Abel's Theorem

F char 0 field.
$f(x) \in F[x]$ irr. poly.
K/F the splitting field.
$G = \mathrm{Aut}(K/F)$.

Thm: The following are eqv.

① a root of $f(x)$ is a nested radical over F.

② all roots of $f(x)$ are nested radicals over F

③ G is solvable.

Nested radical

$\alpha \in K$ is a nested radical if there is a chain

$$F_0 = F \subset F_1 \subset \dots \subset F_n$$

with $\alpha \in F_n$ and

$$F_{i+1} = F_i[a_i]$$

where a_i is a p^{th} root of an element of F_i

that is $a_i^p \in F_i$

for some prime p.

(eqv. to yesterday's def)

Key : Understand p^{th} root extensions

F, $a \in F$ adjoin $a^{1/p}$
i.e. a root of $x^p - a$.

↳ "Kummer theory"

Setup : F char 0
p prime number.

Assume F contains all p^{th} roots of 1.

i.e. $x^p - 1$ splits into linears over F.

Prop: $X^p - 1$ has distinct roots in F.

Pf: $\gcd(X^p - 1, pX^{p-1}) = 1$

Roots of $X^p - 1 \subset F^\times$ is a subgp of size p

$\Rightarrow$ must be cyclic.

& any $\zeta \neq 1$ with $\zeta^p = 1$ generates it.

ζ is one p^{th} root of 1

$\zeta \neq 1$ then the others are

$1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$.

F containing p^{th} roots of 1

Take $a \in F$

<u>Thm</u>: We have the two possibilities

① $a = b^p$ for some $b \in F$

then
$$x^p - a = (x-b)(x-\zeta b)\cdots(x-\zeta^{p-1} b)$$

② $x^p - a$ is irreducible

& its Galois gp is cyclic of order p.

Say K/F is a splitting field & $b \in K$ is a root of $x^p - a$

then

$$X^p - a = (X-b)(X-b\zeta)\cdots(X-b\zeta^{p-1})$$

in $K[x]$ and the Galois group acts by

$$b \mapsto b\cdot\zeta^i$$

for $i=0,1,\ldots,p-1$

Proof: Say a is not a pth power in F.

Let K/F be a splitting field of $X^p - a$.

Let $b \in K$ be a root of $X^p - a$. Then the roots are $b, b\zeta, \ldots, b\zeta^{p-1} \in K$.

$$(X^p - a) = (X-b)(X-b\zeta)\cdots(X-b\zeta^{p-1})$$

$G = \mathrm{Gal}(K/F)$.

We see $K = F[b]$

$g \in G$ is determined by where it sends b.

Say $g \neq 1$, $g : b \mapsto \zeta^i b$

$i \not\equiv 0 \bmod p$. $\exists j$ s.t. $ij \equiv 1 \bmod p$

$h = g^j$ sends $b \mapsto \zeta b$.

$$
\begin{tikzcd}
b \arrow[r, "h"] & \zeta b \arrow[r, "h"] & \zeta^2 b \arrow[d, dotted] \\
\zeta^{p-1} b \arrow[u, "h"] & {} \arrow[l, "h"] & {} \arrow[l]
\end{tikzcd}
$$

$\Rightarrow$ All roots in one orbit.

$\Rightarrow$ $x^p - a$ is irreducible. $/F$.

$\Rightarrow$ b has deg p

$\Rightarrow$ K/F is of deg p

$\Rightarrow$ G is cyclic of order p

Converse: F char 0

contains p^{th} roots 1.

Suppose K/F is Galois of deg p ($\Rightarrow G = \mathrm{Aut}(K/F)$ is cyclic)

Then $\exists\ b \in K,\ b \notin F$ with $a = b^p \in F$.

Then $K = F[b]$

and b is a root of

$X^p - a$.

Pf: K/F Galois

$$G = \mathrm{Aut}(K/F) \cong \mathbb{Z}/p\mathbb{Z}.$$

Need $b \in K$ s.t. $b \notin F$

& $b^p \in F$.

Take $\sigma \in G$ a generator.

$\sigma : K \longrightarrow K$ fixing F.

K is an F-vector space

σ is F-linear:

$$\sigma(f_1 k_1 + f_2 k_2)$$

$$= \sigma(f_1 k_1) + \sigma(f_2 k_2)$$

$$= \sigma(f_1)\sigma(k_1) + \cdots$$

$$= f_1 \sigma(k_1) + f_2 \sigma(k_2)$$

Pf: $\sigma^p = id$.

eigenvalues of σ must be pth roots of unity $\in F$.

$\sigma \neq id$.

Linear algebra $\Rightarrow \exists$ eigenvector whose e-g value is ζ^i for $i \not\equiv 0 \pmod p$.

$b \in K$ is a such eigen vector.

$\sigma(b) = \zeta^i b \qquad b \notin F$

$\sigma(b^p) = b^p \in F$.

$\square$

V an F-vector space of fin dim

$\sigma : V \to V$ linear $\sigma \neq id$

s.t. $\sigma^p = id$

then σ has an eigenvectors with e-value ζ^i.

$$X^p - 1 = (X-1) \cdot (X-\zeta)(X-\zeta^2) \cdots (X-\zeta^{p-1})$$

$$(\sigma^p - id) = 0.$$

$$= (\sigma - id)(\underline{\sigma - \xi \cdot id}) \cdots (\underline{\sigma - \xi^{p-1} \cdot id})$$

Want $\sigma - \xi^i \cdot id$ has a Kernel.

$\sigma \neq id \Rightarrow$ at least one of the factors $(\sigma - \xi^i \cdot id)$ must be non invertible $\Rightarrow$ has a Kernel.