thus L/E is normal by Thm. 2. □

Ex: (1)

$$\begin{tikzcd}[row sep=large] \mathbb{Q}(\zeta_3, \sqrt[3]{2}) \arrow[dd, dash, bend right=60, "\text{normal}"'] \arrow[d, dash, "2"', "\text{normal}"] \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "\underline{\text{not}}\ \text{normal}"] \\ \mathbb{Q} \end{tikzcd}$$

$T^3-2=(T-\sqrt[3]{2})(T^2+\sqrt[3]{2}+(\sqrt[3]{2})^2)$
does not split over $\mathbb{Q}(\sqrt[3]{2})$

(2)

$$\begin{tikzcd}[row sep=large] \mathbb{Q}(\sqrt[4]{2}) \arrow[dd, dash, bend right=60, "\underline{\text{not}}\ \text{normal}"'] \arrow[d, dash, "2"', "\text{normal}"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"', "\text{normal}"] \\ \mathbb{Q} \end{tikzcd}$$

$T^4-2=(T-\sqrt[4]{2})(T+\sqrt[4]{2})\cdot(T^2+\sqrt{2})$
does not split over $\mathbb{Q}(\sqrt[4]{2})$

Def: L/K algebraic

A <u>normal closure of L/K</u> is a splitting field L^{norm} of $\{f_a\}_{a\in L}$ together with an inclusion $L \to L^{\text{norm}}$ where f_a is the min. pol. of a over K.

Cor 4: L/K algebraic, $\bar{L}$ alg. cl. of L

Then

$$L^{\text{norm}} = \bigcap_{\substack{L\subset E\subset \bar{L}\\ E/K \text{ normal}}} E,$$

is a normal closure of L/K,

and L^{norm}/K is normal.

proof: $\cdot$ Clearly L^{norm} is contained in the splitting field $F=\{b\in\bar{L} \mid f_a(b)=0 \text{ for some } a\in L\}$ of $\{f_a\}_{a\in L}$ where $f_a = \mathrm{Mipo}_a$ are is the min. pol. of a over K.

- Conversely, q_α splits over all normal E/K if $\alpha \in L \subset E$.

  $\Rightarrow$ q_α splits over L^{norm}.

  $\Rightarrow$ $F \subset L^{norm}$

Thus $L^{norm} = F$ is a normal closure of L/K.

By Thm. 2, L^{norm}/K is normal. $\square$