4.6 Radical extensions (2nd lecture)

recall:

Lemma 4: $K \subset E \subset L$ finite s.t. all of E/K, L/E, L/K are Galois

$$\begin{array}{c} L \\ | \;\text{solv.} \\ E \\ | \;\text{solv.} \\ K \end{array} \qquad \text{solv.}$$

Then L/K is solvable if and only if

both L/E and E/K are solvable.

Lemma 5: $K(a)/K$ simple radical

$\sigma : K(a) \to \bar{F}$ s.t. $\sigma(K) \subset F$ for some field F

Then $F(\sigma(a))/F$ is simple radical.

$$\begin{tikzcd} K(a) \arrow[r, "\sigma"] \arrow[d, dash, "\text{simp. rad.}"'] & F(\sigma(a)) \arrow[d, dash, "\text{simp. rad.}"] \\ K \arrow[r, "\sigma|_K"'] & F \end{tikzcd}$$

Thm 7: L/K separable, finite

Then L/K is contained in a radical extension

if and only if L^{norm}/K is solvable.

proof: last lecture: "$\Leftarrow$"; missing: "$\Rightarrow$":

- Assume that there is a radical tower

$$K = F_0 \subset \ldots \subset F_s$$

s.t. $L \subset F_s$ where $F_i = F_{i-1}(a_i)/F_{i-1}$ is

simple radical. Consider $F_s \subset \bar{K}$ as a subfield.

- Let $\sigma_1 = id_{F_s}, \ldots, \sigma_r : F_s \xrightarrow{\quad} \bar{K}$ be all

$$\begin{tikzcd} F_s \arrow[rr] & & \bar{K} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

embeddings. By Lemma 5, the successive

adjunction of the elements

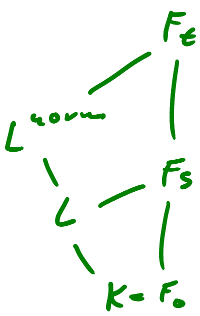
$\sigma_1(a_1), \sigma_1(a_2), \ldots, \sigma_1(a_s), \sigma_2(a_1), \ldots, \sigma_r(a_s)$

yields a radical tower $(t = rs)$

$$K = F_0 \subset \ldots \subset F_s \subset F_{s+1} = F_s(\sigma_2(a_1)) \subset \ldots \subset F_t = K(\sigma_j(a_i))_{\text{all } i,j}$$

Then F_t/K is a normal closure of F_s/K

since $\{\sigma_j(a_i)\}_{j=1\ldots r}$ are all roots of Mipo_{a_i}.



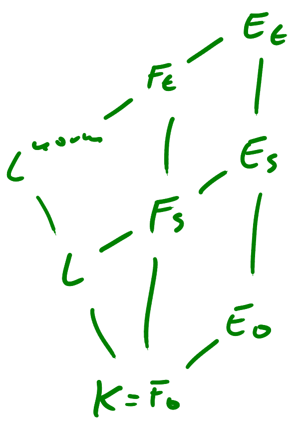
Since $a_1 \ldots a_s$ are separable over K,

all $\sigma_j(a_i)$ are separable over K,

and thus F_t/K is finite Galois.

Since $L \subset F_s$, we have $L^{norm} \subset F_t$.

- Let n be the largest divisor of $[F_t : K]$ that is not divisible by char K. Consider



$$E_0 = F_0(\zeta_n) \subset \ldots \subset E_t = F_t(\zeta_n).$$

By Lemma 5, E_i/E_{i-1} is simple radical for $i = 1 \ldots t$, i.e. $E_i = E_{i-1}(a_i')$ for a root $a_i' \in E_i$ of a polynomial of the form $f_i = T^{n_i} - b_i$ (char $K \nmid n_i$)

or $f_i = T^p - T - b_i$ (char $K = p$)

→ $\underline{g_i = T^{n_i} - s_i}$: $\quad \operatorname{char} K \nmid [E_i : E_{i-1}] \,\big|\, [E_t : K]$

$\quad \Rightarrow [E_i : E_{i-1}] \,|\, n$

$\quad \Rightarrow E_i / E_{i-1}$ is Kummer (Thm. 4.5.1)

→ $\underline{g_i = T^p - T - s_i}$: $\quad E_i / E_{i-1}$ is Artin-Schreier (Thm. 4.5.2)

$\Rightarrow$ In either case, E_i / E_{i-1} is cyclic.

Thus

$$\{e\} = \operatorname{Gal}(E_t/E_t) \triangleleft \underset{\operatorname{Gal}(E_t/E_{t-1})}{\operatorname{Gal}(E_t/E_{t-1})} \triangleleft \ldots \triangleleft \underset{\operatorname{Gal}(E_1/E_0)}{\operatorname{Gal}(E_t/E_0)}$$

is a normal series with cyclic factors

$$\operatorname{Gal}(E_i/E_{i-1}) = \operatorname{Gal}(E_t/E_{i-1}) / \operatorname{Gal}(E_t/E_i)$$

$\Rightarrow E_t / E_0$ is solvable.

$$\begin{tikzcd}
 & E_t \arrow[d, dash, "\text{solvable}"] \\
L^{\text{norm}} \arrow[ur, dash] \arrow[r, "\text{norm}"] \arrow[dr, dash, "\text{solvable}"'] & E_0 = K(\zeta_n) \arrow[d, dash, "\text{solvable}"] \\
 & K
\end{tikzcd}$$

By Thm. 4.3.2, $E_0 = K(\zeta_n)/K$ is abelian

$\Rightarrow E_t / K$ solvable (Lemma 4)

$\Rightarrow L^{\text{norm}} / K$ solvable (Lemma 4). $\square$

<u>Thm 8</u> (Galois' solvability theorem)

$\operatorname{char} K = 0$

$f = \sum c_i T^i \in K[T]$

$a_1, \ldots, a_n \in \overline{K}$ roots of f

$L = K(a_1, \ldots, a_n)$ splitting field of f/K

If L/K is <u>not</u> solvable, then there is <u>no</u> formula for the a_j in the c_i in terms of $+, -, \cdot, /$ and $\sqrt[n]{\ }$.

proof: If there was such a formula, then adjoining n-th roots $\sqrt[n]{s}$ would yield a radical tower

$$K = E_0 \subset \ldots \subset E_r$$

s.t. $L \subset E_r \Rightarrow L/K$ is solvable by Thm. 7. ↯ □

Def: L/K

$a_1 \ldots a_n \in L$

L is a <u>rational function field in $a_1 \ldots a_n$ over K</u>

if

$$K[T_1 \ldots T_n] \longrightarrow L$$
$$T_i \longmapsto a_i$$

is injective and the induced map

$$\mathrm{Frac}(K[T_1 \ldots T_n]) \longrightarrow L$$

is an isomorphism.

<u>Thm 9</u> (Abel)

$K = k_0(c_0 \ldots c_{n-1})$ rat. fct. field in $c_0 \ldots c_{n-1}$ over k_0

$f = T^n + c_{n-1}T^{n-1} + \ldots + c_0 \in K[T]$

L splitting field of f over K

$a_1 \ldots a_n \in L$ roots of f $\left(= \prod_{i=1}^{n} (T - a_i) \in L[T]\right)$

Assume that $k_0(a_1 \ldots a_n)$ is a rat. fct. field in $a_1 \ldots a_n$ over k_0. Then $\mathrm{Gal}(L/K) \simeq S_n$.

In particular, if $\mathrm{char}\, K = 0$ and $n \geq 5$, then L is not contained in any radical extension of K.

Rem: It follows from the theory of transcendence bases (section 5.2) that $K_0(a_1 \ldots a_n)$ is always a rat. fct. field over K_0.

proof: $f = T^n + c_{n-1}T^{n-1} + \ldots + c_0 = \prod (T - a_i)$ in $L[T]$

$\Rightarrow c_i = (-1)^i \sum\limits_{1 \le e_1 < \ldots < e_i \le n} a_{e_1} \cdot \ldots \cdot a_{e_i}$

injective by hypothesis

$\Rightarrow c_0 \ldots c_{n-1} \in K_0[a_1 \ldots a_n] = \mathrm{im}\left(K_0[T_1 \ldots T_n] \to L\right)$, $T_i \mapsto a_i$

$\Rightarrow L \simeq \mathrm{Frac}\left(K_0[T_1 \ldots T_n]\right)$

$\Rightarrow$ every permutation of $\{a_1 \ldots a_n\}$ induces a unique $\sigma : L \to L$ (over K_0).

Since $\sigma(c_i) = c_i$, $\sigma|_K = \mathrm{id}_K$

$\Rightarrow S_n < \mathrm{Aut}_K(L)$ and $K \subset L^{S_n}$

claim: $[L:K] \le n!$

Consider

$$K \subset K(a_1) \subset \ldots \subset K(a_1 \ldots a_n) = L$$

Then a_1 is a root of $f_1 = f$, and for $i \ge 2$, a_i is a root of

$$f_i = \frac{f}{(T-a_1)\cdots(T-a_{i-1})} = \frac{f_{i-1}}{T-a_{i-1}},$$

which is in $K(a_1 \ldots a_{i-1})[T]$ since $(T - a_{i-1}) \mid f_{i-1}$.

Since $\deg q_i = n-(i-1)$,

$$[L:K] = \prod_{i=1}^{n} [K(a_1 \ldots a_i) : K(a_1 \ldots a_{i-1})]$$
$$\leq \prod_{i=1}^{n} \deg q_i = n!$$

Thus the claim. ✓

- By Artin's theorem (Thm. 3.3.3), L/L^{S_n} is Galois with Galois group S_n.

$\Rightarrow$ $n! = \# S_n = [L:L^{S_n}] \leq [L:K] \leq n!$

$\Rightarrow$ $K = L^{S_n}$ and L/K Galois with

$Gal(L/K) = S_n$.

- By Thm. 4.2.1, S_n is not solvable for $n \geq 5$. Thus the last claim of the theorem follows from Thm. 7. $\square$

<u>Ex:</u> $f = T^5 - 4T + 2 \in \mathbb{Q}[T]$

L splitting field of f

<u>claim:</u> $G = Gal(L/\mathbb{Q}) = S_5$

- $a_1 \ldots a_5 \in L$ roots of $f = \prod_{i=1}^{5} (T - a_i)$

$\Rightarrow$ $G \curvearrowright \{a_1 \ldots a_5\}$ yields $\iota : G \hookrightarrow S_5$.

- f irreducible in $\mathbb{Z}[T]$ (Eisenstein criterion for 2)

$\Rightarrow$ f irreducible in $\mathbb{Q}[T]$ (Gauß Lemma)

· Thus

$$\mathbb{Q} \subset \underset{(\text{deg. } 5)}{\mathbb{Q}[T]/(f)} \cong \mathbb{Q}(a_1) \subset L$$

$\Rightarrow 5 \mid [L:\mathbb{Q}] = \#G$, but $5^2 \nmid \#G$

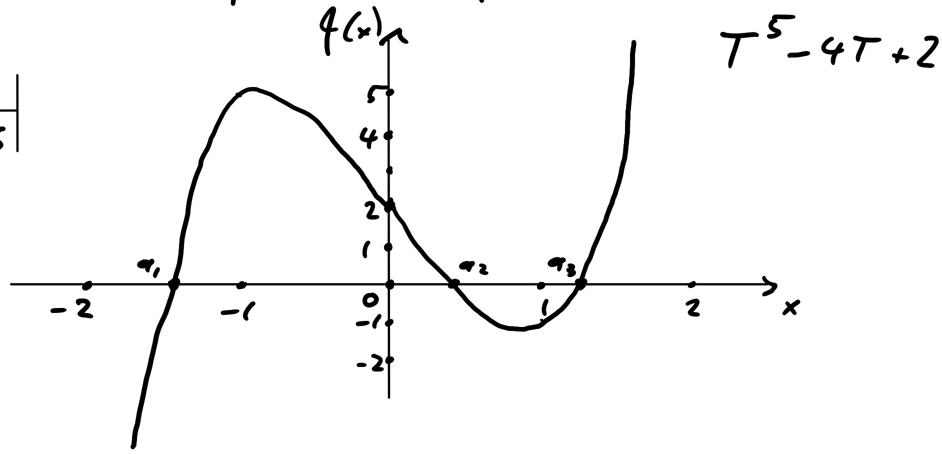
$\Rightarrow G$ has a 5-Sylow subgroup (Sylow's thm.)

$\Rightarrow \exists\, \sigma \in G$ of order 5

$\Rightarrow z(\sigma) \in S_5$ is a 5-cycle

· Consider f as a function $f: \mathbb{R} \to \mathbb{R}$:

x	-2	-1	0	1	2
$f(x)$	-22	5	2	-1	26



Note that $f' = 5T^4 - 4$ has 2 real zeros $\pm \sqrt[4]{4/5} \rightsquigarrow$ 2 local extrema

· By the intermediate value thm.,

$f: \mathbb{R} \to \mathbb{R}$ has 3 real roots, say $a_1, a_2, a_3 \in \mathbb{R}$

and thus 2 complex roots $a_4, a_5 \in \mathbb{C} - \mathbb{R}$

· $L \hookrightarrow \mathbb{C} \overset{\tau}{\circlearrowleft}$ complex conj yields an automorphism $\tau: L \to L$ of order 2.
$\quad\setminus_{\mathbb{Q}}/$

$\Rightarrow z(\tau) \in S_5$ is a transposition

· Since $S_5 = \langle 5\text{-cycle}, 2\text{-cycle} \rangle$, $G = S_5$. ⚡