Lecture 11. Splitting fields and normal extensions

$f \in k[x]$, $\deg f \geq 1$.

Def (Splitting field).

A field ext. $k \subset K$ is called a splitting field of f, if

(i) $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_i \in K$

(ii) $K = k(\alpha_1, \ldots, \alpha_n)$

Theorem: (1) For any $f \in k[x]$, $\deg f \geq 1$, there exists a splitting field K ~~for~~ of f.

(2) Let K_i, $i=1,2$ be two splitting fields of f. Then $\exists$ k-isomorphism $\sigma: K_1 \xrightarrow{\sim} K_2$.

(2)': Assume $k \subset K \subset \bar{k}^a$. K a splitting field of f.

Let K' be another splitting field of k. Then ~~any~~ $\exists$ k-embedding $K' \hookrightarrow \bar{k}^a$ and it induces an isomorphism $K' \simeq K (\subset \bar{k}^a)$

Pf: (1) Let $k \subset \bar{k}$ be an alg closure. Then over $\bar{k}[x]$

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_i \in \bar{k}.$$

Set $K = k(\alpha_1, \dots, \alpha_n)$. Then clearly

(i) over K,

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$$

$$(k[x] \subset K[x] \subset \bar{k}[x])$$

$$\begin{array}{ccccc} f & \mapsto & f & \longmapsto & f \\ & & ?\,\| & & \| \\ & & c\prod(x-\alpha_i) & \to & c\prod(x-\alpha_i) \end{array}$$

(ii) $K = k(\alpha_1, \dots, \alpha_n)$.

Therefore $k \subset K \subset k^a$ is a splitting field of f.

(2) follows from $(2)'$:

Consider:

$$\begin{tikzcd} K_1 \arrow[rr, squiggly, "\sigma"] & & \overline{K_2} = \bar{k} \\ & K_2 \arrow[ur, dash] & \\ k \arrow[uu, dash] \arrow[ur, dash] & & \end{tikzcd}$$

Check: $\overline{K_2}$, which is an alg closure of K_2, is also an algebraic closure of k.

Then by the proof of Main Thm 2 in last lecture,

we know that, $\exists$ k-embedding: $K_1 \xhookrightarrow{\sigma} \bar{k}$

Claim: $\sigma(K_1) \subset K_2 \overset{\text{EX}}{\Longrightarrow} \sigma: K_1 \xrightarrow{\sim} K_2$. (i.e. $\sigma(K_1) = K_2$)

Write: over K_1, $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_i \in K_1$,
$c \in k$

Write over K_2 (and over $\overline{K_2}=\overline{k}$),

$$f(x) = c(x-\beta_1)\cdots(x-\beta_n). \qquad \begin{array}{l} c\in k \\ \beta_i \in K_2 \ (\subset \overline{K_2}) \end{array}$$

Since σ is ~~an~~ k-embedding,

$f^\sigma = f$ (note

$\Rightarrow$ $f(x) = c(x-\sigma(\alpha_1))\cdots,(x-\sigma(\alpha_n))$

$\sigma(\alpha_i)\in\overline{k}$, $i=1\ldots n$.

By the unique factorization property for $\overline{k}[x]$,

we get $\{\sigma(\alpha_1),\ldots,\sigma(\alpha_n)\} = \{\beta_1,\ldots,\beta_n\}$.

$\Longrightarrow$ $\sigma(\alpha_i)\in K_2$. $\forall i$

$\Rightarrow$ claim

#

Let $\{f_i\}_{i\in I}$ be a family of polys in $k[x]$. A splitting field K of this family is Similarly defined. (Exercise!).

Cor: For an arbitrary family $\{f_i\}_{i\in I}$ of polynomials in $k[x]$, there exists a splitting field of this family, unique up to k-iso.

Pf: Exercise.

Thm: $k \subset K \subset \bar{k}$, TFAE

NOR 1: Every embedding of K to $\bar{k}$ induces an automorphism of K.

NOR 2: K is the splitting field of a family of polynomials in $k[x]$.

NOR 3: Every irred poly of $k[x]$ which has a root in K splits into linear factors in K.

pf: NOR 2 $\Rightarrow$ NOR 1 (Cor)

NOR 1 $\Rightarrow$ NOR 3.

Let $f(x) \in k[x]$ irred. and $\exists\, \alpha \in K$, s.t $f(\alpha) = 0$.
monic

Consider:

$$\begin{tikzcd}
K \arrow[d, dash] \arrow[r, "\tau_i"] & \bar{k} \\
k(\alpha) \arrow[d, dash] \arrow[ur, "\sigma_i"'] & \\
k \arrow[uur, "id"'] &
\end{tikzcd}$$

Let $f(x) = (x-\underset{\underset{\alpha}{\shortparallel}}{\alpha_1})(x-\alpha_2)\cdots(x-\alpha_n)$ in $\bar{k}[x]$.

It is show: $\alpha_i \in K$, $i \geq 1$.

Define k-embedding

$$\sigma_i : k(\alpha) \hookrightarrow \bar{k}$$

by $\sigma_i(\alpha) = \alpha_i$, $i \geq 1$

By the extension theorem proven in the last lecture,

$$\exists\ \tau_i : K \hookrightarrow \bar{k},\quad \tau_i|_{k(\alpha)} = \sigma_i$$

Since $\sigma_i|_k = id$, $\tau_i|_k = id$.

Thus τ_i is a k-embedding of K into $\bar{k}$.

NOR 1 $\Rightarrow$ $\tau_i : K \xrightarrow{\simeq} \tau_i(K) = K$

In particular

$$\tau_i(\alpha) = \sigma_i(\alpha) = \alpha_i \in K, \quad \forall i.$$

NOR 3 $\Rightarrow$ NOR 2

$\forall \alpha \in K$, $f_\alpha \in k[x]$ irred poly of α over k.

Then $K = k(S)$, $S = \{\alpha \in K\}$

NOR 3 $\Rightarrow$ $f_\alpha(x) = c(x - \underset{\alpha}{\underset{\shortparallel}{\alpha_0}})(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_i \in K$.

Thus K is the splitting field of the family

$\{f_\alpha\}_{\alpha \in S}$.

#

Thm: (1) Normal extensions remains normal under lifting. i.e.

$$\begin{tikzcd}[column sep=small]
 & K.F \arrow[dr, dash, "\leftarrow \text{normal}"] & \\
K \arrow[ur, dash] \arrow[dr, dash, "\text{normal}"'] & & F \arrow[dl, dash, "\text{any ext}"] \\
 & k &
\end{tikzcd}$$

, $K, F \subset L$.

(2) $\left.\begin{matrix} K \\ | \\ E \\ | \\ k \end{matrix}\right\}$ normal $\Rightarrow$ $\begin{matrix} K \\ | \\ E \end{matrix} \leftarrow$ normal $\left(\text{But } \begin{matrix} E \\ | \\ k \end{matrix} \text{ not nece. normal!} \right)$

(3)

$$\begin{tikzcd} & L \arrow[d, dash] & \\ & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash, "\text{norm}"'] & & K_2 \arrow[dl, dash, "\text{nml}"] \\ & k & \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} K_1K_2 \arrow[d, dash] \\ K_1 \cap K_2 \arrow[d, dash] \\ k \end{tikzcd}$$

normal

normal

Pf: (1) K / k normal $\Rightarrow \exists \{f_i\}_{i \in I}$, $f_i \in k[x]$

s.t. (1) $f_i = c_i \prod (x - \alpha_{ij})$ $\quad \alpha_{ij} \in K$

(2) $K = k(\alpha_{ij} \cdots)$

Then $K \cdot F / F$ is the splitting field of family

$\{f_i(x)\}_{i \in I}$, $f_i \in k[x] \subset F[x]$.

Thus NOR 2 is satisfied for $K \cdot F / F$, hence it is normal.

(2) Fix $\begin{matrix} \bar{k} \\ | \\ K \\ | \\ E \\ | \\ k \end{matrix}$. K/k normal $\overset{\text{NOR 1}}{\Rightarrow}$ $\forall$ k-embedding of K into $\bar{k}$ induces auto of K.

$\Rightarrow$ $\forall$ E-embedding of K into $\bar{k}$ induces auto of K $\Rightarrow$ K/E normal.

(3) Fix

$$\begin{tikzcd}[column sep=small]
 & \bar{k} \arrow[d, dash] & \\
 & L \arrow[d, dash] & \\
 & K_1 K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[r, dash] \arrow[dr, dash] & K_1 \cap K_2 \arrow[r, dash] \arrow[d, dash] & K_2 \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

$\sigma : \cancel{K_1} \cdot K_2 \longrightarrow \bar{k}$ is a k-embedding

Note. $\sigma(K_1 \cdot K_2) \underset{\text{check!}}{=} \sigma(K_1) \cdot \sigma(K_2) \overset{\text{NOR 1}}{=} K_1 \cdot K_2$

$\overset{\text{NOR1}}{\Longrightarrow} K_1 K_2 / k$ normal

Similarly, $\tau : K_1 \cap K_2 \longrightarrow \bar{k}$ k-embedding, $\exists \sigma : K_1 K_2 \hookrightarrow \bar{k}$ extends τ

$\tau(K_1 \cap K_2) = \sigma(K_1 \cap K_2) \overset{\text{check!}}{=} \sigma(K_1) \cap \sigma(K_2) \overset{\text{NOR 1}}{=} K_1 \cap K_2$

$\ulcorner$ $\subset$: obvious

$\supset$: $\sigma^{-1}(\sigma(K_1) \cap \sigma(K_2)) \subset \sigma^{-1}(\sigma(K_1)) \cap \sigma^{-1}(\sigma(K_2)) = K_1 \cap K_2$,

where $\sigma^{-1} : \sigma(K_1 K_2) \xrightarrow{\sim} K_1 K_2$ $\lrcorner$

Thus, $K_1 \cap K_2 / k$ is normal

#

Warning: (normal extension do not form a distinguished class)

(1)
$$\begin{tikzcd} \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "\leftarrow \text{normal}"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "\leftarrow \text{normal}"] \\ \mathbb{Q} \end{tikzcd} \qquad \text{But} \qquad \begin{tikzcd} \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \quad \underline{\text{not normal}} \;!!!$$

(2)
$$\begin{tikzcd} \mathbb{Q}(\sqrt[4]{2}, i) \arrow[d, dash, "\leftarrow \text{normal}"] \arrow[dd, dash, bend right, "\text{normal}"'] \\ \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "\leftarrow \underline{\text{not normal}\;!!!}"] \\ \mathbb{Q} \end{tikzcd}$$

Ex: Determine $Gal(\mathbb{Q}(\sqrt[4]{2}, i) \mid \mathbb{Q})$

$\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

$$f(x) = (x - \underbrace{\sqrt[4]{2}}_{=\alpha_1})(x - \underbrace{\sqrt[4]{2}\, i}_{=\alpha_2})\underbrace{(x + \sqrt[4]{2})}_{= x - \underbrace{(-\sqrt[4]{2})}_{=\alpha_3}}\underbrace{(x + \sqrt[4]{2}\, i)}_{= x - \underbrace{(-\sqrt[4]{2}\, i)}_{=\alpha_4}}$$

Note: $Gal(\mathbb{Q}(\sqrt[4]{2}, i)) \times \underset{\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}}{\overset{\Downarrow}{X}} \longrightarrow \underset{\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}}{\overset{\|}{X}}$

is a <u>group action</u>. (check this !!!)

Thus:

$$\underset{G}{\underbrace{\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)\,|\,\mathbb{Q})}} \hookrightarrow S_4 = \mathrm{Perm}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

Note: $\sigma \in G$ is determined by its image

$$\sigma(\sqrt[4]{2}) \text{ and } \sigma(\sqrt[4]{2}\, i) = \sigma(\sqrt[4]{2}) \cdot \sigma(i)$$

and $\sigma(i)$ can take the possible values $\{i, -i\}$

	$\sqrt[4]{2} = \alpha_1$	$\sqrt[4]{2}\, i = \alpha_2$	$-\sqrt[4]{2} = \alpha_3$	$-\sqrt[4]{2}\, i = \alpha_4$	i
$id = \sigma_1$	α_1	α_2	α_3	α_4	i
$[1234] = \sigma_2$	α_2	α_3	α_4	α_1	i
$[12][34] = \sigma_3$	α_2	α_1	α_4	α_3	$-i$
$[13][24] = \sigma_4$	α_3	α_4	α_1	α_2	i
$[13] = \sigma_5$	α_3	α_2	α_1	α_4	$-i$
$[24] = \sigma_6$	α_1	α_4	α_3	α_2	$-i$
$[1432] = \sigma_7$	α_4	α_1	α_2	α_3	i
$[14][23] = \sigma_8$	α_4	α_3	α_2	α_1	$-i$

$\mathbb{Q}(\sqrt[4]{2}, i)$

2 | 4 normal

$\mathbb{Q}(\sqrt[4]{2})$ $\mathbb{Q}(i)$

4 | 2 normal

$\mathbb{Q}$

<u>check</u>: they are automorphisms. !!!

$$G = \langle \sigma_2, \sigma_6 \rangle \simeq D_4$$

Def: (normal closure)

For $k \subset K \subset \bar{k}$, the normal closure K^n of K over k

is the smallest normal ext over k which contains K; (if it exists)

Prop: For $k \subset K \subset \bar{k}$, K^n exists and it is equal to

the compositum of all k-embeddings of K into $\bar{k}$.

pf: put $K^n = \bigcap_{\substack{\bar{k} \supset E \supset k \\ E|k \text{ normal}}} E$.

Then, it is clear that $K^n | k$ normal (check this!)

Now we show that

$$K^n = \prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ k}} \overbrace{\sigma(K)}^{K^\sigma}$$

$$\begin{tikzcd} K^n \arrow[r, "\tau"] & \bar{k} \\ K \arrow[u, dash] \arrow[ur, "\sigma"'] & \\ k \arrow[u, dash] \arrow[uur] & \end{tikzcd}$$

$\forall \sigma \in K \hookrightarrow \bar{k}$, $\exists$ ext $\tau : K^n \hookrightarrow \bar{k}$

$K^n | k$ normal $\Rightarrow \tau(K^n) \subset K^n$

$\Rightarrow \tau(K) = \sigma(K) \subset K^n$.

$$\Rightarrow \prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ k}} \sigma(K) \subset K^n.$$

it remains to show

$$\prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ \vee \\ k}} \sigma(K) \qquad \text{normal}$$

But this is clear:

$$\forall\ \tau : \prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ \vee \\ k}} \sigma(K) \longrightarrow \bar{k}$$
$$\diagdown \quad \diagup$$
$$k$$

$\forall \sigma : K \hookrightarrow \bar{k}$,

$\tau\sigma$: is again a k-embedding of K into $\bar{k}$.

Thus: $$\tau\Big(\prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ \vee \\ k}} \sigma(K)\Big) = \prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ \vee \\ k}} \tau\sigma(K)$$

$$= \prod_{\substack{\sigma : K \hookrightarrow \bar{k} \\ \vee \\ k}} \sigma(K)$$

#

Lecture 12 Seperable extensions

Def: (Seperable polynomial)

$f(x) \in k[x]$ is seporable if it has no multiple roots.

Prop: $f(x) \in k[x]$ ~~irreducible~~. It is seperable iff

$$(f(x), f'(x)) = k[x].$$

Pf: W.L.o.G. assume $f(x)$ monic. Note $f'(x) \in k[x]$.

~~($\Rightarrow$)~~ over $\bar{k}[x]$,

$$f(x) = \prod_i (x - x_i)^{r_i}, \quad x_i \neq x_j, \quad x_i \in \bar{k}, \quad r_i \geq 1$$

$$f'(x) = \sum_i r_i (x - x_i)^{r_i - 1} \prod_{j \neq i} (x - x_j)^{r_j}$$

Now: If $f(x)$ is seperable, then $r_i = 1$, $\forall i$.

$$\Rightarrow f'(x_i) = \prod_{j \neq i} (x_i - x_j) \neq 0 \quad \forall i$$

$\Rightarrow$ over $\bar{k}[x]$,

$$GCD(f(x), f'(x)) = 1 \iff (f(x), f'(x)) = \bar{k}[x]$$

$\Rightarrow$ over $k[x]$, $(f(x), f'(x)) = k[x]$ (why?)

Conversely,

assume $(f(x), f'(x)) = k[x]$.

Then $\exists\ a(x), b(x) \in k[x]$, s.t

$$a(x)\cdot f(x) + b(x)\, f'(x) = 1 \qquad (*)$$

~~If~~ $f(x)$ is NOT separable, then $\exists\ r_i \geq 2$.

Then

$$f'(x_i) = \sum_{l \neq i} \Big[r_l (x_i - x_l)^{r_l - 1} \overbrace{\prod_{j \neq l} (x_i - x_j)^{r_j}}^{=0} \Big]$$

$$+ \ r_i \underbrace{(x_i - x_i)}_{=0}{}^{r_i - 1} \prod_{j \neq i} (x_i - x_j)^{r_j}$$

$$= 0.$$

Thus $\underbrace{a(x_i) \overbrace{f(x_i)}^{0} + b(x_i)\cdot \overbrace{f'(x_i)}^{0}}_{=0} \overset{(*)}{=} 1$.

Contradiction!

#

Cor: Char $k = 0$.

$f(x) \in k[X]$, irreducible poly

Then $f(x)$ is separable.

Pf: If char $k = 0$, then

$$\deg f'(x) = \deg f(x) - 1 < \deg f(x)$$

Since $f(x)$ irred . $(f(x))$ maximal

But $(f(x), f'(x)) \supsetneq (f(x))$ $\Bigg\} \Rightarrow$

$$(f(x), f'(x)) = k[X] \xRightarrow{\text{Prop}} f(x) \text{ separable}$$

Example: $k = \mathbb{F}_p(t)$, $f(x) = x^p - t \in k[x]$.

Then $f(x)$ is irreducible, but NOT separable.

Exercise: check $f(x) \in k[X]$ irreducible polynomial.

Def: $K|k$ alg ext. ~~is called separable, if~~:

$\alpha \in K$ is a separable elt over k if $f_\alpha \in k[X]$ is separable

poly. $\cancel{K}$

$K|k$ is called <u>seperable ext</u>, if any $\alpha \in K$ is seperable over k.

<u>Theoren: char $k=0$. Then any algebraic ext</u>

<u>$K|k$ is seperable.</u>

<u>Example</u>: $k = \mathbb{F}_p(t)$, $K = \dfrac{\mathbb{F}_p(t)[x]}{(x^p - t)}$ $(= \mathbb{F}_p(t^{1/p}))$

$K|k$ is inseperable. extension.

<u>Theorem</u>: <u>Seperable extensions form a distinguished class.</u>

Coro $K|k$ algebraic. There exists a <u>maximal seperable subext</u>

$k \subset k^s \subset K$. i.e. $\forall k \subset F \subset K$, $F|k$ sep $\Rightarrow F \subset k^s$.

pf: Define $k^s = k(\alpha \mid \alpha \in K$, seperable over $k)$.

which the compositum of $\{k(\alpha)\}_{\alpha \text{ sep}}$ in K.

By Theorem, $k^s | k$ is again seperable.

clearly, it is the maximal subext, which is sep over k

#

Pf of Theorem :

(1)
$$\begin{tikzcd} E \arrow[d, dash, "\leftarrow \text{sep}"] \\ F \arrow[d, dash, "\leftarrow \text{sep}"] \\ k \end{tikzcd} \iff \begin{tikzcd} E \arrow[d, dash, "\leftarrow \text{sep.}"] \\ k \end{tikzcd}$$

($\Leftarrow$) trivial.

($\Rightarrow$). $\alpha \in E$. $\left(f_\alpha \in k[x] \text{ irred poly. of } \alpha \text{ over } k\right)$

Let $f_\alpha^F(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ be the irred. poly of α over F.

Let $F_0 = k(a_0, \ldots a_n) \subset F$. Consider

$$\begin{tikzcd} & & E \arrow[dd, dash, "\text{sep.}"] \\ k(\alpha) \arrow[urr, dash] \arrow[dd, dash] & & \\ & & F \arrow[dd, dash, "\text{sep}"] \\ k(a_0, \ldots a_n) = F_0 \arrow[urr, dash] \arrow[drr, dash, "\text{Sep.}"'] & & \\ & & k \end{tikzcd}$$

Note: $f_\alpha^F \in F_0[x]$, and it is irreducible. over $F_0[x]$.,

~~The irreducible~~ as it is irreducible over $F[x]$.

Thus, ~~α~~ f_α^F is the irreducible poly of α over F_0.

Thus, Since α is separable over F, α is also separable over F_0.

Thus, we reduce ~~to~~ the ~~following~~ situation

$$\begin{array}{c} E \\ \big| \text{ finite sep} \\ F \\ \big| \text{ finite sep} \\ k \end{array} \quad \overset{?}{\Rightarrow} \quad \begin{array}{c} E \\ \big| \text{ sep.} \\ k \end{array}$$

To achieve this, we use the following criterion for finite separable extension

Prop: $\begin{array}{c} E \\ | \\ k \end{array}$ finite extension. Then it is separable if and only if the $\underbrace{\text{number of } k\text{-embeddings of } E \text{ into } \overline{k}}_{\substack{\parallel \\ [E:k]_s}}$ is equal to $[E:k]$.

(separable degree)

Pf: If $E = k(\alpha)$, then we know that

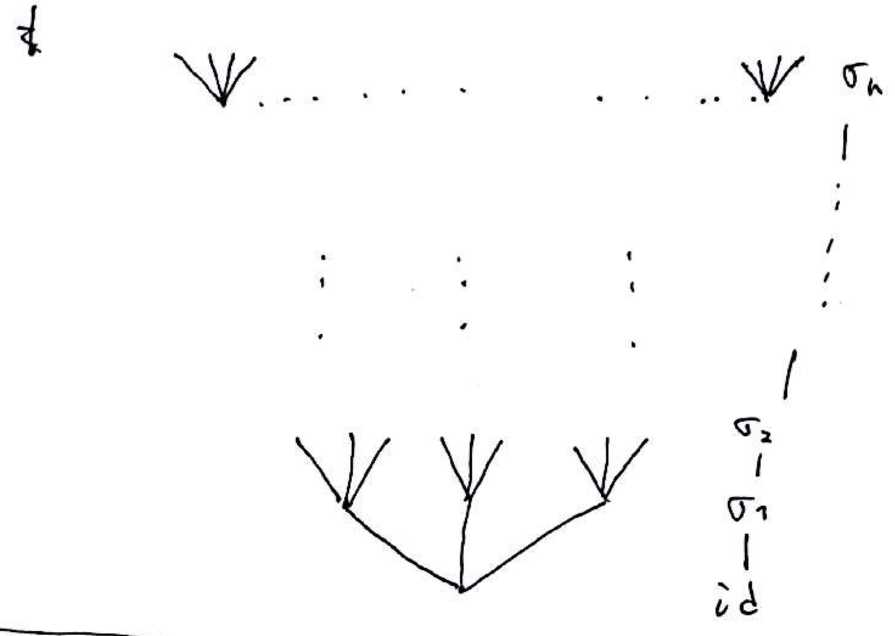
$$\#\left\{k(\alpha) \hookrightarrow \overline{k}\right\} = \#\{\text{distinct roots of } f_\alpha\}$$

$$\le \#\{\text{roots of } f_\alpha\} = \deg f_\alpha = [k(\alpha):k]$$

Thus, the prop is clear for simple ext.

In general, we take a tower of simple extensions:

$$
\begin{array}{c}
E = E_n \stackrel{\Delta}{=} k(\alpha_1, \dots \alpha_n) \\
| \\
E_{n-1} \stackrel{\Delta}{=} k(\alpha_1 \dots \alpha_{n-1}) \\
\vdots \\
E_1 \stackrel{\Delta}{=} k(\alpha_1) \\
| \\
k
\end{array}
$$



Or, we consider first the case

Tree like picture

$$
\begin{array}{c}
k(\alpha_1, \alpha_2) \\
| \\
k(\alpha_1) \\
| \\
k \hookrightarrow \bar{k}
\end{array}
$$

claim:

$$\#\{k\text{-embeddings of } k(\alpha_1,\alpha_2) \hookrightarrow \bar{k}\} = \#\{k\text{-embeddings of } k(\alpha_1) \hookrightarrow \bar{k}\} \cdot \#\{k(\alpha_1)\text{-embeddings of } k(\alpha_1,\alpha_2) \hookrightarrow \bar{k}\}.$$

$$\#\{k\text{-embeddings of } k(\alpha_1,\alpha_2) \hookrightarrow \bar{k}\} \stackrel{\Delta}{=} [k(\alpha_1,\alpha_2) : k]_s$$

$$\#\{k\text{-embeddings of } k(\alpha_1) \hookrightarrow \bar{k}\} \stackrel{\Delta}{=} [k(\alpha_1) : k]_s$$

$$\#\{k(\alpha_1)\text{-embeddings of } k(\alpha_1,\alpha_2) \hookrightarrow \bar{k}\} = [k(\alpha_1,\alpha_2) : k(\alpha_1)]_s$$

why ?

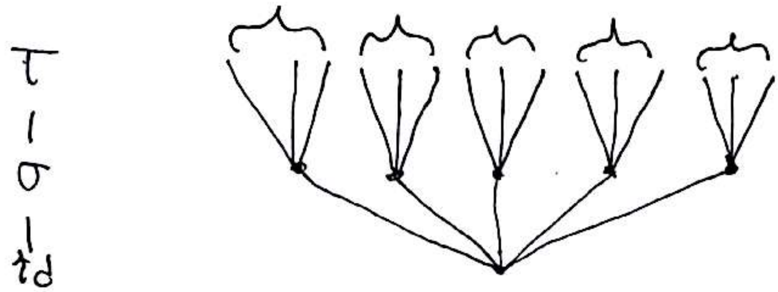
$$\tau : k(\alpha_1, \alpha_2) \hookrightarrow \bar{k},$$

put $\tau|_{k(\alpha_1)} = \sigma : k(\alpha_1) \hookrightarrow \bar{k}$. Then τ extends σ

Fix $\sigma : k(\alpha_1) \hookrightarrow \bar{k}$, there are $\#\{k(\alpha_1)\text{- embeddings of } k(\alpha_1,\alpha_2) \hookrightarrow \bar{k}\}$ extensions of σ (Show this !)

~~But,~~ Moreover, there are $\#\{k\text{-embeddings of } k(\alpha_1) \hookrightarrow \bar{k}\}$ of σ in total.

The claim follows. The picture looks as follows :



By induction: we get in general

$$[E:k]_s = \prod_{i=1}^{n} [E_i : E_{i-1}]_s , \qquad E_0 = k$$

or in general:

$$\begin{array}{l} E \\ \mid \leftarrow \text{finite} \\ F \\ \mid \leftarrow \text{finite} \\ k \end{array} \qquad [E:k]_s = [E:F]_s \cdot [F:k]_s$$

Since $E_i \mid E_{i-1}$ is simple extension, let $f_{\alpha_i}^{E_{i-1}}$ be the minimal of α_i over E_{i-1}, it follows that

$$[E_i : E_{i-1}]_s = \# \{\text{distinct roots of } f_{\alpha_i}^{E_{i-1}}\}$$

$$\leq \deg f_{\alpha_i}^{E_{i-1}} = [E_i : E_{i-1}]$$

Thus $[E : k]_s = \prod [E_i : E_{i-1}]_s \leq \prod [E_i : E_{i-1}] = [E : k]$

"=" holds $\Leftrightarrow \forall i: \ [E_i : E_{i-1}]_s = [E_i : E_{i-1}]$

Now: assume $E|k$ separable, $\Rightarrow$ ~~$\forall \alpha_i \in$~~ α_i is separable over k

$\Rightarrow \alpha_i$ is sepperable over E_{i-1}.

$$\Rightarrow [E_i : E_{i-1}]_s = [E_i : E_{i-1}]$$

$$\Rightarrow [E : k]_s = [E : k].$$

Conversely, $[E : k]_s = [E : k]$. Take any $\alpha \in E$.

If α were not separable over k. Then

$$[k(\alpha) : k]_s \lneq [k(\alpha) : k]$$

But $[E : k]_s = [E : k(\alpha)]_s \cdot [k(\alpha) : k]_s$

$< [E : k(\alpha)] \cdot [k(\alpha) : k] = [E : k]$ $\lightning$.

Thus, any $\alpha \in E$ is separable over k.

#.

(2):
$$\begin{tikzcd}
& EF \arrow[dl, dash] \arrow[dr, dash, "sep"] & \\
E \arrow[dr, dash, "sep"'] & & F \arrow[dl, dash, "*"] \\
& k &
\end{tikzcd}$$
, Separable ext ~~is~~ remains separable under lifting:

This is clear: since $E = k(\alpha \mid \alpha \in E)$,

$$EF = F(\alpha \mid \alpha \in E)$$

The irred. poly of α over F is ~~x~~ a factor of the irred poly of α over k.

Thus, α is sep over $k \Rightarrow \alpha$ is sep over F.

#

To conclude this ~~lecture~~, we summarize the above two lectures as follows:

~~E~~ $k \subset K \subset \bar{k}$.

(1) $\begin{matrix} K \\ | \\ k \end{matrix}$ normal $\Leftrightarrow \underset{\text{the normal closure of } K \text{ over } k.}{\overset{}{K^n}} = K$ (~~in gene~~

~~k~~

$K|k$ non-normal $\iff$ $K^n \supsetneq K \supset k$

(2) $\begin{array}{c} K \\ | \\ k \end{array}$ sep $\iff$ $K^s = K$

K^s: the maxial sep. subext.

$K|k$ non-separable $\iff$ $K \supsetneq K^s \supset k$

(3) $K|k$ arbitrary ext. Then

$$\begin{tikzcd}[column sep=small]
 & & K^n \arrow[d, dash, "\text{normal + separable}"] \\
K \arrow[urr, dash] \arrow[drr, dash] & & (K^n)^s \arrow[d, dash] \\
 & & k
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
K \arrow[d, dash] & \\
 & (K^s)^n \\
K^s \arrow[ur, dash] \arrow[d, dash] & \\
k \arrow[uur, dash, "\text{normal + separable}"'] &
\end{tikzcd}$$

(Show this!)

Theorem (Primitive Element Theorem)

Let E/k be a finite extension. Then $E = k(\alpha)$, for some $\alpha \in E$ if and only if there exists only a finite number of fields F such that $k \subset F \subset E$. If E is separable over k, then there exists such an elt α.

Pf: Step 1. $|k| < +\infty$. i.e. k is a finite field.

Then E^* is cyclic (why?) then $\exists\, \xi \in E$

s.t $E^* = k(\xi)$ and therefore $E = k(\xi)$

Step 2. $|k| = +\infty$.

($\Rightarrow$) Assume $\exists$ only finitely many intermediate fields

Take any $\alpha, \beta \in E$. Consider

$$k(\alpha + c\beta). \quad c \in k$$

$\Rightarrow \exists\, c_1 \neq c_2 \in k$, s.t

$$k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$$

$\Rightarrow (c_1 - c_2)\beta \in k(\alpha + c_1\beta) \Rightarrow \beta \in k(\alpha + c_1\beta)$

$\Rightarrow \alpha \in k(\alpha + c_1\beta)$

Thus $k(\alpha, \beta) = k(\alpha + c_1\beta)$, for some $c \in k$

Proceed inductively. Since $E|k$ finite. $\exists\, \alpha_1, \dots \alpha_n \in E$

s.t $E = k(\alpha_1, \dots \alpha_n)$

Now, $\exists\, c_2, \dots c_n \in k$, s.t

$$E = k(\xi), \quad \xi = \alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n$$

($\Leftarrow$) Assume $E = k(\alpha)$.

Let $k \subset F \subset E = k(\alpha)$

set $f_\alpha^F \in F[X]$ be the irred of α over F.

Get a map

$$\begin{array}{ccc} \{F \mid k \subset F \subset E\} & \xrightarrow{\phi} & E[X] \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ F & \longmapsto & f_\alpha^F \end{array}$$

Note: $\forall F$, $f_\alpha^F \mid f_\alpha$

$\Rightarrow |\mathrm{Im}(\phi)| < +\infty$.

Claim: ϕ is injective.

That is F is uniquely determined by f_α^F

Let $F_0 = k(a_i, 0 \leq i \leq \deg f_\alpha^F)$ be the

subfield of E generated by the coeff. of f_α^F.

Note $f_\alpha^F \in F[X]$

Thus $k \subset F_0 \subset F \subset E$.

$f_\alpha^F \in F_0[X]$ is irred, as $f_\alpha^F \in F[X]$ irreducible.

Thus $f_\alpha^{F_0} = f_\alpha^F$.

Now $\underset{\underset{\deg f_\alpha^{F_0}}{\parallel}}{[E : F_0]} = \underset{\underset{\deg f_\alpha^F}{\parallel}}{[E : F]}[F : F_0]$ $\Rightarrow [F : F_0] = 1$

$\Rightarrow F = F_0$.

Thus F is uniquely determined by f_α^F. (✱).

Therefore $|\{F \mid k \subset F \subset E\}| < +\infty$.

Step 3: $|k| = +\infty$, and E/k separable, finite. ~~WLOG~~

Let $\{\sigma_i \ 1 \leq i \leq n\}$ be the distinct k-embedding to $\bar{k}$,

where $n = [E : k]$.

WLOG. $E = k(\alpha, \beta)$ (in general, by induction).

Claim: $\exists\ c \in k$, s.t $k(\alpha, \beta) = k(\alpha + c\beta)$.

For this, consider the polynomial

$$P(x) = \prod_{i \neq j} (\sigma_i \alpha + \sigma_i \beta \cdot x - \sigma_j \alpha - \sigma_j \beta \cdot x)$$

Note $P(x) \neq 0$.

Since $|k| = +\infty$, $\exists\ c \in k$, s.t

$$P(c) \neq 0.$$

Thus, $\sigma_i(\alpha + c\beta) = \sigma_i \alpha + c \sigma_i \beta \neq \sigma_j \alpha + c \sigma_j \beta$

$= \sigma_j(\alpha + c\beta)$, $i \neq j$

$$\left.\begin{array}{ll} \text{Hence} & [k(\alpha + c\beta) : k] \geq n \\ \text{But} & [k(\alpha+c\beta) : k] \leq [E : k] = n \end{array}\right\} \Rightarrow$$

$$E = k(\alpha + c\beta).$$

#