$F \subset E$ fields.

- F is a subfield of E

  That is F is closed under $(+, -, \times, \div)$

- E is a field extension of F

We can view E as a vector space over F.

$[E:F] \triangleq \dim_F E$.

If $[E:F] < +\infty$, then E is a finite ext. of F.

otherwise, infinite ext.

Pick $\alpha \in E$. Consider the can. morphism

$$\begin{array}{ccc} F[X] & \xrightarrow{\phi_\alpha \,=\, ev_\alpha} & E \\ \downarrow & & \downarrow \\ \sum_i a_i x^i & \longmapsto & \sum_i a_i \alpha^i \end{array}$$

ϕ_α is the evaluation map at α.

- ϕ_α is a ring homomorphism.
- ϕ_α is also F- vector space hom-morphism.

$\ker(\phi_\alpha) = (f_\alpha) \subseteq F[x]$

f_α monic. Since $\frac{F[x]}{(f_\alpha)} \simeq \text{im}(\phi_\alpha) = F[\alpha] \subseteq E$ (Subring)

$\overset{\text{Ex}}{\Rightarrow}$ (f_α) prime ideal.

Case 1. $f_\alpha = 0$. (i.e $\deg f_\alpha = -\infty$)

In this case, we call α is "transcendental" over F.

Case 2. f_α irreducible (i.e $\deg f_\alpha \neq 0$)

In this case, we call α "algebraic" over F.

The poly. f_α is called the <u>irreducible poly. of α over F</u>.

Note that: $F[\alpha] \subseteq E$ is a subfield!

Example: $\mathbb{Q} \subset \mathbb{C}$

- $\alpha = \pi, e, \ldots$ transcendal over $\mathbb{Q}$.
- $\alpha = \sqrt{2}, \sqrt{-1}, \ldots$ algbraic over $\mathbb{Q}$.

The irre. poly of $\sqrt{2}$ over $\mathbb{Q}$. : $x^2 - 2 \in \mathbb{Q}[x]$

- - - of $\sqrt{-1}$ - - : $x^2 + 1 \in \mathbb{Q}[x]$

An ext $F \subset E$ is called algebraic if

$\forall \alpha \in E$, α is algebraic over F.

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \in \mathbb{C}$

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$\mathbb{Q}(\sqrt{2})$ is algebraic ext of $\mathbb{Q}$:

For $\alpha = a+b\sqrt{2}$:

$b=0, \Rightarrow f_\alpha := x-a$ irred poly

$b \neq 0 \Rightarrow f_\alpha = (x-a)^2 - 2b$ irred poly

Prop: $F \subset E$ finite ext. Then E is alg over F.

pf: Pick any $\alpha \in E$

Consider the subset

$$\{1, \alpha, \alpha^2, \cdots \alpha^n, \cdots\} \subseteq E$$

Since $\dim_F E < +\infty$, it follows that, $\exists\, n \in \mathbb{N}$,

s.t

$\{1, \alpha \dots, \alpha^n\}$ linearly dependent

ie, $\exists\ a_i \in F$, not all zero, s.t

$$\sum_{i=0}^{n} a_i \cdot \alpha^i = 0$$

Thus $f(x) = \sum_{i=0}^{n} a_i \cdot x^i \in \ker(\phi_\alpha) \neq 0$ $\neq 0$

Thus α is algebraic over F. #

But: E alg $F \not\Rightarrow E$ finite over F.

Ex: $\overline{\mathbb{Q}} \triangleq \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$

Claim 1: $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

It is clear that $0 \neq \alpha \in \overline{\mathbb{Q}}$, then

(i). $-\alpha \in \overline{\mathbb{Q}}$

(ii) $\alpha^{-1} \in \overline{\mathbb{Q}}$

It suffices to show: $\alpha, \beta \in \overline{\mathbb{Q}}$, $\alpha+\beta, \alpha\cdot\beta \in \overline{\mathbb{Q}}$.

For this, consider the tower

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\alpha,\beta)$$

Note $\alpha \in \overline{\mathbb{Q}} \Rightarrow \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) < +\infty$

$= \deg(f_\alpha)$ ← Ex!

$\beta \in \overline{\mathbb{Q}} \Rightarrow$ the irred poly of β over $\mathbb{Q}$

$$f_\beta \in \mathbb{Q}[X],\ 0 \le \deg f_\beta < +\infty$$

But $f_\beta \in \mathbb{Q}(\alpha)[X]$, and $f_\beta(\beta) = 0$

Thus for $\mathbb{Q}(\alpha)[X] \xrightarrow{\Psi_\beta} \mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\alpha,\beta)$.

$\ker(\Psi_\beta) \neq 0$ (as $f_\beta \in \ker(\Psi_\beta)$)

Thus $\dim_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha,\beta) < +\infty$ ← Ex.

$(\le \deg f_\beta)$

It follows from the next prop. that

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty.$$

Thus $\mathbb{Q}[\alpha, \beta)$ is alg over $\mathbb{Q}$

Since $\alpha+\beta,\ \alpha, \beta \in \mathbb{Q}(\alpha, \beta)$, they are alg over $\mathbb{Q}$.

#

Claim 2: $\dim_{\mathbb{Q}} \overline{\mathbb{Q}} = +\infty$.

Consider the irred. poly

$$x^n - 2 \in \mathbb{Q}[x]$$

Let $\alpha_n \in \mathbb{C}$ be a solution of

$$x^n - 2 = 0. \quad (\text{Thus } f_{\alpha_n} = x^n - 2$$

Then $\mathbb{Q} \subset \mathbb{Q}(\alpha_n) \subset \overline{\mathbb{Q}} \subset \mathbb{C}$

$$\dim_{\mathbb{Q}} \overline{\mathbb{Q}} \geq \dim_{\mathbb{Q}} \mathbb{Q}(\alpha_n) = \deg f_{\alpha_n} = n \to \infty.$$

#.

A tower of fields is a sequence of field extensions.

$$F_1 \subset F_2 \subset \cdots \subset F_n$$

Prop: $F_1 \subset F_2 \subset F_3$. Then $[F_3 : F_1] = [F_3 : F_2] \cdot [F_2 : F_1]$.

Pf: Show: $\{x_i\}_{i\in I}$ a basis of F_2 over F_1

$\{y_j\}_{j\in J}$ - - - F_3 over F_2

Then $\{x_i \cdot y_j\}_{\substack{i\in I \\ j\in J}}$ - - - of F_3 over F_1.

It is clear that $\{x_i y_j\}$ spans F_3.

Assume $\sum a_{ij}\, x_i \cdot y_j = 0$. for a. a. $a_{ij} = 0$,

$a_{ij} \in F_1$

$$\sum_j \Big(\sum_i a_{ij} \cdot x_i\Big) y_j$$

$\forall i,\ x_i \in F_2. \Rightarrow \sum_i a_{ij} \cdot x_i \in F_2$

$\{y_j\}$ F_2-basis $\Rightarrow$ $\sum_i a_{ij} \cdot x_i = 0, \ \forall j.$

$\{x_i\}$ F_1-basis $\Rightarrow$ $a_{ij} = 0. \ \forall i.$

#

Cor: $F_1 \subseteq F_2 \subseteq F_3$. F_3 finite over F_1

$\Leftrightarrow$ F_3 finite over F_2 and F_2 is finite over F_1.

$k \subset E$

Take $\{\alpha_1 \dots \alpha_n\} \subset E$

$k(\alpha_1, \dots \alpha_n) \subset E$

$\|\Delta$

the smallest subfield containing k and $\alpha_1 \dots \alpha_n$

$\|$ check!

$$\left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots \alpha_n)} \;\middle|\; f, g \in k[x_1, \dots, x_n],\ g(\alpha_1, \dots \alpha_n) \neq 0 \right\}$$

(~~$k(x_1, \dots, x_n)$~~)

Def: A field E is called finitely generated over k, if

$\exists\ \alpha_1, \dots \alpha_n \in E$, s.t

$$E = k(\alpha_1, \dots, \alpha_n)$$

Prop: E/k finite $\Rightarrow$ E/k finitely generated.

pf: Take any k-basis $\{\alpha_1 \dots \alpha_n\}$ of E

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

#

Def (Compositum)

$E, F \subset L$, $E.F \subset L$ is defined to be

Smallest subfield containing E and F.

clearly, if $k \subset E \cap F \overset{\text{subfield}}{\subset} L$.

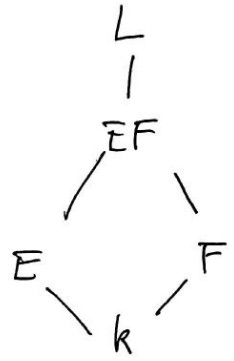
and $E = k(\alpha_1, \ldots \alpha_n)$ for some $\{\alpha_1 \ldots \alpha_n\} \subset E$.

then $E \cdot F = F(\alpha_1, \ldots \alpha_n)$ and thus $E.F/F$ is f.g

[Symmetrically, $F = k(\beta_1, \ldots \beta_m)$

$E \cdot F = E\{\beta_1, \ldots, \beta_m\}$]

Picture:



Prop: $E = k(\alpha_1, \ldots \alpha_n) \subset L$. assume $\forall i$, α_i is algebraic over k. Then E/k is finite (hence algebraic)

pf: use the tower

$$k \subset k(\alpha_1) \subset \underset{\| \\ k(\alpha_1)(\alpha_2)}{k(\alpha_1,\alpha_2)} \subset \cdots \subset k(\alpha_1 \cdots \alpha_{n-1}) \subset \underset{\| \\ k(\alpha_1 \cdots \alpha_{n-1})(\alpha_n)}{k(\alpha_1 \cdots \alpha_n)}$$

Put $k_i = k(\alpha_1 \cdots \alpha_i)$

Then α_{i+1} algebraic over k

$\Rightarrow \alpha_{i+1}$ algebraic over k_i

$\Rightarrow [k_{i+1} : k_i] = [k_i(\alpha_{i+1}) : k_i] \leq [k(\alpha_{i+1}) : k] < +\infty$

$\Rightarrow [k_n : k] = \pi [k_{i+1} : k_i] < +\infty.$ #

$\mathcal{C}$ = certain class of extension fields $F \subset E$.

$\mathcal{C}$ is distinguished if it satisfies the following

(1) $k \subset F \subset \bar{E}$.

$(k \subset E) \in \mathcal{C} \iff (k \subset F) \in \mathcal{C}$ and $(F \subset \bar{E}) \in \mathcal{C}$

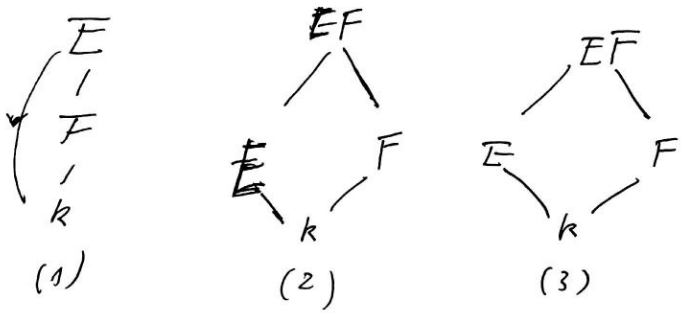
(2) $(k \subset \bar{E}) \in \mathcal{C}$. F/k any ext, $E, F \subset L$

then $(F \subset EF) \in \mathcal{C}$.

(3) $k \subset F$, $k \subset E$ $\in \mathcal{C}$.

$E, F \subset L$. Then $(k \subset FE) \in \mathcal{C}$.

Pictures:



(1)+(2) $\Rightarrow$ (3)

Prop: The class of algebraic extensions is distinguished.

So is the class of finite extensions.

pf: For finite extension, this is the consequence of the above results. To algebraic ext:

(1): E/F alg, F/k alg $\Rightarrow E/k$ alg.

$\alpha \in E$, $f_\alpha \in F[X]$ the irred. poly of α over F.

$$X^n + \sum_{i=n-1} a_i X^i.$$

Take ~~k~~ $k(\alpha, a_0 \cdots a_{n-1}) \subset E$

ϕ ϕ

$k(a_0, \cdots a_{n-1}) \subset F$

ϕ ϕ

k $=$ k

$a_i \in F$ alg over k, $\forall i$

$\Rightarrow k(a_0, \cdots a_{n-1})/k$ finite

$\Rightarrow k(\alpha, a_0, \cdots a_{n-1})/k$ finite

$\Rightarrow \alpha/k$ alg.

(2) E/k alg $\Rightarrow EF/F$ alg.

$$EF = \bigcup_{\alpha \in E} F(\alpha)$$

α/k alg $\Rightarrow$ α/F alg, since $k \subset F$. #

Lecture 10. Algebraic Closure

$F \subset E$ field extension

Then $\iota : F \longrightarrow \bar{E}$ the inclusion map is an inj.

field homo. (field embedding)

But there are other inj. field homo.:

$\mathbb{Q}(\sqrt{2}) \xhookrightarrow{\iota} \bar{\mathbb{Q}}$ $\sqrt{2}$ is the solution of $x^2 - 2 = 0$ with $\sqrt{2} \in \mathbb{R}_{>0}$

$\mathbb{Q}(\sqrt{2}) \xrightarrow{\sigma} \bar{\mathbb{Q}}$ is another field embedding

$a + b\sqrt{2} \longmapsto a - b\sqrt{2}$

Note $\sigma(\mathbb{Q}(\sqrt{2})) = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

From the algebraic point of view, $-\sqrt{2}$ has NO difference from $\sqrt{2}$.

Note also: The set of all field embeddings $\mathbb{Q}(\sqrt{2}) \hookrightarrow \bar{\mathbb{Q}} = \{\iota = {}^{id}, \sigma\}$

pf: Note

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \bar{\mathbb{Q}} \\ \cup & & \cup \\ \mathbb{Q} & & \end{array}$$

$\sigma|_{\mathbb{Q}} = id$

This is because, as σ is field morphism,

$$\left.\begin{array}{l}\sigma(0)=0\\ \sigma(1)=1\end{array}\right\} \Rightarrow \sigma(a)=a, \quad \forall a \in \mathbb{Q}$$

Thus, σ is determined by its image on $\sqrt{2}$.

$f_{\sqrt{2}}(x) = x^2 - 2 \in \mathbb{Q}[x]$ is the minimum irreducible poly of $\sqrt{2}$ over $\mathbb{Q}$.

Thus
$$0 = \sigma(0) = \sigma\left((\sqrt{2})^2 - 2\right)$$
$$= (\sigma(\sqrt{2}))^2 - \sigma(2)$$
$$= (\sigma(\sqrt{2}))^2 - 2$$

$\Rightarrow \sigma(\sqrt{2})$ is again a root of $x^2 - 2 = 0$

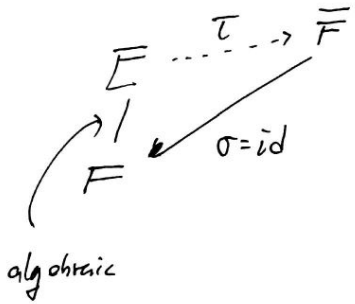
if $\sigma \neq id$, then $\sigma(\sqrt{2}) = -\sqrt{2}$. #

Then check directly that

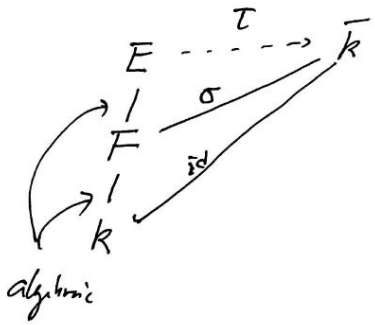
$\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ is indeed a field embedding.

#

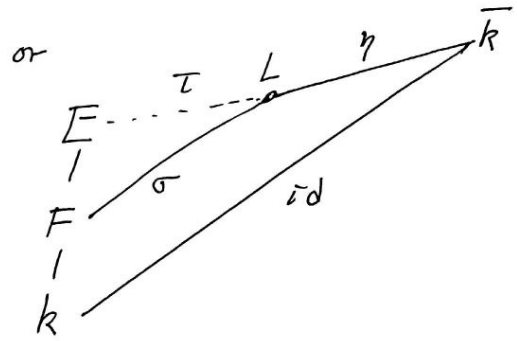
Consider:



or



or



AIM: Construction of an algebraic closure.

Definition: A field L is algebraically closed, if every polynomial in $L[X]$ of deg ≥ 1 has a root in L.

Prop: L algebraically closed.

Then $\forall f(x) \in L[x]$, $\deg f \geq 1$.

Then $\exists!\ \alpha_1, \ldots \alpha_n \in L$, $c \in L$, s.t

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

Pf: L alg. clsd $\Rightarrow$ $\exists\ \alpha_1 \in L$, s.t

$$f(\alpha_1) = 0$$

Euclidean division $\Rightarrow$ $\exists\ q(x), r(x) \in L[x]$

$$f(x) = (x-\alpha_1)q(x) + r(x)$$

$$\deg r(x) = 0 \quad \text{or} \quad r(x) = 0$$

$$\Updownarrow$$

$$r(x) = a \neq 0$$

$$0 = f(\alpha_1) = (\alpha_1 - \alpha_1)q(\alpha_1) + a = a \Rightarrow a = 0$$

Thus $f(x) = c(x-\alpha_1)q(x)$,

By induction on degree, $\Rightarrow \exists \alpha_1 \dots \alpha_n \in L$

$$f(X) = (X-\alpha_1)\dots(X-\alpha_n)\cdot c, \qquad c^* \in L$$

Certainly $\alpha_1 \dots \alpha_n$, and c are uniquely det. by f.

Cor: L alg. clsd, f irred poly in $L[X]$ is of degree one. #

Main thm 1: $\forall$ k field, there exists an algebraic extension $\bar{k}$, such that $\bar{k}$ is algebraically closed.

* Such $\bar{k}$ is called an algebraic closure of k. (existence of alg closure).

Main thm 2: k field, k_1, k_2 are alg ext of k,

if k_1, k_2 are both alg. closed, then k-isomorphism.

$\exists$ $k_1 \simeq k_2$

k

* Algebraic closure $\bar{k}$ of k is unique up to k-isomorphism.

Cor: k field, ~~$\bar{k}$~~

Ex: k field, $\bar{k}$ an alg clsre of k

$\bar{k}$ is an alg clsre of $\bar{k}$. Then $\bar{\bar{k}} = \bar{k}$.

Proof of Main Thm 1:

Step 1: $f_1, \dots, f_n \in k[x]$, $\deg f_i \geq 1$.

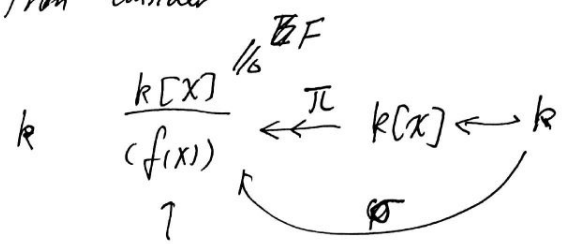
Then $\exists$ ext E/k. s.t

f_i has a root in E for each i.

Pf: It suffices to show $n=1$, and for this, we

can assume $f = f_1 \in k[x]$ irreducible.

Then consider



Set $\xi = \pi(X) \in \bar{F}$. Then

set $f(X) = \sum a_i X^i$, $a_i \in k$

$f^\sigma(X) = \sum \sigma(a_i) X^i$, $\sigma(a_i) \in F$

Then $f^\sigma(\xi) = f^\sigma(\pi(X)) = \pi(f(X)) = 0$

Now set $S = F \setminus \sigma(k)$

Set $E = k \amalg S$, and

Thus $k \subset E$. and $\begin{array}{ccc} E & \xrightarrow{\tilde{\sigma}} & F \\ \cup & 1\text{-}1 & \| \\ k & \xrightarrow{\sigma} & F \end{array}$ (i.e. $\tilde{\sigma}|_k = \sigma$)

put: $x, y \in E$.

$$x + y = \tilde{\sigma}^{-1}\left(\tilde{\sigma}(x) + \tilde{\sigma}(y)\right)$$

$$x \cdot y = \tilde{\sigma}^{-1}\left(\tilde{\sigma}(x) \cdot \tilde{\sigma}(y)\right)$$

Then E is a field, containing k as a subfield.

Moreover. $\alpha = \tilde{\sigma}^{-1}(\xi) \in E$ satisfies $f(\alpha) = 0$

as $\tilde{\sigma}(f(\alpha)) = f^\sigma(\xi) = 0$. #

Step 2 (E. Artin)

Construct first $k \subset E_1$ such that

$$\forall f(x) \in k[X], \quad f(\alpha) = 0, \text{ for some } \alpha \in E_1.$$

$$S = \{ X_f \mid f \in k[X], \deg f \geq 1 \}$$

$$k[S] = \left\{ \sum_{\text{finite sum}} a_i X_{f_i} \mid a_i \in k \right\} \quad \text{polynomial ring}$$

Consider the ideal

$$I = (f(X_f) \mid X_f \in S) \subseteq k[S]$$

Claim: I is not ~~the~~ unit ideal. i.e $k[S]$.

Indeed, assume the contrary, $\exists\, g_i \in k[S]$

$$\sum_{\text{finite sum}} g_i f_i(X_{f_i}) = 1 \qquad (*)$$

write $X_{f_i} = X_i$, $1 \leq i \leq n$.

write $g_i = g_i(X_1, \ldots X_n, \ldots X_N)$

Then rewrite $(*)$ into

$\sum_{\text{finite sum}} g_i(x_1 \dots x_N) f_i(x_i) = 1 \neq 0$. By Step 1, we take a finite ext $k \subset F$, s.t $\exists \alpha_i \in F$,

$$f_i(\alpha_i) = 0.$$

Then set $x_1 = \alpha_1, \dots, x_n = \alpha_n$, $x_{n+1} = \dots = x_N = 0$

we get

$$\sum g_i(\alpha_1 \dots \alpha_n, 0, \dots 0) f_i(\alpha_i) = 1$$

$$\| $$

$$\sum g_i(\alpha_1 \dots \alpha_n, 0 \dots 0) \cdot 0$$

$$\| $$

$$0$$

Contradiction! Thus $I \subset m$ for some max. ideal m.

Consider

$$k \hookrightarrow k[x] \xrightarrow{\pi} k[x]/m = F_1, \quad \pi \circ \sigma = \mathrm{id}_k$$

Then F_1 is a field ext of $\sigma(k)$. By the trick we used in s.t $\forall f \in k[x]$, $\deg(f) \geq 1$, f^σ has a root in F_1.

Step 1, we get $k \subset E_1$, s.t

$\forall f \in k[X]$, $\deg f \geq 1$, $f(X)$ has a root in E_1.

Now, we do the same thing consecutively, to get

$$k \subset E_1 \subset E_2 \subset \cdots \subset E_n \subset E_{n+1} \subset \cdots$$

s.t E_{n+1} is an ext of E_n, with all poly in $E_n[X]$

of degree ≥ 1 has a root in E_{n+1}.

Set: $E = \bigcup_{i \geq 1} E_i$. In an obvious way, E is a field.

E is alg. closed: $\forall f(x) \in E[X]$, $\exists n \in \mathbb{N}$

s.t $f(x) \in E_n[X]$ (as $f(x)$ has only finitely many coefficients).

Thus $f(x)$ has a root in $E_n \subset E$.

Step 3: Let $\overline{k} = \{a \in E \mid a \text{ alg over } k\}$

$k \subset \overline{k} \subset E$ ($\overline{k} \subset E$: subfield; $k \subset E$: algebraic). For $f(x) \in \overline{k}[X]$

$\exists\ \alpha \in \bar{E}, \quad f(\alpha) = 0$

State $f(x) = \sum_{i=1}^{n} a_i x^i, \quad a_i \in \bar{k}$

Then α is alg over $k(a_1, \cdots, a_n)$, a_i alg w. k, $\forall i$

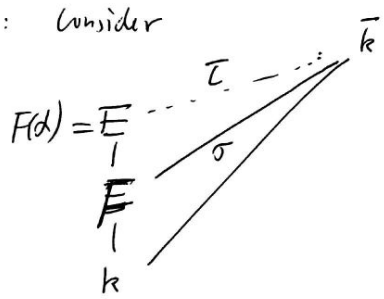
$\Rightarrow \alpha$ is alg over k. $\Rightarrow \alpha \in \bar{k}$.

Thus $\bar{k}$ is alg closed.

#

Proof of Main Thm 2:

Step 1: Consider



Given embedding $F \xrightarrow{\sigma} \bar{k}$, we show $\exists\ \tau : \overset{F(\alpha)}{\overset{\|}{\bar{E}}} \longrightarrow \bar{k}$

extends σ.

Let $f_\alpha \in F[x]$ be the irred. poly of α over F.

Since $\bar{k}$ is alg clsd, $\exists\ \beta \in \bar{k}$, s.t. $f_\alpha^\sigma(\beta) = 0$.

Now $F(\alpha) = F[\alpha]$, we define a map

$$\begin{array}{ccc} F[\alpha] & \xrightarrow{\tau} & \overline{k} \\ \downarrow & & \downarrow \\ f[\alpha] & \longmapsto & f^{\sigma}(\beta) \end{array}$$

This map is well-defined:

Suppose $f, g \in F[x]$, such that

$$f(\alpha) = g(\alpha)$$

Then $(f-g)(\alpha) = 0 \Rightarrow f_{\alpha} \mid f-g$

$$\Rightarrow f_{\alpha}^{\sigma} \mid f^{\sigma} - g^{\sigma}$$

$$\Rightarrow f_{\alpha}^{\sigma}(\beta) = f^{\sigma}(\beta) - g^{\sigma}(\beta)$$

$$0$$

ie $f^{\sigma}(\beta) = g^{\sigma}(\beta)$

This map is clearly an field embedding, and extends σ.
(check this !!!)

Rmk:

$$\#\{\tau : E \longrightarrow \bar{k},\ \tau|_F = \sigma\}$$

$$= \#\{\text{distinct roots of } f^\sigma_\alpha \text{ in } \bar{k}\}$$

Pf: The above proof shows that a distinct root of f^σ in $\bar{k}$ gives rise to a distinct extension of σ.

Thus $\#\{\text{distinct roots of } f^\sigma \text{ in } \bar{k}\} \le \#\{\tau : F \hookrightarrow \bar{k},\ \tau|_F = \sigma\}$.

On the other hand, given ext τ of σ:

we have

$0 = \tau(0) = \tau(f_\alpha(\alpha)) = f^\sigma_\alpha(\tau(\alpha))$, which says that

~~then~~ $\tau(\alpha)$ is a root of f^σ_α in $\bar{k}$.

and τ is uniquely determined by $\tau(\alpha) \in \bar{k}$, since $\tau|_F = \sigma$ and $E = F[\alpha]$.

Thus,

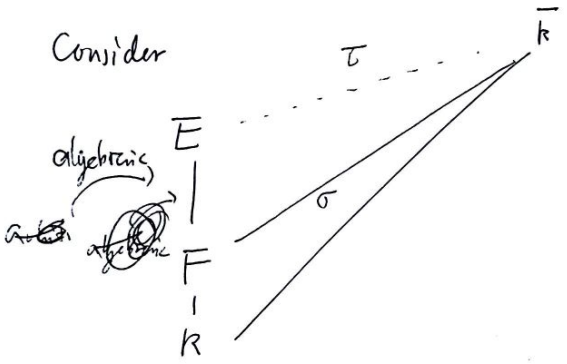
$$\#\{\tau : F \longrightarrow \bar{k},\ \tau|_F = \sigma\} \le \#\{\text{distinct roots of } f^\sigma \text{ in } \bar{k}\}.$$

#.

This remark generalizes the previous discussion on $\mathrm{Gal}(\sqrt{2}) \hookrightarrow \overline{G}$.

Step 2: (Zorn's Lemma).

Consider



$S = \{(L, \eta) \mid F \subset L \subset E,\ \eta \text{ extends } \sigma\}$

- $S \neq \phi$, $(F, \sigma) \in S$
- $(L_2, \eta_2) \geq (L_1, \eta_1)$ if $L_1 \subseteq L_2$, and η_1 extends η_2.
- $S' = \{(L_i, \eta_i)\}_{i \in I} \subseteq S$ totally ordered.

  $i < j \Rightarrow (L_i, \eta_i) < (L_j, \eta_j)$.

Then an maximal elemt in S is

$E \supset L \triangleq \bigcup_{i \in I} L_i \supset F$, define $\eta : L \to \bar{k}$ by

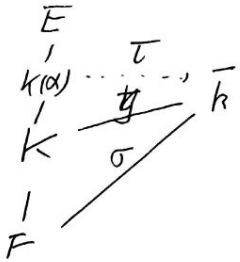
$\eta|_{L_i} \triangleq \eta_i$

Thus, by Zorn's lemma, we have a maximal element

(K, η) in S.

Claim: $K = \bar{E}$.

Otherwise, $\exists \alpha \in E \setminus K$, and consider

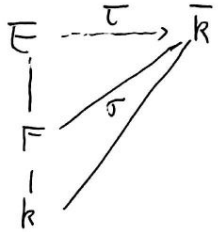


By Step 1, Given $\eta: K \longrightarrow \bar{k}$, $\exists\ \tau: K(\alpha) \longrightarrow \bar{k}$

extends η.

This contradicts with the maximality of (K, η).

Step 3: Cosider $E|F$ alg. + E alg closed.



claim: τ is an isomorphism.

Consider :

$$\begin{array}{c} \overline{k} \\ | \\ \tau(E) \\ | \\ \sigma(F) \\ | \\ k. \end{array}$$

E alg closed $\Rightarrow$ $\tau(E)$ is also alg. closed.

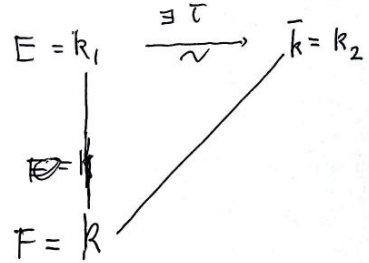
$\forall\, a \in \overline{k}$, a is alg over $\tau(E)$

$\Rightarrow$ $f_a \in \tau(E)[X]$ the ind poly of a over $\tau(E)$.

is of degree one.

$\Rightarrow$ $a \in \tau(E)$ i.e $\tau(E) = \overline{k}$.

Now apply the Main theorem 2 follows :



#