Discriminants

- detecting separability
  and $\mathrm{Aut}(\mathbb{C}(K/\mathbb{Q}) < A_n < S_n$
  or not.

Let $\alpha_1, \ldots, \alpha_n$ be indeterminates (variables)

so $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ = rational functions $\dfrac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$

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

$$\in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)[x]$$

$$\in \mathbb{Z}[\alpha_1, \ldots, \alpha_n][x]$$

$$= x^n - \underbrace{(\alpha_1 + \cdots + \alpha_n)}_{\substack{s_1 := \\ \text{1st elementary} \\ \text{symmetric} \\ \text{function}}} x^{n-1} + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)}_{s_2} x^{n-2}$$

$$- \cdots + (-1)^n \underbrace{\alpha_1\alpha_2 \cdots \alpha_n}_{s_n}$$

$$\in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{S_n}[x]$$

PROP: $\mathbb{Q}(\alpha_1,\dots,\alpha_n)^{S_n} = \mathbb{Q}(s_1, s_2, \dots, s_n)$, where $s_1 = \alpha_1+\dots+\alpha_n$, $s_n = \alpha_1\alpha_2\cdots\alpha_n$

proof: Notice that

$$\mathbb{Q}(\alpha_1,\dots,\alpha_n) = \mathrm{Split}_{\mathbb{Q}(s_1,\dots,s_n)}(f(x))$$

$$\begin{tikzcd}
\mathbb{Q}(\alpha_1,\dots,\alpha_n) \arrow[dd, dash, "\text{finite of degree} \le n!"'] \arrow[dr, dash, "\deg\ |S_n| = n!"] & \\
& \mathbb{Q}(\alpha_1,\dots,\alpha_n)^{S_n} \arrow[dl, equal, "\text{must be equal!}"] \\
\mathbb{Q}(s_1, s_2,\dots,s_n) &
\end{tikzcd}$$

with $s_1 = \alpha_1+\dots+\alpha_n$, $s_n = \alpha_1\alpha_2\cdots\alpha_n$.

$$\begin{tikzcd}
\mathbb{K} \arrow[d, dash, "\text{Galois}", "{[\mathbb{K}:\mathbb{L}] = |H|}"'] \\
\mathbb{L} = \mathbb{K}^H \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

$$f(x) := (x-\alpha_1)\cdots(x-\alpha_n) \in \mathbb{Q}(s_1,\dots,s_n)[x]$$

$\blacksquare$

REMARK: In fact,

$$\mathbb{Z}[\alpha_1,\dots,\alpha_n]^{S_n} = \mathbb{Z}[s_1, s_2, \dots, s_n]$$

(see D&F Exer. 14.6 #37–43)

DEF'N:

Define $\sqrt{D} := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j) \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$

and $D := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$
$(\in \mathbb{Z}[\alpha_1, \ldots, \alpha_n])$

PROP: Every permutation $\sigma \in S_n$ has $\sigma(\sqrt{D}) = \underset{\pm 1}{\underset{\shortparallel}{\mathrm{sgn}(\sigma)}} \cdot \sqrt{D}$

and hence

- $\sigma \in A_n \iff \sigma(\sqrt{D}) = +\sqrt{D}$
- $\sigma \in S_n \iff \sigma(D) = D$

so $D \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{S_n}$
$= \mathbb{Q}(s_1, s_2, \ldots, s_n)$

and hence D has an expression in $\mathbb{Q}(s_1, s_2, \ldots, s_n)$ (even in $\mathbb{Z}[s_1, s_2, \ldots, s_n]$).

PROP: Every permutation $\sigma \in S_n$ has $\sigma(\sqrt{D}) = \underbrace{\mathrm{sgn}(\sigma)}_{= \pm 1} \cdot \sqrt{D}$

and hence

- $\sigma \in A_n \iff \sigma(\sqrt{D}) = +\sqrt{D}$
- $\sigma \in S_n \iff \sigma(D) = D$

proof: Every $\sigma \in S_n$ permutes the factors $\alpha_i - \alpha_j$ of $\sqrt{D}$ up to sign, and $\sigma_i = (i, i+1)$ negates $\sqrt{D}$:

e.g. $n=4$

$$\sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)$$

$\sigma_2 = (2, 3)$, with $2 = i$, $3 = i+1$

negated! $\alpha_3 - \alpha_2$

Since every σ_i negates $\sqrt{D}$,

$$\sigma(\sqrt{D}) = \mathrm{sgn}(\sigma)\sqrt{D} \quad \forall \sigma \in S_n.$$

∎

EXAMPLES:

① Quadratics $n=2$

$$f(x) = (x-\alpha_1)(x-\alpha_2) = x^2+bx+c$$

$$= x^2 - \underbrace{(\alpha_1+\alpha_2)}_{s_1}x + \underbrace{\alpha_1\alpha_2}_{s_2} \Rightarrow \begin{array}{l} b = -s_1 \\ c = s_2 \end{array}$$

Then $D = (\alpha_1-\alpha_2)^2$

$$= \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 \in \mathbb{Q}(\alpha_1,\alpha_2)^{S_2} = \mathbb{Q}(s_1,s_2)$$

$$= (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2$$

$$= s_1^2 - 4s_2$$

$$= b^2 - 4c \in \mathbb{Q}(s_1,s_2) \ (= \mathbb{Q}(b,c))$$

---

② Cubic $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$$= x^3 - s_1x^2 + s_2x - s_3$$

$$= x^3 + ax^2 + bx + c$$

has $D = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 \in \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)^{S_3}$

$$= \mathbb{Q}(s_1,s_2,s_3)$$

$$= \mathbb{Q}(a,b,c)$$

$$= \alpha_1^4\alpha_2^2 + \cdots$$

$$= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

THM: For any field $\mathbb{F}$ and any $f(x) \in \mathbb{F}[x]$ of degree n

$$\overset{\shortparallel}{x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0} \quad \text{with } a_i \in \mathbb{F},$$

one has (i) $\underset{(\in \mathbb{F})}{D} \neq 0 \iff f$ separable

i.e. roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$ are distinct in any splitting field $\mathbb{K}$ over $\mathbb{F}$ for f

(ii) D is a square in $\mathbb{F}$

$$\iff G = Gal(\underbrace{Split_{\mathbb{F}}(f)}_{\mathbb{K}}/\mathbb{F}) \leq A_n$$

EXAMPLES for quadratics

① $f(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$ has $D = 2^2 - 4 \cdot 1 = 0$

$= (x+1)^2$

② $f(x) = x^2 + 3x + 2$ in $\mathbb{Q}[x]$ has $D = 3^2 - 4 \cdot 2 = 1$
$= 1^2$ in $\mathbb{Q}$

$= (x+1)(x+2)$ $\quad G = \{1\} = A_2$
(since $\mathbb{K} = \mathbb{Q}$)

③ $f(x) = x^2 + 3x + 1$ in $\mathbb{Q}[x]$ has $D = 3^2 - 4 = 5$
not a square in $\mathbb{Q}$

$$= (x - \underbrace{\tfrac{-3+\sqrt{5}}{2}}_{\alpha_1})(x - \underbrace{\tfrac{-3-\sqrt{5}}{2}}_{\alpha_2}) \quad G = S_2 \quad \sqrt{5} \mapsto \pm\sqrt{5}$$

THM: For any field $\mathbb{F}$ and any $f(x) \in \mathbb{F}[x]$ of degree n

$$\overset{\shortparallel}{x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0} \quad \text{with } a_i \in \mathbb{F},$$

one has (i) $\underset{(\in \mathbb{F})}{D} \neq 0 \iff f$ separable

i.e. roots $\alpha_1, \dots, \alpha_n$ of $f(x)$ are distinct in any splitting field $\mathbb{K}$ over $\mathbb{F}$ for f

If $D \neq 0$, then

(ii) D is a square in $\mathbb{F}$

$$\iff G = \mathrm{Gal}(\underbrace{\mathrm{Split}_{\mathbb{F}}(f)}_{\mathbb{K}} / \mathbb{F}) \leq A_n$$

---

proof: Factor $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ where $\alpha_1, \dots, \alpha_n \in \underset{\mathrm{split}_{\mathbb{F}}(f(x))}{\overset{\shortparallel}{\mathbb{K}}}$

(i) Then $D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \mathbb{F}$

$$= \text{expression in } \underset{\pm a_{n-1}}{\overset{\shortparallel}{s_1}}, \underset{\pm a_{n-2}}{\overset{\shortparallel}{s_2}}, \dots, \underset{\pm a_0}{\overset{\shortparallel}{s_n}} \in \mathbb{F}$$

so $D \neq 0 \iff \alpha_i \neq \alpha_j \ \forall i \neq j$

i.e. f separable.

(ii) If $D \neq 0$, then $\sqrt{D} = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$

(ii) If $D \neq 0$, then $\sqrt{D} = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$

$\sqrt{D} \in \mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x))$ since $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$

$|$ ← Galois, since $f(x)$ is <u>separable</u> ($D \neq 0$!)

$\mathbb{K}^G = \mathbb{F}$

and hence $\overset{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}{\overset{\shortparallel}{G}} \leq A_n \iff$

every $\sigma \in G$ has $\sigma(\sqrt{D}) = \sqrt{D}$

$\iff \sqrt{D} \in \mathbb{K}^G = \mathbb{F}$

$\iff D$ is a perfect square in $\mathbb{F}$.

$\blacksquare$

§14.7 Solvability by radicals

Recall a group G was <u>solvable</u> if $\exists$ a <u>subnormal</u> series

$$\underset{\underset{H_0}{\|}}{G} \triangleright H_1 \triangleright H_2 \triangleright \ldots \triangleright H_{s-1} \triangleright \underset{\underset{\{1\}}{\|}}{H_s}$$

with H_i / H_{i+1} <u>abelian</u>

(and if G is finite, equivalent to say H_i/H_{i+1} <u>cyclic</u>).

<u>DEF'N</u>: $\mathbb{K}/\mathbb{F}$ is a (simple) <u>radical</u> extension if $\mathbb{K} = \mathbb{F}(\sqrt[n]{a})$ for some $a \in \mathbb{F}$.

Say α algebraic$/\mathbb{F}$ can be <u>expressed by radicals</u> if it lies in some <u>root extension</u>

i.e. some $\mathbb{K}/\mathbb{F}$ that lies atop a tower

$$\mathbb{F} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_{s-1} \subset \mathbb{K}_s = \mathbb{K} \ni \alpha$$

where each $\mathbb{K}_i / \mathbb{K}_{i-1}$ is a radical extension.

e.g. $\alpha = \sqrt[4]{1+\sqrt[5]{3-\sqrt[7]{2}+6\left(\sqrt[7]{2}\right)^3}} + 10$

$$\underset{\substack{\| \\ \mathbb{K}_0 \\ \| \\ \mathbb{F}}}{\mathbb{Q}} \overset{\text{radical}}{\text{---}} \underset{\substack{\| \\ \mathbb{K}_1}}{\mathbb{Q}(\sqrt[7]{2})} \overset{\text{radical}}{\text{---}} \overset{=\mathbb{K}_2}{\mathbb{Q}\left(\sqrt[7]{2}, \sqrt[5]{3-\sqrt[7]{2}+6(\sqrt[7]{2})^3}\right)}$$

$$\overset{\text{radical}}{\text{---}} \; \mathbb{K}_2(\alpha) = \mathbb{K}_2(\alpha - 10) = \mathbb{K} \ni \alpha$$

Say $f(x) \in \mathbb{F}[x]$ is <u>solvable by radicals</u> if all its roots (in $\overline{\mathbb{F}}$) can be <u>expressed by radicals</u> $/\mathbb{F}$.

Want to head toward...

<u>THM</u> (Galois) If $\mathrm{char}(\mathbb{F})=0$, then $f(x) \in \mathbb{F}[x]$ is solvable by radicals $\iff \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable (as a finite group) where $\mathbb{L} := \mathrm{split}_{\mathbb{F}}(f(x))$

EXAMPLE: $f(x) = x^2 + bx + c \in \mathbb{Q}(b,c)[x]$

is irreducible

but $f(x) = 0$ implies

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

we can factor it

$$f(x) = \Big(x - \underbrace{\frac{-b + \sqrt{b^2-4c}}{2}}_{\alpha_1 :=}\Big)\Big(x - \underbrace{\frac{-b - \sqrt{b^2-4c}}{2}}_{\alpha_2 :=}\Big)$$

where $\alpha_1, \alpha_2 \in \overbrace{\mathbb{Q}(\alpha_1, \alpha_2)}^{=\mathbb{L}} = \mathbb{Q}(\sqrt{D})$

$D := b^2 - 4c$

$$\begin{array}{c} \mathbb{Q}(\alpha_1,\alpha_2) \\ \Big| \\ \mathbb{Q}(b,c) = \mathbb{F} \end{array}$$

degree 2, a radical extension

i.e. the "general" quadratic is solvable by radicals and $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = S_2$ is solvable,

and same for general cubic
for general quartic } see §14.7

but not the general quintic.

EXAMPLE: Assuming Galois's Thm, then there are definitely explicit quintics e.g. $\boxed{f(x) = x^5 - 4x + 2}$ which are not solvable by radicals, because $\boxed{\mathrm{Gal}(\underset{\substack{\| \\ \mathrm{split}_{\mathbb{Q}}(f(x))}}{\mathbb{K}}/\mathbb{Q}) = S_5}$

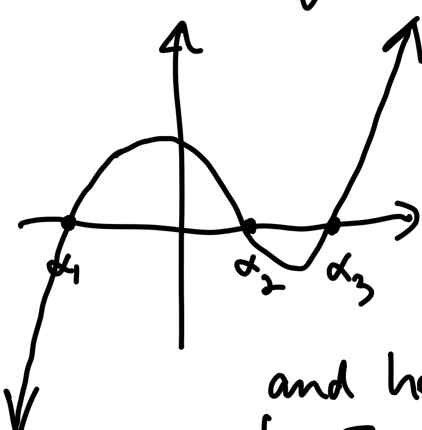
and we asserted or proved in 8201 that S_5, A_5 were not solvable groups

not solvable, since solvability is preserved by subgroup & quotient group.

simple

The group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is all of S_5 since...

we can graph $y = f(x)$ using calc techniques and deduce it has only 3 real roots $\alpha_1, \alpha_2, \alpha_3$ and two complex roots α_4, α_5 $(\alpha_5 = \overline{\alpha_4})$ in $\mathbb{C}$

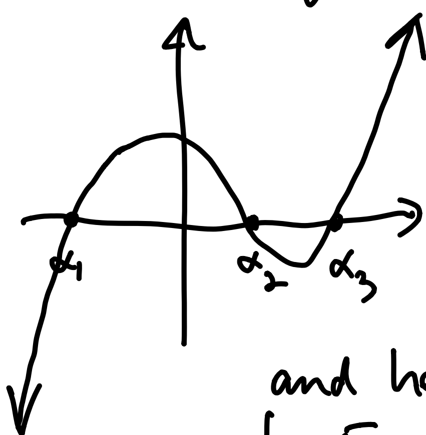


Since $\mathbb{K}/\mathbb{Q}$ has degree divisible by 5 (check $f(x) \in \mathbb{Q}[x]$ is irreducible via Eisenstein at $p=2$)

and hence G has order divisible by 5, and hence contains $\sigma \in S_5$ of order 5.

The group $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is all of S_5 since...

we can graph $y = f(x)$ using calc techniques and deduce it has only 3 real roots $\alpha_1, \alpha_2, \alpha_3$ and two complex roots α_4, α_5 $(\alpha_5 = \overline{\alpha_4})$ in $\mathbb{C}$



Since $\mathbb{K}/\mathbb{Q}$ has degree divisible by 5 (check $f(x) \in \mathbb{Q}[x]$ is irreducible via Eisenstein at $p=2$)

and hence G has order divisible by 5, and hence contains $\sigma \in S_5$ of order 5.

Hence G contains some 5-cycle $(ijklm)$, and it also contains the transposition $(\alpha_4\, \alpha_5)$ because $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \bar{z}$ restricts to $\mathbb{K}$ giving such an element of $G = \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$.

Conjugating (α_4, α_5) by the 5-cycle $(ijklm)$ gives enough transpositions to generate all of S_5.

Hence $G = S_5$.

GOAL:

THM (Galois) If $\mathrm{char}(\mathbb{F})=0$, then $f(x)\in\mathbb{F}[x]$ is solvable by radicals

$$\iff \mathrm{Gal}(\mathbb{L}/\mathbb{F}) \text{ is solvable (as a finite group)}$$

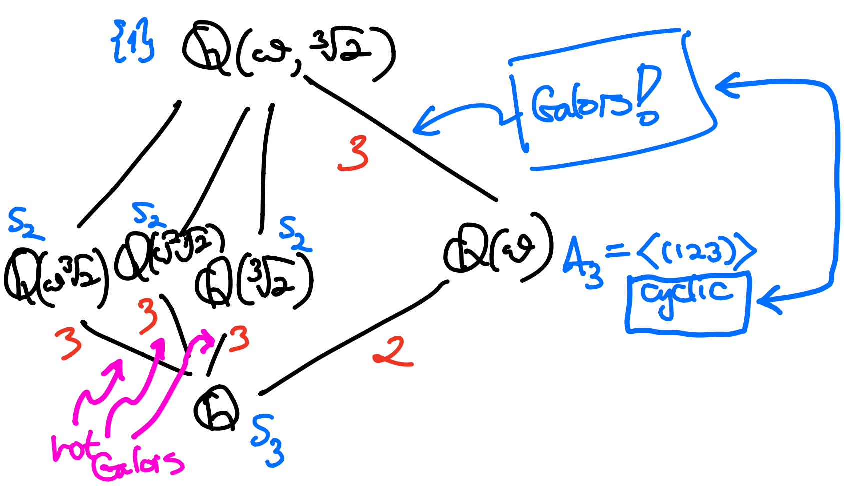
where $\mathbb{L} := \mathrm{split}_{\mathbb{F}}(f(x))$

---

3 issues

- root extensions aren't Galois always! $\mathbb{Q}(\sqrt[3]{2})$ | not Galois! $\mathbb{Q}$
- is its Galois closure still a root extension
- need to have roots of unity around to make radical extension $\iff$ cyclic extensions

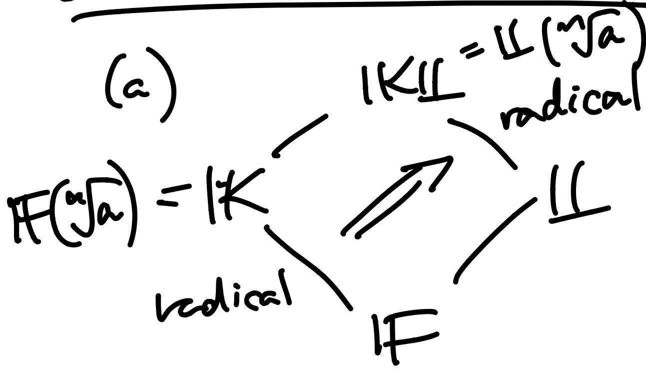
  ↑ cyclic Galois group

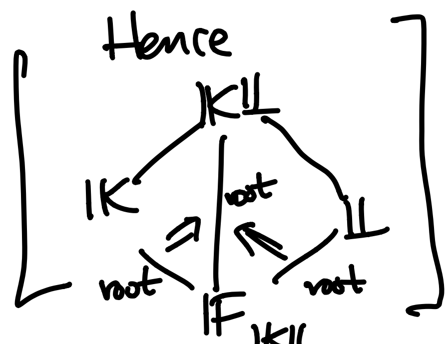


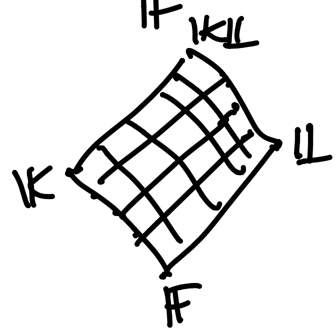
SOME EASY LEMMAS:

char(𝔽)=

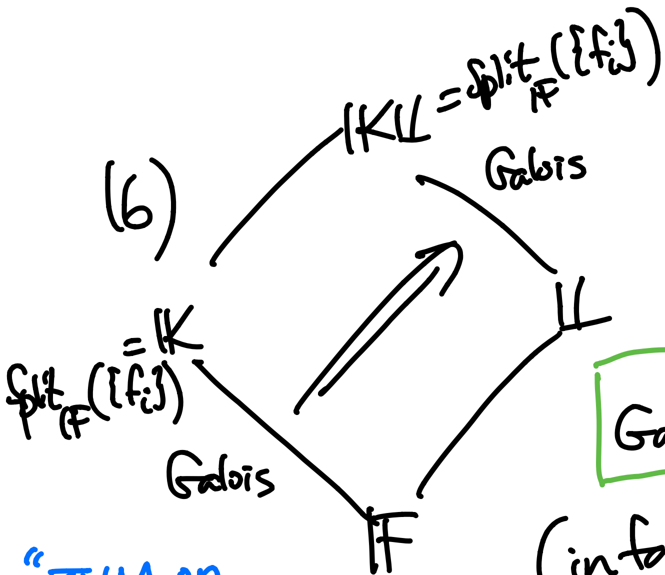
(a)







(b)

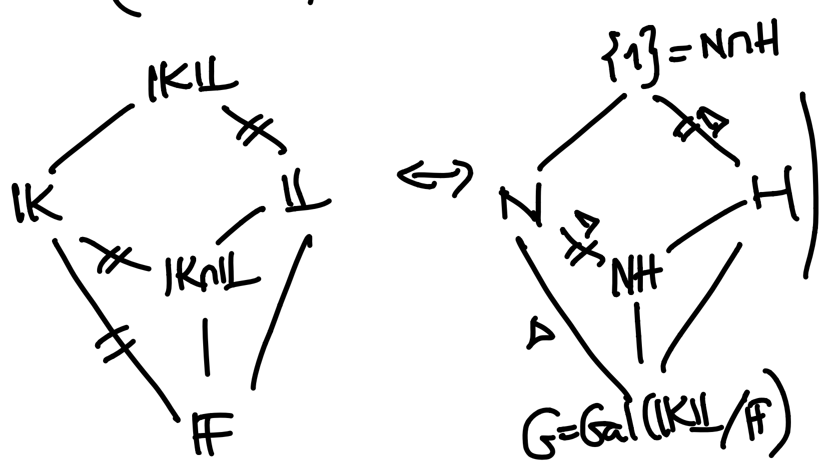


with

$$\boxed{\mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) \overset{(*)}{\leq} \mathrm{Gal}(\mathbb{K}/\mathbb{F})}$$

(in fact, $\mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) = H \cong \mathrm{Gal}(\mathbb{K}/\mathbb{K}\cap\mathbb{L})$)

"THM on natural irrationalities"



(c)

$$\begin{tikzcd}
 & \mathbb{K}\mathbb{L} = \mathrm{Split}_{\mathbb{F}}(\{f_i\}\cup\{g_j\}) \arrow[dl, dash] \arrow[dd, dash, "\text{Galois}"] \arrow[dr, dash] & \\
\mathrm{Split}_{\mathbb{F}}(\{f_i\}) = \mathbb{K} \arrow[dr, dash, "\text{Galois}"'] \arrow[r, phantom, "\Rightarrow"] & & \mathbb{L} = \mathrm{Split}_{\mathbb{F}}(\{g_j\}) \arrow[dl, dash, "\text{Galois}"] \arrow[l, phantom, "\Leftarrow"'] \\
 & \mathbb{F} &
\end{tikzcd}$$

<u>proof:</u> We only have left to prove this part of (b):

$$\begin{tikzcd}
 & \mathbb{K}\mathbb{L} \arrow[dl, dash] \arrow[dr, dash, "\text{Galois}"] & \\
\mathbb{K} \arrow[dr, dash, "\text{Galois}"'] \arrow[rr, phantom, "\Rightarrow"] & & \mathbb{L} \arrow[dl, dash] \\
 & \mathbb{F} &
\end{tikzcd}$$

with $\boxed{\mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) \overset{(*)}{\leq} \mathrm{Gal}(\mathbb{K}/\mathbb{F})}$

Given $\sigma \in \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) \leq \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{F})$,
$\sigma(\mathbb{K}) = \mathbb{K}$ because $\mathbb{K}$ is a normal extension of $\mathbb{F}$,
so we get a homomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) &\xrightarrow{\varphi} \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \\ \sigma &\longmapsto \sigma|_{\mathbb{K}} \end{aligned}$$

and it remains to show $\ker(\varphi) = \{1\}$.

$$\boxed{\mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) \overset{(*)}{\leq} \mathrm{Gal}(\mathbb{K}/\mathbb{F})}$$

Given $\sigma \in \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) \leq \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{F})$,
$\sigma(\mathbb{K}) = \mathbb{K}$ because $\mathbb{K}$ is a normal extension of $\mathbb{F}$,
so we get a homomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L}) &\xrightarrow{\varphi} \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \\ \sigma &\longmapsto \sigma|_{\mathbb{K}} \end{aligned}$$

and it remains to show $\ker(\varphi) = \{1\}$.

Given $\varphi(\sigma) = 1$, that says $\varphi|_{\mathbb{K}} = 1_{\mathbb{K}}$
but $\sigma|_{\mathbb{L}} = 1_{\mathbb{L}}$ since $\sigma \in \mathrm{Gal}(\mathbb{K}\mathbb{L}/\mathbb{L})$,
so $\sigma|_{\mathbb{K}\mathbb{L}} = 1_{\mathbb{K}\mathbb{L}}$, i.e. $\ker \varphi = \{1\}$. ∎

THE KUMMER LEMMA:

Assume $\mathrm{char}(\mathbb{K}) = 0$ and
$\mu_n := \left\{ \begin{array}{c} \text{all } n^{\text{th}} \text{ roots} \\ \text{of } 1 \end{array} \right\} \subset \mathbb{K}$. Then

(i) A radical extension $\mathbb{K}(\sqrt[n]{a})$ is always Galois, with Galois group $\mathbb{Z}/d\mathbb{Z}$ for some d dividing n.

(ii) Conversely, if $\mathbb{L}/\mathbb{K}$ Galois, with $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/d\mathbb{Z}$ for $d|n$, then $\mathbb{L} = \mathbb{K}(\sqrt[d]{a})$ for some $a \in \mathbb{K}$.

THE KUMMER LEMMA:

Assume $\mathrm{char}(\mathbb{K})=0$ and $\mu_n := \left\{ \begin{matrix} \text{all } n^{\text{th}} \text{ roots} \\ \text{of } 1 \end{matrix} \right\} \subset \mathbb{K}$. Then

(i) A radical extension $\mathbb{K}(\sqrt[n]{a})$ is always Galois, with Galois group $\mathbb{Z}/d\mathbb{Z}$ for some d dividing n.

(ii) Conversely, if $\mathbb{L}/\mathbb{K}$ Galois, with $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/d\mathbb{Z}$ for $d \mid n$, then $\mathbb{L} = \mathbb{K}(\sqrt[d]{a})$ for some $a \in \mathbb{K}$.

---

proof: (i): Since $\mu_n \subseteq \mathbb{K}$, $\mathbb{K}(\sqrt[n]{a}) = \mathrm{split}_{\mathbb{K}}(x^n - a)$ and hence Galois over $\mathbb{K}$ since $\mathrm{char}(\mathbb{K})=0$.

The map $\mathrm{Gal}(\mathbb{K}(\sqrt[n]{a})/\mathbb{K}) \xrightarrow{\varphi} \mu_n \leq \mathbb{C}^\times$

that takes $\sigma \longmapsto \dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta_n^j$ for some j and $\zeta_n = e^{2\pi i/n}$

This φ is a homomorphism since

if $\varphi(\sigma) = \zeta^j$ $(\zeta = \zeta_n)$ i.e. $\sigma(\sqrt[n]{a}) = \zeta^j \sqrt[n]{a}$

$\varphi(\tau) = \zeta^k$ $\qquad \tau(\sqrt[n]{a}) = \zeta^k \sqrt[n]{a}$

then
$$\begin{aligned}(\sigma \circ \tau)(\sqrt[n]{a}) &= \sigma(\tau(\sqrt[n]{a})) \\ &= \sigma(\zeta^k \sqrt[n]{a}) \\ &= \sigma(\zeta^k)\, \sigma(\sqrt[n]{a}) \\ &= \zeta^k \cdot \zeta^j \cdot \sqrt[n]{a}\end{aligned}$$

$\sigma = \mathbb{1}_{\mathbb{K}}$
$\mu_n \subset \mathbb{K}$

i.e. $\varphi(\sigma \circ \tau) = \zeta^k \cdot \zeta^j$

Once we know φ is a homomorphism,
it's injective since any $\sigma \in \mathrm{Gal}(\mathbb{K}(\sqrt[n]{a})/\mathbb{K})$
is completely determined by $\varphi(\sigma) = \zeta^j$
since it tells us $\sigma(\sqrt[n]{a}) = \zeta^j \cdot \sqrt[n]{a}$.

For (ii), if $\mathbb{L}/\mathbb{K}$ is Galois with
$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/d\mathbb{Z}$ and $d \mid n$, then
let $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \{1, \sigma, \sigma^2, \ldots, \sigma^{d-1}\} = \langle \sigma \rangle$
and pick a prim. d^{th} root of unity $\zeta_d =: \zeta$
and pick some $\alpha \in \mathbb{L}$ for which

$$\boxed{\beta := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{d-1}\sigma^{d-1}(\alpha)} \neq 0 \text{ in } \mathbb{L}$$

[Such an α exists, otherwise
$1 + \zeta\cdot\sigma + \zeta^2\cdot\sigma^2 + \ldots + \zeta^{d-1}\sigma^{d-1} : \mathbb{L}^\times \longrightarrow \mathbb{L}$
is the zero map, giving an $\mathbb{L}$-lin. dependence
among distinct characters $1, \sigma, \sigma^2, \ldots, \sigma^{d-1}$ on $\mathbb{L}^\times$]
contradicting Dedekind Lemma

Then $\sigma(\beta) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \ldots + \zeta^{d-2}\sigma^{d-1}(\alpha) + \zeta^{d-1}\alpha$
$= \zeta^{-1}\cdot\beta$

so $\sigma(\beta^d) = \sigma(\beta)^d = (\zeta^{-1}\cdot\beta)^d = \zeta^{-d}\cdot\beta^d = \beta^d$

i.e. $\beta^d \in \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$

Note also that $\beta \notin \mathbb{L}^H$ for any $H \subsetneq \langle\sigma\rangle$

since $\sigma(\beta) = \zeta^{-1}\cdot\beta$

so $\sigma^j(\beta) = \zeta^{-j}\cdot\beta \neq \beta$ if $j < d$.

Hence β generates $\mathbb{L}$ over $\mathbb{K}$, i.e.

$\mathbb{L} = \mathbb{K}(\beta) = \mathbb{K}(\sqrt[d]{a})$ where $a = \beta^d$. $\boxtimes$

<u>LEMMA</u>: When $\mathrm{char}(\mathbb{F}) = 0$, any α in a root extension $\mathbb{K}$ of $\mathbb{F}$, also lies in a root extension $\mathbb{F} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_s = \mathbb{K}$

where
- $\mathbb{K}/\mathbb{F}$ is Galois
- $\mathbb{K}_1/\mathbb{K}_0$ is cyclotomic $\mathbb{K}_1 = \mathbb{K}_0(\zeta_n)$ for some n.
- every $\mathbb{K}_{i+1}/\mathbb{K}_i$ is Galois with $\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i)$ cyclic iso. to $\mathbb{Z}/d_i\mathbb{Z}$ with $d_i \mid n$.

(so Kummer applies!)

LEMMA: when $\mathrm{char}(\mathbb{F})=0$, any α in a root extension $\mathbb{K}$ of $\mathbb{F}$, also lies in a root extension $\mathbb{F}=\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_s=\mathbb{K}$

where
- $\mathbb{K}/\mathbb{F}$ is Galois
- $\mathbb{K}_1/\mathbb{K}_0$ is cyclotomic $\mathbb{K}_1=\mathbb{K}_0(\zeta_n)$ for some n.
- every $\mathbb{K}_{i+1}/\mathbb{K}_i$ is Galois with $\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i)$ cyclic iso. to $\mathbb{Z}/d_i\mathbb{Z}$ with $d_i \mid n$.

(so Kummer applies!)

---

proof: Start with $\mathbb{F}=\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_s=\mathbb{K}$ $(*)$

and $\mathbb{K}_{i+1}=\mathbb{K}_i(\sqrt[n_i]{a_i})$ $a_i \in \mathbb{K}_i$

1st make $\mathbb{K}/\mathbb{F}$ Galois:

Let $\mathbb{L}$:= normal closure of $\mathbb{K}/\mathbb{F}$

$$= \mathbb{F}(\{\text{roots of } m_{\alpha,\mathbb{F}}(x) : \alpha \in \mathbb{K}\})$$

$$= \mathbb{F}(\{\sigma(\alpha) \text{ for } \alpha\in\mathbb{K} \text{ and } \sigma\in \mathrm{Gal}(\mathbb{L}/\mathbb{F})\})$$

$$= \mathbb{F}(\{\sigma(\mathbb{K}) : \sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{F})\})$$

$$= \text{compositum of } \{\sigma(\mathbb{K}) : \sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{F})\}$$

$$\begin{tikzcd} & \mathbb{L} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{K} \arrow[rr, "\sigma"] \arrow[dr, dash] & & \sigma(\mathbb{K}) \arrow[dl, dash] \\ & \mathbb{F} & \end{tikzcd}$$