Kummer's thm

Assume char 0. Let p be a prime & F a field that contains p^{th} roots of 1. Then the following are eqv.

1. $F \subset K$ Galois of deg p
2. $K \cong F[x]/(x^p - b)$ for some $b \in F$ not a p^{th} power.

identity on F.

Pf $1 \Rightarrow 2$. Let $\sigma \in \mathrm{Aut}(K/F)$ be a generator.

Enough to show $\exists$ $a \in K$ s.t. $\sigma(a) = \zeta_p^i a$, $i \in \{1, 2, \ldots, p-1\}$

Set $b = a^p \in F$ Then min poly of a is $x^p - b$.

$\Leftrightarrow$ $\sigma : K \to K$ has eigenvalue ζ_p^i for some $i \in \{1, \ldots, p-1\}$

Ex. $F[\alpha,\beta,\gamma] \supset F[\sqrt{\Delta}]$ $G = A_3$ = cyclic perms.

$\sigma = (\alpha\beta\gamma)$

Taking α,β,γ as a basis $\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

$\sigma : K \to K$ linear map $\sigma: F^p \to F^p$

Let $F \subset L$ be an ext^n. s.t. char poly of σ splits in L.

We know $\sigma^p = Id. \Rightarrow$ Eigenvalues of σ are p^{th} roots of unity. $\Rightarrow$ L was unnecessary ($F = L$ suffices).

Use Cayley-Hamilton Thm: A matrix satisfies its own char poly.

Rule out: char poly of σ is $(X-1)^p$, suppose it is.

σ satisfies $(X-1)^p = 0$ & $X^p - 1 = 0 \Rightarrow$ satisfies $\gcd((X-1)^p, X^p-1) = 0$

$\Rightarrow$ satisfies $X - 1 = 0$. contradiction. because $\sigma \neq id$.

$\square$

② $\Rightarrow$ ① $\quad b \in F$ not a pth power.

<u>Want</u>: $\underline{X^p - b \text{ is irred.}}$ ✓ $\quad F[x]/(x^p - b)$ is <u>Galois</u> of deg. ~~order~~ p

Let $F \subset K$ be a splitting field of

$$X^p - b.$$

Let $a \in K$ be a root. We show a has deg p over F.

$\Rightarrow X^p - b$ is its min poly $\Rightarrow X^p - b$ is irred.

$$\text{Degree of } a = \# \underbrace{\text{Galois conjugates of } a}_{\text{Orbit of } a \text{ under } G = \mathrm{Aut}(K/F).}$$

Take $\sigma \in G$ that does not fix a.

Then $\sigma(a) = \zeta_p^i \cdot a$ for some $i \in \{1, \dots, p-1\}$.

$$a \overset{\sigma}{\longmapsto} \zeta_p^i a \overset{\sigma}{\longmapsto} \zeta_p^{2i} a \; \cdots$$ gives p Galois conj of a.

$\Rightarrow \deg(a/F) \geq p$ but also $\leq p$ $\quad a$ sat $\underline{\underline{X^p - b.}}$

Then $F[x]/(x^p-b)$ is the splitting field of x^p-b

$\Rightarrow$ Galois. & also of deg p.

$\square$.

$\underbrace{F \subset K}_{p^{th}\text{ root ext.}} \iff$ Gal. gp is $\mathbb{Z}/p\mathbb{Z}$.

Given $F \subset K$ Galois can we find

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset K = F_k$$

where $F_i \subset F_{i+1}$ is a p_i^{th} root ext. $\iff$ Galois with gp $\mathbb{Z}/p_i\mathbb{Z}$.

$F \subset K$ Galois. Want

$$\underbrace{F \subset L}_{\text{Galois}} \underbrace{\subset K}_{\text{Gabis.}}.$$

Galois ↑ NOT

Gabis. ↑ automatic.

<u>ex.</u> $\underbrace{\mathbb{Q} \subset \mathbb{Q}}_{\text{NOT Galois.}}[2^{1/3}] \subset \mathbb{Q}[2^{1/3}, \zeta_3]$

$\underbrace{\mathbb{Q} \subset}_{\text{Galois}} \mathbb{Q}[\zeta_3] \underbrace{\subset \mathbb{Q}}_{\text{Gabis.}}[2^{1/3}, \zeta_3]$

Let $F \subset K$ be a Galois ext. $G = \mathrm{Aut}(K/F)$.
L be an intermediate field with $H = \mathrm{Aut}(K/L)$

The following are eqv.

1. $L \supset F$ is Galois.
2. $\forall\ \sigma \in G$ we have $\sigma(L) = L$
3. $H \subset G$ is a <u>normal</u> subgroup.

In this case, have a hom.

$$\begin{array}{ccc} \mathrm{Aut}(K/F) & \longrightarrow & \mathrm{Aut}(L/F) \\ \| & & \wr\wr \\ G & & G/H \end{array}$$

This is surj. with
Kernel H.

$$\underbrace{\underbrace{F \subset L}_{\text{Galois}}\;\underbrace{\subset K}_{\text{Galois}}}_{\text{Galois.}}$$

$$\underbrace{\underbrace{\qquad\qquad}_{G/H}\;\underbrace{\qquad\qquad}_{H.}}_{G}$$