TWO MAIN THMS OF GALOIS THEORY!

THM 1: $\mathbb{K}/\mathbb{F}$ finite

$\Rightarrow$ (i) $\mathbb{F} \subseteq \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$ (silly!)

(ii) $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$

and TFAE:

(a) equality in (i): $\mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

(b) $\exists$ some group $G \leq \mathrm{Aut}(\mathbb{K})$ for which $\mathbb{F} = \mathbb{K}^G$

(c) equality in (ii): $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$

(d) $\mathbb{K} = \mathrm{Split}_{\mathbb{F}}(f(x))$ where $f(x)$ is any separable polynomial in $\mathbb{F}[x]$

All of these (a) – (d) can be used to define $\mathbb{K}/\mathbb{F}$ Galois

THM 2: When $\mathbb{K}/\mathbb{F}$ is Galois,

with $G := \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$

one has a bijection

$$\left\{ \begin{array}{c} \mathbb{K} \\ | \\ \mathbb{L} \\ | \\ \mathbb{F} \end{array} \ \text{subfields} \right\} \longleftrightarrow \left\{ \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \ \text{subgroups} \right\}$$

$$\mathbb{L} \longmapsto H := \underbrace{\{\sigma \in G : \sigma|_{\mathbb{L}} = 1_{\mathbb{L}}\}}_{=\mathrm{Aut}(\mathbb{K}/\mathbb{L})}$$

$$\mathbb{L} := \mathbb{K}^H \longleftarrow H < G$$

with

$$\begin{array}{c} \mathbb{K} \\ | \\ \mathbb{L} = \mathbb{K}^H \\ | \\ \mathbb{F} \end{array}$$

always Galois, $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) = H$

degree $[G:H]$, and Galois $\Leftrightarrow H \lhd G$ in which case, $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = G/H$

NEXT TIME:

- can easily compute $m_{\alpha,\mathbb{F}}(x)$ for $\alpha \in \mathbb{K}$
- $\mathbb{L}_1 \mathbb{L}_2$, $\mathbb{L}_1 \cap \mathbb{L}_2$ corr. $H_1 \cap H_2$, $\langle H_1, H_2 \rangle$

REMARK from a question asked after class:

Since for any $H < \mathrm{Aut}(\mathbb{K})$

we know from THM 1 that

$$\mathbb{K}/\mathbb{K}^H \text{ is Galois}$$

so we have equality in

$$\mathbb{K}^H \subset \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{K}^H)}$$

i.e. $$\boxed{\mathbb{K}^H = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{K}^H)}}$$

... and $$H \leq \mathrm{Aut}(\overbrace{\mathbb{K}/\underbrace{\mathbb{K}^H}_{\mathbb{L}}}^{\text{Galois}})$$

also has equality:

THM 2 $\Rightarrow$ $$H = \mathrm{Aut}(\mathbb{K}/\underbrace{\mathbb{K}^H}_{\mathbb{L}})$$

$\mathbb{L} = \mathbb{K}^H$

so $\mathbb{L} \leftrightarrow H$

What we didn't say at end of last time...

Given $\alpha \in \mathbb{K}$ with $\mathbb{K}/\mathbb{F}$ Galois,

$$\begin{array}{c}\mathbb{K}\\ |\\ \mathbb{F}\end{array}$$

and $G := \mathrm{Aut}(\mathbb{K}/\mathbb{F})$

then $$m_{\alpha,\mathbb{F}}(x) = \prod_{\substack{\text{distinct}\\ \text{Galois images}\\ \{g(\alpha) : g \in G\}}} (x - g(\alpha))$$

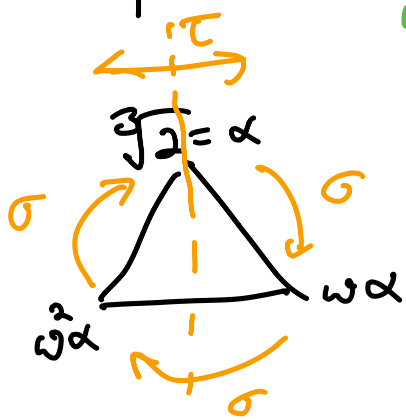
Note that this is a separable polynomial

$$\left[\text{where } H := \{g \in G : g(\alpha) = \alpha\} \quad = \prod_{gH \in G/H} (x - g(\alpha)) \right]$$

EXAMPLE: Let's compute

$m_{\beta,\mathbb{Q}}(x)$ for $\underset{\omega+2}{\overset{\|}{\beta}} \in \mathbb{K} = \mathrm{Split}_{\mathbb{Q}}(x^3-2)$

$= \mathbb{Q}(\omega, \alpha)$, $\omega = e^{2\pi i/3}$, $\alpha = \sqrt[3]{2}$



Who are the distinct Galois images $\{g(\beta) : g \in G\}$?

$= \{1(\beta), \tau(\beta)\}$

$= \{\beta, \tau(\beta)\}$

$= \{\omega+2, \omega^2+2\}$

$\Longrightarrow m_{\beta,\mathbb{Q}}(x) =$

$(x-(\omega+2))(x-(\omega^2+2))$

$= x^2 - (\omega+\omega^2+4)x + (\omega+2)(\omega^2+2)$

$= x^2 - (-1+4)x + \omega^3 + 2(\omega+\omega^2) + 4$

$= x^2 - 3x + 1 + 2(-1) + 4$

$= x^2 - 3x + 3$

$\in \mathbb{Q}[x]$

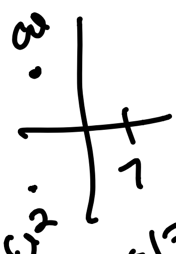
$\tau(\omega) = \omega^2$	$\sigma(\alpha) = \omega\alpha$
$\tau(\alpha) = \alpha$	$\sigma(\omega) = \omega$

$\Downarrow$

$\sigma(\omega+2) = \omega+2$

$\sigma(\beta) = \beta$

$\sigma^2(\beta) = \beta$



$\omega^2+\omega+1=0$

$H = \{g \in G : g(\beta) = \beta\}$

$= \langle \sigma \rangle$

$= \{1, \sigma, \sigma^2\}$

G/H has coset reps $\{1, \tau\}$

NON-GALOIS EXAMPLES

(1) $$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}) = \mathbb{K} \\ | \\ \mathbb{Q} \end{array} \Bigg\}$$ not Galois, not splitting

and $|\underset{\sigma}{\underset{\cup}{\mathrm{Aut}}}(\mathbb{K}/\mathbb{Q})| = |\{1\}| < [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$

σ sends $\sqrt[3]{2}$ to a root of x^3-2 inside $\sqrt[3]{2}$

i.e. $\sigma = 1_{\mathbb{K}}$

(2) $$\begin{array}{c} \mathbb{K} = \mathrm{Split}_{\mathbb{F}}(x^p - t) = \mathbb{F}_p(t^{1/p}) = \mathbb{F}_p(t)(t^{1/p}) \\ \Big|\, p \\ \mathbb{F} = \mathbb{F}_p(t) \end{array} \Bigg\}$$ not Galois, splitting but not for a separable polynomial

since $x^p - t = (x - t^{1/p})^p$

and $|\underset{\sigma}{\underset{\cup}{\mathrm{Aut}}}(\mathbb{K}/\mathbb{F})| = |\{1\}| < [\mathbb{K}/\mathbb{F}] = p$

σ send $t^{1/p}$ to another root of $x^p - t$, i.e. to itself

③ Let $\mathbb{F}$ be any infinite field of char p, e.g. $\mathbb{F}_p(t)$, $\overline{\mathbb{F}_p}$

Then consider $\mathbb{F}(u^{1/p}, v^{1/p}) = \mathbb{K}$

$$
\begin{tikzcd}
 & \mathbb{F}(u^{1/p}, v^{1/p}) = \mathbb{K} \arrow[dl, dash, "p"'] \arrow[d, dash, "p"] \arrow[dr, dash, "p"] & \\
\mathbb{F}(u^{1/p}, v) \arrow[dr, dash, "p"'] & \mathbb{F}(u, v^{1/p}) \arrow[d, dash, "p"] \quad \ldots & \mathbb{F}(u, v, u^{1/p} + c v^{1/p}) \ldots \arrow[dl, dash, "p"] \\
 & \mathbb{F}(u, v) &
\end{tikzcd}
$$

where $c \in \mathbb{F}$

splits $x^p - (u + c^p v) \in \mathbb{F}(u,v)[x]$

$\mathbb{K}/\mathbb{F}(u,v)$ is not Galois, and has ∞ many intermediate subfields, since...

If $\mathbb{F}(u,v,u^{1/p} + cv^{1/p}) = \mathbb{F}(u,v,u^{1/p} + c'v^{1/p})$

then it contains

$$
\begin{array}{r}
u^{1/p} + cv^{1/p} \\
u^{1/p} + c'v^{1/p} \\
\hline
(c-c')v^{1/p}
\end{array}
\quad \underset{c-c' \in \mathbb{F}}{\Rightarrow} \quad v^{1/p} \text{ is in it}
$$

subtract

$\Rightarrow v^{1/p} \in \mathbb{F}(u,v,u^{1/p} + cv^{1/p})$

$\Rightarrow u^{1/p} \in \mathbb{F}(u,v,u^{1/p} + cv^{1/p})$

$\Rightarrow \mathbb{F}(u,v,u^{1/p} + cv^{1/p}) = \mathbb{K} = \mathbb{F}(u^{1/p}, v^{1/p})$ contradiction.

Why should $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$?

Dedekind's lemma:

For G a group and $\mathbb{K}$ a field, a linear character is a group homomorphism $G \xrightarrow{\tau} \mathbb{K}^\times$

i.e. $\tau(gh) = \tau(g)\tau(h)$

Then $\tau_1, \tau_2, \ldots, \tau_n : G \longrightarrow \mathbb{K}^\times$ distinct characters are $\mathbb{K}$-lin. indep. inside $\{\text{functions } G \longrightarrow \mathbb{K}\}$ with pointwise addition & scaling,

i.e. $c_1\tau_1(g) + \ldots + c_n\tau_n(g) = 0$ for some $c_1, c_2, \ldots, c_n \in \mathbb{K}$ and $\forall g \in G$

then $c_1 = \ldots = c_n = 0$.

proof: Assume we had such a dependence

$$(*) \quad c_1\tau_1(g) + \cdots + c_k\tau_k(g) = 0 \quad \forall g \in G$$

with $c_1, \ldots, c_k \neq 0$
and k minimal

We'll create a smaller dependence.

Then $\tau_1 \neq \tau_2$ so pick $h \in G$ with $\boxed{\tau_1(h) \neq \tau_2(h)}$.

Mult. $(*)$ by $\tau_1(h)$, giving

$$\underline{c_1\tau_1(h)\tau_1(g)} + c_2\tau_1(h)\tau_2(g) + \cdots + c_k\tau_1(h)\tau_k(g) = 0 \quad \forall g \in G$$

Also

$$c_1\tau_1(hg) + c_2\tau_2(hg) + \cdots + c_k\tau_k(hg) = 0$$

$$\underline{c_1\tau_1(h)\tau_1(g)} + c_2\tau_2(h)\tau_2(g) + \cdots + c_k\tau_k(h)\tau_k(g) = 0$$

subtract

$$c_2\big(\underbrace{\tau_1(h) - \tau_2(h)}_{\neq 0}\big)\tau_2(g) + \cdots + c_k\big(\tau_1(h) - \tau_k(h)\big)\tau_k(g) = 0 \quad \forall g \in G$$

a smaller dependence. ∎

COR (to Dedekind's Lemma)

If $[\mathbb{K}:\mathbb{F}] < \infty$, then

$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$.

proof: Why does $[\mathbb{K}:\mathbb{F}] < \infty$

imply $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ finite?

$\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ α_i algebraic

so $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is determined

by choices of $\sigma(\alpha_i) \in \underbrace{\{\text{roots of } m_{\mathbb{F},\alpha_i}(x)\}}_{\text{finitely many choices.}}$

So let $[\mathbb{K}:\mathbb{F}] = m$

and $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = n$

and show a contradiction

if $m < n$.

Let $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \{\tau_1, \tau_2, \ldots, \tau_n\}$ distinct
and think of them as characters

$$\begin{array}{c} G \xrightarrow{\tau_i} \mathbb{K}^\times \\ \shortparallel \\ \mathbb{K}^\times \end{array}$$

If $[\mathbb{K}:\mathbb{F}] = m < n$, let
$\mathbb{K}$ have $\mathbb{F}$-basis $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$.
Consider the $m \times n$ matrix

$$m \left\{ \begin{array}{c} \alpha_1 \\ \vdots \\ \alpha_m \end{array} \right. \underbrace{\begin{bmatrix} \tau_1(\alpha_1) & \cdots & \tau_n(\alpha_1) \\ & & \\ \tau_1(\alpha_m) & \cdots & \tau_n(\alpha_m) \end{bmatrix}}_{n} \quad m < n$$

$\tau_1 \quad\quad \tau_n$

which has a $\mathbb{K}$-lin. dependence on its columns say $\sum_{i=1}^{n} c_i \tau_i(\alpha_j) = 0 \quad \forall j = 1, \ldots, m.$

We'll show $\sum c_i \tau_i$ vanishes on every $\alpha \in \mathbb{K}^\times$,
since $\alpha = \sum_{j=1}^{m} b_j \alpha_j$ with $b_j \in \mathbb{F}$

$$\boxed{\sum_{i=1}^{n} c_i \tau_i(\alpha_j) = 0} \qquad \forall j = 1, \dots, m$$

$\alpha \in \mathbb{K}^\times$ has $\alpha = \sum_{j=1}^{m} b_j \alpha_j$, $b_j \in \mathbb{F}$

Since $\tau_i \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, they're

$\mathbb{F}$-linear:

$$\tau_i(\alpha\beta) = \tau_i(\alpha)\tau_i(\beta)$$

$$\tau_i(\alpha+\beta) = \tau_i(\alpha) + \tau_i(\beta)$$

$$\tau_i(c\alpha + d\beta) = c\tau_i(\alpha) + d\tau_i(\beta)$$

$\forall c, d \in \mathbb{F}$ since $\tau_i|_{\mathbb{F}} = 1_{\mathbb{F}}$

So
$$\sum_{i=1}^{n} c_i \tau_i(\alpha) = \sum_{i=1}^{n} c_i \tau_i\left(\sum_{j=1}^{m} b_j \alpha_j\right)$$

$$= \sum_{i=1}^{n} c_i \sum_{j=1}^{m} b_j \tau_i(\alpha_j)$$

$$= \sum_{j=1}^{m} b_j \underbrace{\left(\sum_{i=1}^{n} c_i \tau_i(\alpha_j)\right)}_{=0 \ \forall j=1,\dots,m.} = 0$$

∎

When do we get equality?

PROP: (a) If $G < \mathrm{Aut}(\mathbb{K})$ is finite,

then (i) $|G| = [\mathbb{K} : \mathbb{K}^G]$

and (ii) $G = \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$

($G \leq \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$ is clear)

(b) Conversely, suppose $[\mathbb{K} : \mathbb{F}]$ is finite, then

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$$

$$\iff \mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$$

If we believe the PROP,

then it gives (a) $\iff$ (b) $\iff$ (c) in THM 1 from Galois Thy.

When do we get equality.?

PROP: (a) If $G < \mathrm{Aut}(\mathbb{K})$ is finite,

then (i) $|G| = [\mathbb{K} : \mathbb{K}^G]$

and (ii) $G = \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$

($G \leq \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$ is clear)

(b) Conversely, suppose $[\mathbb{K} : \mathbb{F}]$ is finite, then

$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$

$\iff \mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

Also, everything will follow if we can show $|G| \geq [\mathbb{K} : \mathbb{K}^G]$.

1st: Then $[\mathbb{K} : \mathbb{K}^G] \leq |G| \leq |\mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)|$

$G \leq \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$

+ our COR to Dedekind

$\Rightarrow [\mathbb{K} : \mathbb{K}^G] = |G| = |\mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)|$

and $G = \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$

showing (i), (ii) in PROP

$$|G| \geq [\mathbb{K} : \mathbb{K}^G]$$

When do we get equality.

PROP: (a) If $G < \mathrm{Aut}(\mathbb{K})$ is finite,

then (i) $|G| = [\mathbb{K} : \mathbb{K}^G]$

and (ii) $G = \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$

($G \leq \mathrm{Aut}(\mathbb{K}/\mathbb{K}^G)$ is clear)

(b) Conversely, suppose $[\mathbb{K} : \mathbb{F}]$ is finite, then

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$$

$$\iff \mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$$

For (b), Assuming $\underline{[\mathbb{K} : \mathbb{F}] = |\mathrm{Aut}(\mathbb{K}/\mathbb{F})|}$

degree $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|$

$\mathbb{K}$

$|$ ← degree $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})|$ by (a)

$\mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

$|$ ← forces equality here: $\mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

$\mathbb{F}$

i.e. $\Rightarrow$ in (b) holds.

$\Leftarrow$ in (b) is (a) applied to $\underbrace{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}_{=G}$.

Why does

$$|G| \geq [\mathbb{K} : \mathbb{K}^G]$$ hold?

Name $G = \{g_1, \dots, g_n\}$ so $|G| = n$.

Assume we have $\{\alpha_1, \dots, \alpha_n, \alpha_{n+1}\}$ $\mathbb{K}^G$-lin. indep. elements in $\mathbb{K}$, to get a contradiction.

Consider the matrix

$$n\left\{ \underbrace{\begin{bmatrix} g_1(\alpha_1) & \cdots & g_1(\alpha_{n+1}) \\ \vdots & & \\ g_n(\alpha_1) & \cdots & g_n(\alpha_{n+1}) \end{bmatrix}}_{n+1} \right.$$

so it has a column dependence over $\mathbb{K}$ say of minimal size k

$$(*) \quad \sum_{i=1}^{k} c_i \, g_j(\alpha_i) = 0 \qquad \forall j = 1, \dots, n$$

with $c_i \in \mathbb{K}^\times$

WLOG, $c_1 = 1$ in $\mathbb{K}$

$$(*) \quad \sum_{i=1}^{k} c_i \, g_j(\alpha_i) = 0 \qquad \forall j = 1, \dots, n$$

with $c_i \in \mathbb{K}^\times$

WLOG, $c_1 = 1$ in $\mathbb{K}$

We'll show every $c_i \in \mathbb{K}^G$ for $i = 1, \dots, k$ and they lead to a $\mathbb{K}^G$-dependence on the α_i's.

Given any $g \in G$, apply it to $(*)$, giving

$$\sum_{i=1}^{k} g(c_i g_j(\alpha_i)) = 0 \qquad \forall j = 1, \dots, n$$

$$\parallel$$

$$\sum_{i=1}^{k} g(c_i) \, g g_j(\alpha_i)$$

Since g permutes $\{g_1, \dots, g_n\} = G$,

this says $\displaystyle\sum_{i=1}^{k} g(c_i) \, g_j(\alpha_i) = 0 \quad (**)$

Subtracting $(*)$ and $(**)$ gives

$$\sum_{i=1}^{k} \underbrace{(g(c_i) - c_i)}_{=1-1=0 \text{ if } i=1} g_j(\alpha_i) = 0 \qquad \forall j = 1, \dots, n$$

hence this is a smaller dependence, so $g(c_i) - c_i = 0$ $\forall g \in G$ i.e. $c_i \in \mathbb{K}^G$

(*) $\displaystyle\sum_{i=1}^{k} c_i\, g_j(\alpha_i) = 0 \quad \forall j = 1, \dots, n$

with $c_i \in \mathbb{K}^\times$

Now that we know $c_1, \dots, c_k \in \mathbb{K}^G$, we can deduce from (*) that

$$g_j\left(\sum_{i=1}^{k} c_i\, \alpha_i \right) = 0$$

$c_i = g(c_i)$

and $g_j \in \mathrm{Aut}(\mathbb{K})$ so invertible,

so $$\sum_{i=1}^{k} c_i\, \alpha_i = 0$$

a dependence with $\mathbb{K}^G$-coeffs among α_i's. Contradiction.

$\blacksquare$

<u>THM 1</u>: $\mathbb{K}/\mathbb{F}$ finite

$\Rightarrow$ (i) $\mathbb{F} \subseteq \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$ (silly!)

(ii) $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$

and TFAE:

Shown equiv before

(a) equality in (i): $\mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

(b) $\exists$ some group $G \leq \mathrm{Aut}(\mathbb{K})$ for which $\mathbb{F} = \mathbb{K}^G$

(c) equality in (ii): $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$

(d) $\mathbb{K} = \mathrm{Split}_{\mathbb{F}}(f(x))$ where $f(x)$ is ~~any~~ (some) separable polynomial in $\mathbb{F}[x]$

(e) $\mathbb{K}/\mathbb{F}$ is normal & separable,

i.e. every $\alpha \in \mathbb{K}$ has $m_{\alpha,\mathbb{F}}(x)$ splitting completely in $\mathbb{K}[x]$, with distinct roots

Morandi proves (a), (d), (e) equivalent only assuming $\mathbb{K}/\mathbb{F}$ algebraic (his THM 4.9)

(a) equality in (i): $\mathbb{F} = \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}$

(e) $\mathbb{K}/\mathbb{F}$ is normal & separable,

i.e. every $\alpha \in \mathbb{K}$ has $m_{\alpha,\mathbb{F}}(x)$ splitting completely in $\mathbb{K}[x]$, with distinct roots

---

Given $\alpha \in \mathbb{K}$, let $\{\alpha_1, \ldots, \alpha_n\}$ be the distinct images $\{\sigma(\alpha) : \sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})\}$ (so $n \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$)

Then consider

$$f(x) := \prod_{i=1}^{n} (x - \alpha_i)$$

$$= x^n - \underbrace{(\alpha_1 + \cdots + \alpha_n)}_{e_1(\alpha_1, \ldots, \alpha_n)} x^{n-1} + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)}_{e_2(\alpha_1, \ldots, \alpha_n)} x^{n-2} - \cdots + (-1)^n \underbrace{\alpha_1\alpha_2\cdots\alpha_n}_{e_n(\alpha_1, \ldots, \alpha_n)} x^0$$

$$\in \mathbb{K}^{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}[x] \underset{\text{by (a)}}{=} \mathbb{F}[x]$$

REMARK: In fact, $f(x) = m_{\alpha,\mathbb{F}}(x)$, since every $\sigma(\alpha)$ is also a root of $m_{\alpha,\mathbb{F}}(x)$.

which is a polynomial in $\mathbb{F}[x]$ having α as a root. Hence $m_{\alpha,\mathbb{F}}(x)$ divides $f(x)$, and has distinct roots, since $f(x)$ does by construction.

(d) $\mathbb{K} = \mathrm{Split}_{\mathbb{F}}(f(x))$ where
$f(x)$ is ~~any~~ (some) separable polynomial
in $\mathbb{F}[x]$

$\Uparrow$

(e) $\mathbb{K}/\mathbb{F}$ is normal & separable,
i.e. every $\alpha \in \mathbb{K}$ has
$m_{\alpha,\mathbb{F}}(x)$ splitting completely in $\mathbb{K}[x]$,
with distinct roots

Assuming (e),

$$\mathbb{K} = \mathrm{Split}_{\mathbb{F}}\left(\{ m_{\alpha,\mathbb{F}}(x) : \alpha \in \mathbb{K} \} \right)$$

$$= \mathrm{Split}_{\mathbb{F}}\left(m_{\alpha_1,\mathbb{F}}(x), \ldots, m_{\alpha_n,\mathbb{F}}(x) \right)$$

for some $\alpha_1, \ldots, \alpha_n$

e.g., if $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$

$$= \mathrm{Split}_{\mathbb{F}}(f(x)) \text{ where}$$

$$f(x) = \mathrm{l.c.m.}\left(m_{\alpha_1,\mathbb{F}}(x), \ldots, m_{\alpha_n,\mathbb{F}}(x) \right)$$

and since each $m_{\alpha_i,\mathbb{F}}(x)$ has distinct roots,
so does $f(x)$, i.e. $f(x)$ is separable.

(c) equality in (ii): $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$

$\Uparrow$

(d) $\mathbb{K} = \mathrm{Split}_{\mathbb{F}}(f(x))$ where $f(x)$ is (some) any separable polynomial in $\mathbb{F}[x]$

Assuming (d), we'll show by induction on $[\mathbb{K}:\mathbb{F}]$ that $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \geq [\mathbb{K}:\mathbb{F}]$.

If $[\mathbb{K}:\mathbb{F}]=1$, then $\mathbb{K}=\mathbb{F}$, done.

If $[\mathbb{K}:\mathbb{F}] \geq 2$, so let $\alpha \in \mathbb{K}$ be any root of some irreducible factor $m_{\alpha,\mathbb{F}}(x)$ that is at least quadratic, so $[\mathbb{F}(\alpha):\mathbb{F}] \geq 2$.

Strategy:

still a splitting field for some separable $f(x)$; the same $f(x)$!

$$\begin{tikzcd}
\mathbb{K} \arrow[r, "\tau_i"] \arrow[d, dash] & \mathbb{K} \arrow[d, dash] \\
\mathbb{F}(\alpha) \arrow[r] \arrow[d, dash, "\deg n"'] & \mathbb{F}(\alpha_i) \arrow[d, dash] \\
\mathbb{F} \arrow[r, "1_{\mathbb{F}}"] & \mathbb{F}
\end{tikzcd}$$

$\alpha \longmapsto \alpha_i$

$\mathbb{F}(\alpha_i)$ where $m_{\alpha,\mathbb{F}}(x)$ has distinct roots $\{\alpha_1, \ldots, \alpha_n\}$

Strategy:

$$\begin{tikzcd} \mathbb{K} \arrow[r, "\tau_i"] \arrow[d, dash] & \mathbb{K} \arrow[d, dash] \\ \mathbb{F}(\alpha) \arrow[r, "\alpha \mapsto \alpha_i"'] \arrow[d, dash, "\deg n"'] & \mathbb{F}(\alpha_i) \arrow[d, dash] \\ \mathbb{F} \arrow[r, "1_{\mathbb{F}}"] & \mathbb{F} \end{tikzcd}$$

still a splitting field for some separable $f(x)$; the same $f(x)$!

$\mathbb{F}(\alpha_i)$ where $m_{\alpha,\mathbb{F}}(x)$ has distinct roots $\{\alpha_1, \dots, \alpha_n\}$

We claim that if $H := \mathrm{Aut}(\mathbb{K}/\mathbb{F}(\alpha))$ then by induction $|H| \geq [\mathbb{K}:\mathbb{F}(\alpha)]$.

Also, we claim that inside $G = \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, the cosets $\tau_i H$ are all distinct:

if $\tau_i H = \tau_j H$, then
$$\tau_j^{-1}\tau_i H = H$$
$$\tau_j^{-1}\tau_i \in H$$
$$\tau_j^{-1}\tau_i(\alpha) = \alpha$$
$$\Rightarrow \underset{\alpha_i}{\underset{\parallel}{\tau_i(\alpha)}} = \tau_j(\alpha) = \alpha_j$$
contradiction.

Hence
$$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = |G| = [G:H] \cdot |H|$$
$$\geq \underbrace{n}_{\deg(m_{\alpha,\mathbb{F}}(x)) = [\mathbb{F}(\alpha):\mathbb{F}]} \cdot [\mathbb{K}:\mathbb{F}(\alpha)]$$
$$= [\mathbb{K}:\mathbb{F}] \quad \blacksquare$$

THM 2 (augmented):

$\mathbb{K}/\mathbb{F}$ a finite Galois extension, $G=\mathrm{Aut}(\mathbb{K}/\mathbb{F})$.

Then we have inclusion-reversing bijections

$$\left\{\begin{array}{c}\mathbb{K}\\ | \\ \mathbb{L} \\ | \\ \mathbb{F}\end{array} \ \begin{array}{l}\text{intermediate}\\ \text{subfields } \mathbb{L}\end{array}\right\} \rightleftarrows \left\{\begin{array}{c}\text{subgroups}\\ H\end{array} \quad \begin{array}{c}1\\ | \\ H \\ | \\ G\end{array}\right\}$$

$$\mathbb{L} \longmapsto \mathrm{Aut}(\mathbb{K}/\mathbb{L})$$

$$\mathbb{K}^H \longleftarrow H$$

with these properties:

come from previous work

(i) $|H| = [\mathbb{K}:\mathbb{L}]$
$[G:H] = [\mathbb{L}:\mathbb{F}]$ — follows from multiplicativity

(ii) $\mathbb{K}/\mathbb{L}$ is always Galois, with $H=\mathrm{Aut}(\mathbb{K}/\mathbb{L})$ if $\mathbb{L}=\mathbb{K}^H$

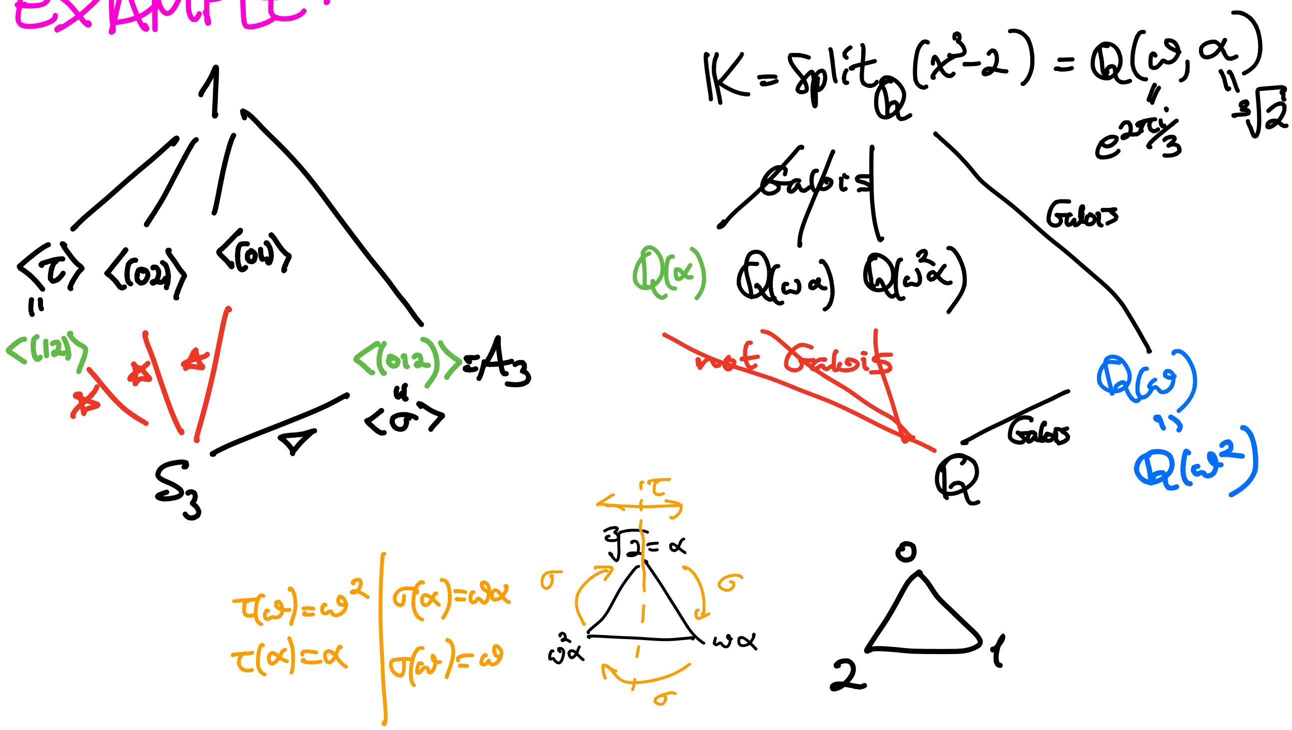
(iii) $\mathbb{L}/\mathbb{F}$ is Galois $\iff \mathbb{L}=\mathbb{K}^H$ with $H \trianglelefteq G$
and in this case $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = G/H$

(iv) Even if $\mathbb{L}/\mathbb{F}$ is not Galois so $H \ntrianglelefteq G$,
there is a bijection
$$\{\text{cosets of } H \text{ in } G/H\} \longleftrightarrow \left\{\begin{array}{c}\text{isomorphisms}\\ \mathbb{L} \longrightarrow \overline{\mathbb{F}}\\ \text{fixing } \mathbb{F}\end{array}\right\} = \mathrm{Emb}(\mathbb{L}/\mathbb{F})$$

(v) $\mathbb{L}_1\mathbb{L}_2 \Leftrightarrow H_1\cap H_2$
$\mathbb{L}_1\cap\mathbb{L}_2 \Leftrightarrow \langle H_1,H_2\rangle$

comes from order-reversing nature of bijections

EXAMPLE:



$\mathrm{Emb}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})$ has 3 elements:

$= [S_3 : \langle(12)\rangle]$

$\alpha \longmapsto \alpha$

$\alpha \longmapsto \omega\alpha$

$\alpha \longmapsto \omega^2\alpha$

$\mathrm{Emb}(\mathbb{Q}(\omega), \overline{\mathbb{Q}})$ has 2 elements:

$= [S_3 : \langle(012)\rangle]$

$\omega \longmapsto \omega$

$\omega \longmapsto \omega^2$

proof of (iv):

We need to understand $\mathrm{Emb}(\mathbb{L}/\mathbb{F})$ when $\mathbb{L} = \mathbb{K}^H$.

$$\mathrm{Emb}(\mathbb{L}/\mathbb{F}) = \{\mathbb{L} \xrightarrow{\tau} \overline{\mathbb{F}}\}$$

$$\begin{tikzcd}[row sep=small] \overline{\mathbb{K}} = \overline{\mathbb{F}} \arrow[d, dash] \\ \mathbb{K} \arrow[d, dash] \\ \mathbb{L} \arrow[r, "\tau"] \arrow[d, dash] & \tau(\mathbb{L}) \arrow[ul, dash] \\ \mathbb{F} \end{tikzcd}$$

Pick $\overline{\mathbb{F}}$ containing $\mathbb{K}$:

Then we claim any $\mathbb{L} \xrightarrow{\tau} \overline{\mathbb{F}}$ has $\tau(\mathbb{L}) \subset \mathbb{K}$, because any $\alpha \in \mathbb{L}$ has $\alpha \in \mathbb{K}$, so $\tau(\alpha)$ is another root in $\overline{\mathbb{F}}$ of $m_{\alpha,\mathbb{F}}(x)$ in $\mathbb{F}[x]$, so $\tau(\alpha) \in \mathbb{K} = \mathrm{split}_{\mathbb{F}}(\{f_i\})$

We claim further that $\tau = \sigma|_{\mathbb{L}}$ of some $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F}) =: G$:

$\mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x))$ so $\mathbb{K} = \mathrm{split}_{\mathbb{L}}(f(x))$ and $\mathbb{K} = \mathrm{split}_{\tau(\mathbb{L})}(\tau f(x))$

so Iso Ext Thm gives

$$\begin{tikzcd} \mathbb{K} \arrow[r, dotted, "\exists \sigma"] \arrow[d, dash] & \mathbb{K} \arrow[d, dash] \\ \mathbb{L} \arrow[r, "\tau"] \arrow[d, dash] & \tau(\mathbb{L}) \arrow[d, dash] \\ \mathbb{F} \arrow[r, "1_{\mathbb{F}}"] & \mathbb{F} \end{tikzcd}$$

with $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = G$

$\sigma|_{\mathbb{L}} = \tau$

Finally $\sigma \in G = \mathrm{Aut}(\mathbb{K}/\mathbb{F})$
$\sigma' \in$

have $\sigma|_{\mathbb{L}} = \sigma'|_{\mathbb{L}}$ when $\mathbb{L} = \mathbb{K}^H$

$\iff \sigma H = \sigma' H$ since ...

$$\sigma|_{\mathbb{L}} = \sigma'|_{\mathbb{L}} \iff$$
$$\sigma^{-1}\sigma'|_{\mathbb{L}} = 1_{\mathbb{L}} \iff$$
$$\sigma^{-1}\sigma' \in \mathrm{Aut}(\mathbb{K}/\mathbb{L}) = H \iff$$
$$\sigma H = \sigma' H.$$

To prove (iii), note that

$$|\mathrm{Emb}(\mathbb{L}/\mathbb{F})| = [G:H] = [\mathbb{L}:\mathbb{F}]$$

and $\underset{\substack{\shortparallel \\ \{\tau \in \mathrm{Emb}(\mathbb{L}/\mathbb{F}) : \\ \tau(\mathbb{L}) = \mathbb{L}\}}}{\mathrm{Aut}(\mathbb{L}/\mathbb{F})} \leq \mathrm{Emb}(\mathbb{L}/\mathbb{F})$

Hence $\mathbb{L}/\mathbb{F}$ is Galois (using $|\mathrm{Aut}(\mathbb{L}/\mathbb{F})| \underset{\text{defn}}{=} [\mathbb{L}:\mathbb{F}]$)

$\iff$ every $\tau \in \mathrm{Emb}(\mathbb{L}/\mathbb{F})$ has $\tau(\mathbb{L}) = \mathbb{L}$

Hence $\mathbb{L}/\mathbb{F}$ is Galois

$\iff$ every $\tau \in \mathrm{Emb}(\mathbb{L}/\mathbb{F})$

has $\tau(\mathbb{L}) = \mathbb{L}$

This is equivalent to $H \; (= \mathrm{Aut}(\mathbb{K}/\mathbb{L})$, $\mathbb{L} = \mathbb{K}^H)$

being normal in G:

Recall $\tau = \sigma|_{\mathbb{L}}$ for some $\sigma \in G$,

and $\sigma(\mathbb{L})$ is the fixed subfield for $\sigma H \sigma^{-1}$:

$$\sigma(\mathbb{L}) = \mathbb{K}^{\sigma H \sigma^{-1}} \quad \text{if } \mathbb{L} = \mathbb{K}^H$$

$$\left(\begin{array}{l} h(\alpha) = \alpha \\ \iff \sigma h(\alpha) = \sigma(\alpha) \\ \iff \sigma h \sigma^{-1} \cdot \sigma(\alpha) = \sigma(\alpha) \end{array} \right)$$

so $\sigma(\mathbb{L}) = \mathbb{L} \quad \forall g \in G$

$$\Updownarrow$$

$\sigma H \sigma^{-1} = H \quad \forall g \in G$

$$\Updownarrow$$

$H \trianglelefteq G$ $\blacksquare$

§14.3 Finite fields

Let's play with an...

EXAMPLE

$$\mathbb{F}_{2^3} = \mathbb{F}_8 \cong \mathbb{F}_2[x]\,/\,(x^3+x+1) \quad \text{with } \beta := \bar{x}, \qquad \beta^3+\beta+1=0$$

(or x^3+x^2+1 would work)

= an $\mathbb{F}_2$-vector space on basis $\{1, \beta, \beta^2\}$

Inside

$$\mathbb{F}_8^\times = \{\underset{\beta^7}{\overset{\beta^0}{1}},\ \overset{\beta}{\beta^1},\ \beta^2,\ \underset{\beta+1}{\beta^3},\ \underset{\beta^2+\beta}{\beta^4},\ \underset{\beta+1+\beta^2}{\underset{\beta^3+\beta^2}{\beta^5}},\ \underset{\beta^2+1}{\underset{\beta^2+\beta+\beta^3}{\beta^6}}\}$$

Let's look at the orbits of $\boxed{\text{Frobenius } \mathbb{F}_8 \xrightarrow{F} \mathbb{F}_8,\ \alpha \mapsto \alpha^2}$

$F \in \mathrm{Aut}(\mathbb{F}_8/\mathbb{F}_2)$

$\mathbb{F}_2$: $0 \circlearrowleft F$, $\quad 1 \circlearrowleft F$

$\beta^8 = \beta \to \beta^2 \to \beta^4 \to \beta$

$\beta^{10} = \beta^3 \to \beta^6 \to \beta^{12} = \beta^5 \to \beta^3$

roots of ...

$$\underbrace{x(x+1)}_{\text{linear}}\ \underbrace{(x^3+x+1)\,(x^3+x^2+1)}_{\text{cubics}} = x^{2^3}-x = x^8 - x \quad \text{in } \mathbb{F}_2[x]$$

check: $x^3+x^2+1 = (x-\beta^3)(x-\beta^6)(x-\beta^5)$