4/15

Monday, April 15, 2019 11:34

$$\begin{tikzcd} K \arrow[d, no head] & \\ L \arrow[d, no head] & \tilde{L} \arrow[dl, no head] \\ F & \end{tikzcd}$$

K/L, L/F separable

$\Longrightarrow$ K/F separable.

$F[x_1, \dots, x_n] \circlearrowleft S_n$ by $\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

f is symmetric if $S_n \cdot f = \{f\}$.

elementary symmetric pol-ls

$$\underset{\displaystyle s_1}{\underset{\shortparallel}{x_1 + \cdots + x_n}}, \quad \underset{\displaystyle s_2}{\underset{\shortparallel}{\sum_{i<j} x_i x_j}}, \quad \underset{\displaystyle s_3}{\underset{\shortparallel}{\sum_{i<j<k} x_i x_j x_k}}, \quad \dots, \quad \underset{\displaystyle s_n}{\underset{\shortparallel}{x_1 \cdots x_n}}$$

<u>Theorem</u>: For any symmetric polynomial f,

$f = g(s_1, \dots, s_n)$ where $g \in F[y_1, \dots, y_n]$.

Examples

① $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2(x_1x_2) = s_1^2 - 2s_2.$

② $(x_1 - x_2)^2 = s_1^2 - 4s_2$

③ $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$

Consider $K = F(x_1, \dots, x_n)$ – rat'l f-ns in $x_1, \dots, x_n$.

Let $L = F(s_1, \dots, s_n) \subseteq K$.

Let $\tilde{L}$ be the subfield of symmetric rational fns.

Then $L \subseteq \tilde{L}$. $S_n \circlearrowright K$, $\tilde{L} = \mathrm{Fix}(S_n)$.

So $[K : \tilde{L}] = |S_n| = n!$.

But $x_1, \dots, x_n$ are the roots of the pol-l

$f = (X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots \pm s_n \in L[X].$

So K is the spl. field of f and $[K : L] \le n!$

$$\begin{array}{l} K \\ \Big| \; n! \\ \tilde{L} \longrightarrow \text{must be } 1, \text{ so } \tilde{L} = L. \\ \Big| \\ L \end{array} \quad (\le n! \text{ from } K \text{ to } L)$$

So for any $h \in \tilde{L}$ (symm, rat'l fns), $h = g(s_1, \dots, s_n)$ for some $g \in F(y_1, \dots, y_n)$.

<u>Corollary</u>: $\mathrm{Gal}(K/L) = \mathrm{Gal}(K/\tilde{L}) \cong S_n$.
$\qquad\qquad\quad \| $
$\qquad\quad \mathrm{Gal}(f)$.

f is "general polynomial of degree n"

$(G \circlearrowright K,\ L = \mathrm{Fix}(G) \Rightarrow \mathrm{Gal}(K/L) = G)$.

Solutions of polynomial eqns in Radicals

<u>Def</u> a Radical Extension is $F(\sqrt[n]{a})/F$ for some $a \in F$

(aka root extension, simple radical extension)

Def A *cyclic extension* is a Galois extension whose Galois group is cyclic.

Theorem Assume that $\omega \in F$, where ω is a primitive root of degree n. (all roots of unity are in F, $x^n - 1$ splits).

$\left(\{\text{roots of unity}\} = \langle \omega \rangle \right)$

Then any radical extension $F(\sqrt[n]{a})/F$ is cyclic.

Proof conjugates of $\alpha = \sqrt[n]{a}$ are $\omega^k \alpha$ for some k, all are in $F(\alpha)$. $\forall\ \varphi \in Gal(F(\alpha)/F)$,

$$(\varphi = \varphi_k)(\alpha) = \omega^k \alpha \quad \text{for some } k,$$

$$(\varphi_k \circ \varphi_\ell)(\alpha) = \omega^\ell(\omega^k \alpha) = \omega^{\ell+k}\alpha,$$

so $\varphi_k \longleftrightarrow k$ is an injetive hom-sm

$Gal(F(\alpha)/F) \cong \mathbb{Z}_n$, so $Gal(F(\alpha)/F)$ is cyclic of order n.

Somewhat **Conversely** Assume that $\omega \in F$ where ω is a primitive root of unity of degree n ($\omega^k \neq 1\ \forall\ k < n$).

Then $\forall$ cyclic extension K/F of degree n, K/F is a radical extension,

$K = F(\alpha)$ where $\alpha^n \in F$.

<u>Proof</u> Let K/F be cyclic, let $Gal(K/F) = \langle \varphi \rangle$, $\varphi^n = 1$.

Lagrange resolvent: $\forall \beta \in K$,

let $(\beta, \omega) = \beta + \omega \varphi(\beta) + \cdots + \omega^{n-1} \varphi^{n-1}(\beta)$.

Then $\varphi((\beta, \omega)) = \varphi(\beta) + \omega \varphi^2(\beta) + \cdots + \omega^{n-1} \varphi^n(\beta)$

$= \omega^{-1} (\beta, \omega)$.

So $\varphi((\beta, \omega)^n) = \omega^{-n} (\beta, \omega)^n = (\beta, \omega)^n$,

so $(\beta, \omega)^n$ is fixed by $\langle \varphi \rangle = Gal$.

So $(\beta, \omega)^n \in F$.

Also, $\forall k < n$, $\varphi^k((\beta, \omega)) = \omega^{-k} (\beta, \omega) \neq (\beta, \omega)$. if $(\beta, \omega) \neq 0$.

So (β, ω) is not fixed by any nontrivial element of Gal, if $(\beta, \omega) \neq 0$.

<u>Lemma</u>: $\exists \beta \in K$ s.t. $(\beta, \omega) \neq 0$.

So $\deg(\beta, \omega) = n$, let $\alpha = (\beta, \omega)$,

then $K = F(\alpha)$, $\alpha^n \in F$. $\square$

proof of lemma: $1, \varphi, \ldots, \varphi^{n-1}$ – distinct aut-sms of K/F.

Fact: they are linearly independent.

So $\forall$ coefficients $a_0, \ldots, a_{n-1}$

there is some β s.t.

$$a_0 \beta + a_1 \varphi(\beta) + \cdots + a_{n-1} \varphi^{n-1}(\beta) \neq 0.$$

In particular, take $a_k = \omega^k$. $\square$

In the proof, we needed $\omega^k \neq 1$ $\forall k < n$.

So we need $\operatorname{char} F \nmid n$.

So we henceforth assume $\operatorname{char} F = 0$

or $\operatorname{char} F >$ all degrees that will appear.

If F contains all roots of 1,

then radical extensions = cyclic extensions.

<u>Defn</u> Call an extension polyradical if it is a tower of radical extensions

$$\begin{array}{ll} \bullet & \ni \alpha \\ | & \\ \vdots & \\ | & \\ K_2 & \sqrt{b+\sqrt{a}} + 2\sqrt{a} \\ | & \\ K_1 & \\ | & \sqrt{a} \\ F & \end{array}$$

<u>Defn</u> Call an extension polycyclic if it is contained in a Galois extension whose Galois group is polycyclic:

$$1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = \mathrm{Gal}$$

s.t. $\forall i$, G_i/G_{i-1} is cyclic.

<u>Fact</u>: Finite Groups are polycyclic iff they are solvable.