3/27

Wednesday, March 27, 2019 11:33

algebraic closure of finite fields:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^{2!}} \subseteq \mathbb{F}_{p^{3!}} \subseteq \cdots$$

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$$

An embedding of an extension K/F to an extension E/F

is a hom-sm $\varphi : K \to E$ s.t. $\varphi|_F = \mathrm{Id}_F$

$$\begin{tikzcd}
K \arrow[rr, "\varphi"] \arrow[dr, dash] & & E \arrow[dl, dash] \\
& F &
\end{tikzcd}$$

which is always injective (since K is a field)

An isomorphism $K/F \xrightarrow{\varphi} K/F$ is called

an automorphism of K/F.

Automorphisms of K/F form a group, $\mathrm{Aut}(K/F)$.

if $[K:F]$ is finite, any embedding $K/F \to K/F$

is an aut-sm.

If $K \subseteq E$, let $\alpha \in K$. Let $\varphi : K \longrightarrow E$ be an embedding of extensions (over F).

Let $f = m_{\alpha,F} \in F[x]$. Then $\varphi(f) = f$, so $0 = \varphi(f(\alpha)) = f(\varphi(\alpha))$. So $\varphi(\alpha)$ is a conjugate of α over F.

eg
$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &\longrightarrow E \\ \sqrt{2} &\longmapsto \pm\sqrt{2} \\ i &\longmapsto \pm i \\ \sqrt[n]{2} &\longmapsto \omega^k \sqrt[n]{2} \quad \text{where } (k,n) = 1. \end{aligned}$$

Let $K = F(\alpha)$, $n = \deg_F \alpha$.

Then in any extn E/F with $K \subseteq E$, α has at most n conjugates in E.

Any embedding $K/F \xrightarrow{\varphi} E/F$ is defined by $\varphi(\alpha)$ which is a conjugate of α.

So $\exists$ at most n embeddings $K/F \longrightarrow E/F$.

$\exists$ exactly n embeddings $K/F \longrightarrow E/F$ iff

. .

$m_{\alpha,F}$ is separable & splits completely in E.

Let $F_1 \subseteq E$. Let $\alpha \in E$,

and let $\varphi : F_1 \to E$, $\varphi(F_1) =: F_2$.

Let $f_1 = m_{\alpha, F_1}$. Let $f_2 = \varphi(f_1)$.

Let $\tilde{\varphi} : F_1(\alpha) \to E$ be a hom-sm s.t. $\tilde{\varphi}|_{F_1} = \varphi$

Then $\tilde{\varphi}(\overset{0}{\overset{\shortparallel}{f_1(\alpha)}}) = \varphi(f_1)(\tilde{\varphi}(\alpha)) = f_2(\tilde{\varphi}(\alpha))$

$$\begin{tikzcd} F_1(\alpha) \arrow[r, "\tilde{\varphi}"] \arrow[d, dash] & E \arrow[d, dash] \\ F_1 \arrow[r, "\varphi"'] & F_2 \end{tikzcd}$$

So $\tilde{\varphi}(\alpha)$ is a root of f_2.

f_1 is irr. iff f_2 is irr.

So $\#\{\tilde{\varphi} : F_1(\alpha) \to E \ : \ \tilde{\varphi}|_{F_1} = \varphi\} = \#$ roots of f_2 in E

$\leq \deg f_2 = \deg f_1 = \deg_{F_1} \alpha$.

Let $[K : F]$ be finite. Then $K = F(\alpha_1, \dots, \alpha_k)$

Tower of simple extensions:

$F(\alpha_1, \dots, \alpha_k) \xrightarrow{\ \ } E$ $\qquad$ $K \subseteq E$.

$$\begin{tikzcd}
F(\alpha_1,\dots,\alpha_k) \arrow[r] & E \\
\vdots \arrow[u, dash] & \\
F(\alpha_1,\alpha_2) \arrow[u, dash] \arrow[uur] & \\
F(\alpha_1) \arrow[u, dash] \arrow[uuur] & \\
F \arrow[u, dash] \arrow[uuuur, "\mathrm{id}_F"'] &
\end{tikzcd}$$

$K \subseteq E$.

embeddings

$K/_F \longrightarrow E/_F$?

Let $n = [K:F] = (\deg_F \alpha_1)(\deg_{F(\alpha_1)} \alpha_2) \cdots (\deg_{F(\alpha_1,\dots,\alpha_{k-1})} \alpha_k)$.

We have $\leq \deg_F \alpha_1$ embeddings $F(\alpha_1)/_F \longrightarrow E/_F$.

$\forall$ embedding $\varphi : F(\alpha_1)/_F \longrightarrow E/_F$, we have at most $\deg_{F(\alpha_1)} \alpha_2$ embeddings $F(\alpha_1,\alpha_2)/_F \to E/_F$ extending φ.

$\vdots$

So we have at most n embeddings $K/_F \longrightarrow E/_F$.

If $\forall i$, α_i is separable over F & $m_{\alpha_i,F}$ splits completely in E, then there are exactly

this is more than .

sufficient (i.e. it's not necessary)

n embeddings $K/_F \longrightarrow E/_F$.

<u>Theorem</u> If $K/_F$ is a finite extension, $K \subseteq E$, $[K:F] = n$, then there are $\leq n$ embeddings $K/_F \longrightarrow E/_F$. If K is generated by separable elements whose minimal polynomials split in E, then the number of such embeddings is n.

If $\exists\, \alpha \in K$ s.t. α is not separable or $m_{\alpha,F}$ doesn't split in E, then

$\#$ embeddings is $< n$.

Bad Version: If K is a splitting field of a separable polynomial, then the number of such embeddings is $= n$.

to see the last part is true, add a bottom floor

$$\begin{array}{c} F(\alpha) \\ | \\ F \end{array}$$

to the tower.

there is a wrong number of extensions at this step. So total $\#$ will be wrong.

<u>Corollary</u>: if K is generated by separable elements,

then every element of K is separable.

(i.e. K is separable).

If additionally, min pol-ls of generating elements split in E, then $\forall \alpha \in K$, $m_{\alpha,F}$ splits in E.

this is
true because
the splittability
of the minimal polynomials
is controllable: we can just pick the right E.