

Lecture 12. Galois extension

201

Def: $K \subset K(\subset \bar{K})$ is Galois if
it is both normal and separable.

~~As~~ before, for alg ext $K|k$, denote

$$G = G(K|k) = \text{Gal}(K|k) = \text{the group } k\text{-auto. of } K$$

The Galois group of $K|k$.

Note: (i) $K|k$ Galois. ~~then~~ one has the canonical identification

$$\{\sigma: K \xrightarrow{\sim} K, \sigma|_k = \text{id}\} \xrightarrow{1-1} \{\sigma: K \hookrightarrow \bar{k}, \sigma|_k = \text{id}\}$$

$$(ii) K|k \text{ finite Galois} \iff |G(K|k)| = [K:k]$$

Note: we have the natural group action:

$$\begin{aligned} G \times K &\longrightarrow K \\ (\sigma, x) &\longmapsto x^\sigma \end{aligned}$$

For $H \leq G$, ~~we~~ we have $H \times K \longrightarrow K$.

Denote

$$K^H = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H\} \subseteq K$$

the fixed pts of K under the H -action.

Note $K \supseteq K^H \subseteq K$ is again field extension!

Theorem (finite Galois correspondence)

Assume $K \subset \bar{K} \subset \bar{K}$ to be finite, Galois. Then

(i)

$$\{E \mid K \subseteq E \subseteq \bar{K}\} \xleftrightarrow{1-1} \{H \mid \emptyset \neq H \subseteq G\}$$

$$E \xrightarrow{\quad} G(K|E)$$

$$K^H \xleftarrow{\quad} H$$

One has $\forall K \subseteq E \subseteq \bar{K}, \quad {}_K G(K|E) = E$

$\forall \emptyset \neq H \subseteq G, \quad G(K|K^H) = H.$

(ii) Let $E = k^H$ (or $H = G(k|E)$).

Then $E|k$ Galois $\Leftrightarrow H \triangleleft G$

Moreover, one has an isomorphism

$$\begin{array}{ccc} G/H & \xrightarrow{\sim} & G(k|k) \\ \downarrow & \longmapsto & \downarrow \\ \sigma & & \sigma|_E \end{array}$$

pf: (i) Note first, one has easily:

$$H \subseteq G(k|k^H)$$

$$E \subseteq k^{G(k|E)}$$

Let us show $H = G(k|k^H)$.

The key is to consider the following:

By Primitive Element Theorem, $\exists d \in k$, s.t.

$$k = k(d).$$

Let $H = \{g_1, \dots, g_n\} \subseteq G$. Consider

$$f(x) = \prod_{i=1}^n (x - g_i(d)) \in k[x].$$

The coeffs of $f(x)$ are

$$c_i(g_1(\alpha), \dots, g_n(\alpha))$$

Then $\forall g \in H$,

$$g(c_i(g_1(\alpha), \dots, g_n(\alpha)))$$

$$= c_i(gg_1(\alpha), \dots, gg_n(\alpha))$$

c_i symmetric \rightarrow

$$= c_i(g_1(\alpha), \dots, g_n(\alpha)).$$

Thus $f(x) \in K^H[x] (= K[x])$

Thus since $f(\alpha) = 0$, it follows that

$$\begin{aligned} \underline{[K : K^H]} &= \text{deg of irred poly of } \alpha \text{ over } K^H \\ &\leq \text{deg } f(x) = n = \underline{|H|} \end{aligned}$$

Since $K|_{K^H}$ is Galois, it follows that

$$|H| \leq |G(K|_{K^H})| = [K : K^H] \leq |H|$$

$$\Rightarrow G(K|_{K^H}) = H.$$

Now:

$$G(K|E) = G(K|_K G(K|E))$$

$$\begin{aligned} \text{Thus } [K: E] &\stackrel{K|E \text{ Galois}}{=} |G(K|E)| = |G(K|_K G(K|E))| \\ &\stackrel{K|_K G(K|E) \text{ Galois}}{=} [K: K^{G(K|E)}] \end{aligned}$$

As $E \subseteq K^{G(K|E)}$, it follows that

$$E = K^{G(K|E)}.$$

This proves (i).

(ii). Let $E = K^H$, for any $H \leq G$.

Note $\forall g \in G$,

$$K^{gHg^{-1}} = g(E) \quad (\text{check!})$$

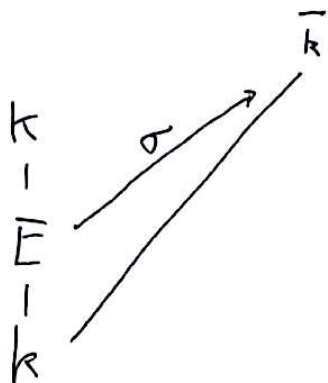
Thus: $E|K$ Galois $\Rightarrow \forall g \in G, g(E) = E$

$$\Rightarrow K^{gHg^{-1}} = E \stackrel{(i)}{\Rightarrow} gHg^{-1} = G(K|E) = H$$

$$\Rightarrow H \triangleleft G.$$

Conversely, assume $H \triangleleft G$.

Consider



$$\exists \tau: k \hookrightarrow \bar{k}, \quad \tau|_E = \sigma.$$

$$K/k \text{ Galois} \Rightarrow \tau(K) = K. \Rightarrow \sigma(E) \subset K.$$

$\Rightarrow \sigma$ is the restriction some elt in $G(K/k)$.

But as shown above, if $\sigma H \sigma^{-1} = H$, it follows from (i)

$$\text{that } \sigma(E) = E.$$

Since σ is arbitrary, it follows that E/k Galois.

Assume: E/k Galois, Consider

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G(E/k) \\ \downarrow & & \downarrow \\ \sigma & \xrightarrow{\quad} & \sigma|_E \end{array}$$

The map is surjective, by the above discussion. It is by def

$$\text{that } \text{Ker}(\phi) = G(K(E)) = H. \text{ Thus } G/H \cong G(E/k).$$

#.

Theorem (E. Artin)

K , field, $G \leq \text{Aut}(K)$, finite group.

$k = K^G$. Then $K|k$ Galois, and $G(K|k) = G$.

pf 1 (Artin).

Note $G \leq G(K|k)$. So it suffices to show

$$[K:k] \leq |G| = n, \text{ as } |G| \leq [K:k].$$

Set $\{\sigma_1, \dots, \sigma_n\} = G$.

prove by contradiction: Assume the contrary that

$$[K:k] > n.$$

Take $d_1, \dots, d_{n+1} \in K$, K -lin. indep.

Consider vectors $\{v_1, \dots, v_{n+1}\} \in K^n$, given by

$$\left\{ \begin{array}{l} v_1 = (\sigma_1(d_1), \dots, \sigma_n(d_1)) \\ \vdots \\ v_{n+1} = (\sigma_1(d_{n+1}), \dots, \sigma_n(d_{n+1})) \end{array} \right.$$

Since $\dim_K K^n = n$, \exists non-trivial K -linear relations ²⁰⁸
 between $\{v_1, \dots, v_{n+1}\}$.

Assume r is the minimal number such that there are
 r -vectors in $\{v_1, \dots, v_{n+1}\}$ with non-trivial K -linear
 relations.

WLOG. say

$$\lambda_1 v_1 + \dots + \lambda_r v_r = 0, \quad \lambda_i \in K$$

$$\xrightarrow{\lambda_1^{-1}} v_1 + \tilde{\lambda}_2 v_2 + \dots + \tilde{\lambda}_r v_r = 0, \quad \tilde{\lambda}_i \neq 0 \in K \quad (*)$$

Now: apply $\sigma \in G$ on $(*)$, we get

$$\sigma(v_1) + \sigma(\tilde{\lambda}_2) \sigma(v_2) + \dots + \sigma(\tilde{\lambda}_r) \sigma(v_r) = 0.$$

Note, up to change of positions of components,

$$\sigma(v_i) = v_i, \quad \text{we}$$

Thus, we can assume

$$v_1 + \sigma(\tilde{\lambda}_2) v_2 + \dots + \sigma(\tilde{\lambda}_r) v_r = 0 \quad (*)^\sigma$$

$$(X)^{\sigma} - (X) \Rightarrow$$

$$[\sigma(\tilde{\lambda}_2) - \tilde{\lambda}_2] v_2 + \dots + [\sigma(\tilde{\lambda}_r) - \tilde{\lambda}_r] v_r = 0.$$

\Rightarrow either $\sigma(\tilde{\lambda}_i) = \tilde{\lambda}_i, \forall i \Rightarrow \tilde{\lambda}_i \in K, \forall i.$

or

we get a non-trivial relation with smaller number of vectors.

Both are impossible!

Lemma:

pf 2. Step 1: Assume \mathbb{E}/K separable.

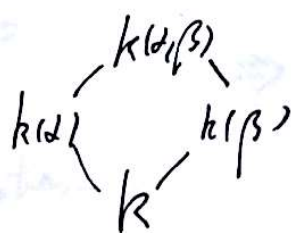
if $\forall \alpha \in \mathbb{E}, [k(\alpha):K] \leq n,$

then $[\mathbb{E}:K] \leq n.$

pf: Take $\alpha \in K$, s.t. $[k(\alpha):K]$ is maximal.

if $k(\alpha) = \mathbb{E}$, then we're done.

Otherwise, $\exists \beta \in \mathbb{E}, \beta \notin k(\alpha)$



Then $k(\alpha, \beta)/K$ separable
Primitive Element Theorem

$$\Rightarrow k(\alpha, \beta) = k(\gamma)$$

But $[k(\gamma):K] > [k(\alpha):K]. \downarrow$

#

Step 2. Take any $\alpha \in k$. Consider the G -orbit

$$G\{\alpha\} = \{\alpha_1, \dots, \alpha_d\} \quad \alpha_i \neq \alpha_j.$$

Consider

$$f(x) = \prod_{i=1}^d (x - \alpha_i).$$

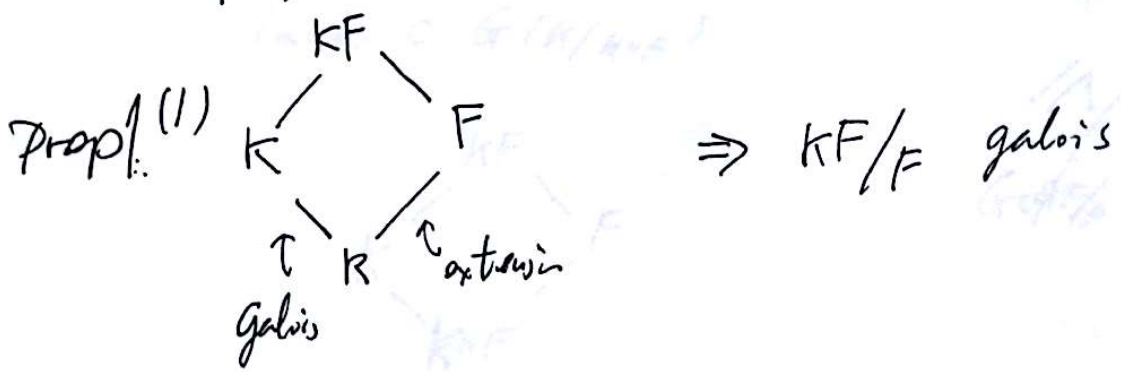
Then $\forall \sigma \in G, \sigma(\alpha_i) = \alpha_j, \forall i$
 $\Rightarrow \sigma(\alpha_1, \dots, \alpha_d) = (\alpha_1, \dots, \alpha_d) \in k^G = k$
 $\Rightarrow f(x) \in k[x]$.

$f_\alpha \mid f$
 \Rightarrow (1) the roots of f_α separable $\Rightarrow k/k$ separable
 (2) $\deg [k(\alpha) : k] \leq d \leq n$

Step 1
 $\Rightarrow [k : k] \leq n.$

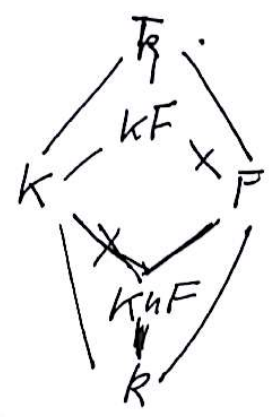
#

The class of Galois extensions is NOT distinguished. But we still have



(2)

Moreover, if



, then

$$G(KF/F) \cong G(K/K \cap F) \leq G(K/K)$$

$$\downarrow \sigma \longmapsto \downarrow \sigma|_K$$

Pf: (1) obvious.

(2). Consider the natural restriction map

$$G(KF/F) \xrightarrow{\phi} G(K/K)$$

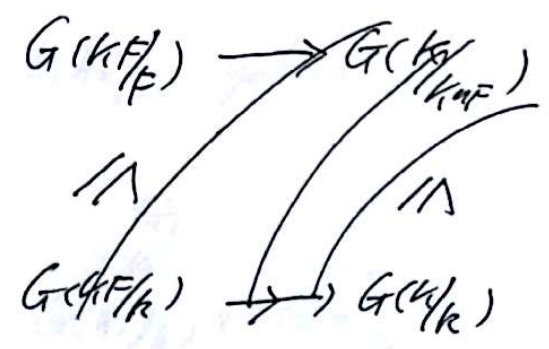
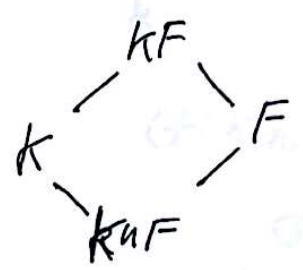
$$\sigma \longmapsto \sigma|_K$$

(this is defined, since K/K is galois, particularly normal)

(i) ϕ is injective. This is obvious.

(ii) $\text{im}(\phi) = G(K/K \cap F)$

$\text{im}(\phi) \subset G(K/K \cap F)$



Assume $kF|k$ finite ext. (for simplicity).

To see $\text{im}(\phi) = G(k/k_{nF}) \leq G(k/k)$, we

consider $K^{\text{im}(\phi)}$:

Since $\text{im}(\phi) \subset G(k/k_{nF})$, $K^{\text{im}(\phi)} \supset k_{nF}$.

Claim that: $K^{\text{im}(\phi)} = k_{nF}$.

Take $\alpha \in K^{\text{im}(\phi)} \subset k \subset kF$.

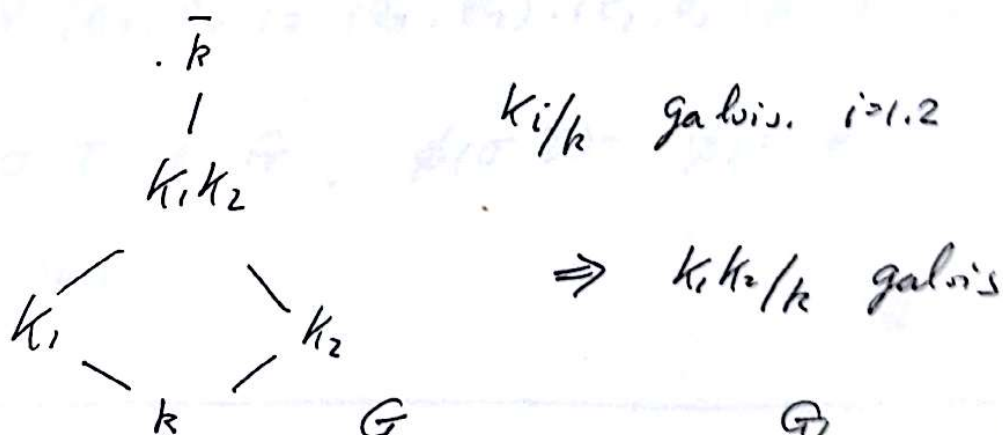
We Galois correspondence for Galois ext $kF|F$.

$\alpha \in F$.

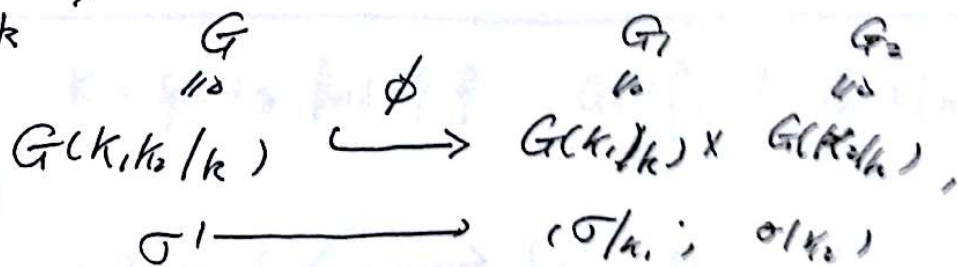
Thus $\alpha \in k_{nF}$. Done!

#

Prop 2:



Moreover:



ϕ is an iso, if $k = k_1 k_2$.

Pf: K_1, K_2
 \downarrow
 k Galois is obvious.

ϕ is obviously injective.

Given $\sigma_1 \in G_1$, last prop implies

$$\exists \sigma \in G(K_1, K_2/K_2) \cong G, \text{ s.t. } \sigma|_{K_2} = \sigma_1$$

$$\text{obviously } \sigma|_{K_2} = e_2 \in G_2$$

Symmetrically, $\sigma_2 \in G_2$, $\exists \tau \in G$, s.t.

$$\begin{cases} \sigma|_{K_2} = \sigma_2 \\ \sigma|_{K_1} = e_1 \in G_1 \end{cases}$$

Thus, $\forall (\sigma_1, \sigma_2) = (\sigma_1, e_2) \cdot (e_1, \sigma_2) \in G_1 \times G_2$

$$\exists \sigma, \tau \in G, \phi(\sigma \cdot \tau) = \phi(\sigma) \cdot \phi(\tau) = (\sigma_1, \sigma_2)$$

$\Rightarrow \phi$ is surj.

#

Definition: $f \in k[x]$, $K = \text{splitting field of } f$. $\text{Gal}(f) \triangleq G(K/k)$
 separable poly

$$\{f \in k[x], \text{ sep.}\} \longleftrightarrow \{G, \text{ finite group}\}$$

Study the "simplest" eqn:

$$x^n - 1 = 0$$

$$f_n(x) = x^n - 1.$$

If $\text{char}(k) = p \mid n$, then $f_n(x) = (x-1)^n$.

It is not separable.

Assume then $\text{char}(k) \nmid n$.

$$f'_n(x) = nx^{n-1} \neq 0, \quad \left. \begin{array}{l} f'_n(x) = 0 \Rightarrow x=0. \\ f''_n(x) = 1 \neq 0. \end{array} \right\} \Rightarrow$$

$f_n(x)$ is separable.

Note. all roots of $f_n(x) = 0$ in \bar{k} form a cyclic subgroup of \bar{k}^* .

Let ξ_n be a primitive root of $f_n(x)$; i.e.

$$\langle \xi_n \rangle = \text{all roots of } f_n.$$

Question: $\text{Gal}(f_n) = ?$

The splitting field of $f_n = k(\xi_n)$.

Note: $\forall \sigma \in G(k(\xi_n)/k)$,

write, $\sigma(\xi_n) = \xi_n^{\phi(\sigma)}$, $\phi(\sigma) \in \mathbb{Z}/n$

claim: $\phi(\sigma) \in (\mathbb{Z}/n)^\times$.

This is easy: $\forall \tau \in G(k(\xi_n)/k)$.

$$(\tau \circ \sigma)(\xi_n) = \tau(\sigma(\xi_n)) = \tau(\xi_n^{\phi(\sigma)}) = \xi_n^{\phi(\sigma)\phi(\tau)}$$

Take $\tau = \sigma^{-1}$, get

$$\phi(\sigma^{-1}) \cdot \phi(\sigma) = 1 \in \mathbb{Z}/n.$$

$$\Rightarrow \phi(\sigma) \in (\mathbb{Z}/n)^\times.$$

we get a homo:

$$G(k(\xi_n)/k) \xrightarrow{\phi} (\mathbb{Z}/n)^\times$$

clearly, ϕ is inj.

However, ϕ is not nec. surjective. (Take $k = \mathbb{R}$ or \mathbb{C})

Theorem: For $k = \mathbb{Q}$,

$$G(\mathbb{Q}(\xi_n) | \mathbb{Q}) \cong (\mathbb{Z}/n)^{\times}.$$

Cor: $(n, m) = 1$,

$$\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}.$$

Pf: $(n, m) = 1$, then $\xi_n \cdot \xi_m$ is a primitive root of order $n \cdot m$.

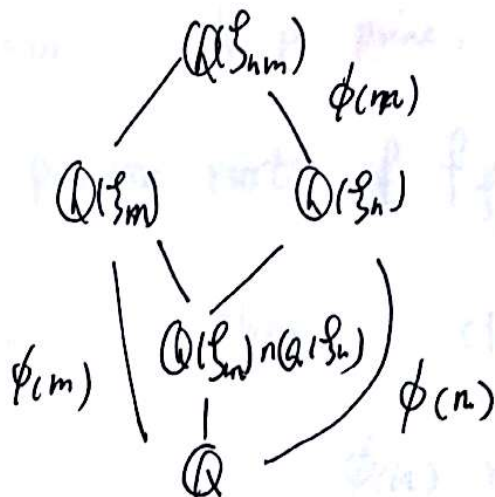
$$\text{Thus } \mathbb{Q}(\xi_n) \cdot \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{nm})$$

Now $|\mathbb{Z}/n|^{\times} = \phi(n)$, and

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m) \quad \text{if } (n, m) = 1.$$

$$\mathbb{Z}/n \cdot m \cong \mathbb{Z}/n \times \mathbb{Z}/m, \quad \text{ring isomorphism.}$$

(Chinese Remainder Theorem)



$$\begin{aligned} & G(\mathbb{Q}(\xi_{nm}) | (\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m))) \\ & \cong G(\mathbb{Q}(\xi_n) | (\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m))) \times \\ & G(\mathbb{Q}(\xi_m) | (\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m))). \end{aligned}$$

$$\text{prop 1} \Rightarrow G(\mathbb{Q}(\zeta_m) | \mathbb{Q}(\zeta_n)) \simeq G(\mathbb{Q}(\zeta_m) | \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))$$

$$\Rightarrow |G(\mathbb{Q}(\zeta_m) | \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))| = \phi(m)$$

$$\Rightarrow \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

#

pf of theorem: it suffices to show $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Let $f_{\zeta_n} \in \mathbb{Q}[X]$ be the irred of ζ_n .

$$\text{Then } X^n - 1 = f_{\zeta_n}(X) \cdot g(X)$$

$$\text{Gau\ss}'s \text{ Lemma} \Rightarrow f_{\zeta_n}, g \in \mathbb{Z}[X]$$

claim: $\forall p$, prime, $(p, n) = 1$, ζ_n^p is again a primitive root of f_{ζ_n}

claim \Rightarrow Thm. claim $\Rightarrow f_{\zeta_n}$ contains at least

$$\phi(n) \text{ roots. But } \deg f_{\zeta_n} = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |G(\mathbb{Q}(\zeta_n) | \mathbb{Q})| \leq \phi(n).$$

pf of claim: it suffices to show

$$f_{\zeta_n}(\zeta_n^p) \neq 0.$$

If not, then $g(\zeta_n^p) = 0$

$\Rightarrow \zeta_n$ is a root of $g(x^p)$

$$\Rightarrow f_{\zeta_n} \mid g(x^p)$$

$$\text{i.e. } g(x^p) = f_{\zeta_n}(x) h(x) \quad (\text{in } \mathbb{Q}[x])$$

g, f_{ζ_n} monic, integral coefficients $\xrightarrow{\text{Gauss's Lemma}} h(x) \in \mathbb{Z}[x]$
monic.

(mod p reduction)

$$\text{Now: } \overline{x^n - 1} = \overline{x^n} \overline{f_{\zeta_n}} \cdot \overline{g}$$

$$\overline{g(x^p)} = (\overline{g(x)})^p$$

$$\overline{g(x^p)} = \overline{f_{\zeta_n}} \cdot \overline{h}$$

$$\Rightarrow (\overline{f_{\zeta_n}}, \overline{g}) \neq 1 \quad (\text{in } \overline{\mathbb{F}_p}[x]) \Rightarrow x^n - 1 \text{ in } \overline{\mathbb{F}_p}$$

has n distinct roots. \downarrow
#

Lecture 13. Some applications of Galois correspondence
Compass and Rule Problem:

Thm 1: One cannot use Compass and rule to divide an arbitrary angle into three equal angles.

Thm 2: $p \in \mathbb{P}$ prime number.

Then one can use Compass and rule to draw regular p -gon $\Leftrightarrow p$ is a Fermat prime. That is

$$p = 2^{2^m} + 1 \quad \text{for some } m \in \mathbb{N}.$$

Set-up:

Def: (Constructible point), line and circle)

$\mathbb{P} \in \mathbb{C}$, Given $(0,0), (1,0) \in \mathbb{C}$, we construct

Constructible pts, lines, circles by

(0) $(0,0), (1,0)$ are constructible

(1) Any line passing through two constructible pts

is a constructible line

(2) Any circle with its center a constructible point as and passing another constructible point is

a constructible circle
 (3) The intersection points of constructible lines/circles.
 between
 between a constructible line and a constructible
 circle
 are constructible points.

If $(a, 0) \in \mathbb{C}$ is a constructible point, we call $a \in \mathbb{R}$
 a constructible number.

Key properties: ~~Also~~

$$F = \{ a \in \mathbb{R} \mid a \text{ is a constructible number} \} \subset \mathbb{R}$$

(1) $\mathbb{Q} \subset F \subset \mathbb{R}$ is a subfield.

(2) \forall finitely many $a_1, \dots, a_n \in F$, there exists

a tower

$$\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_m \stackrel{K}{=} \mathbb{R}, \text{ s.t.}$$

$$(i) \mathbb{Q}(a_1, \dots, a_n) \subset K$$

$$(ii) K_i = K_{i-1}(\sqrt{\gamma_i}), \text{ for some } \gamma_i \in K_{i-1}$$

Conversely, any number in a tower with properties (i)-(ii)
 is constructible.

Proof of Thm 1:

Take $\alpha = 60^\circ = \frac{\pi}{3}$, $\cos \alpha = \frac{1}{2}$ is constructible.

Claim that $\cos 20^\circ$ is however not constructible.

In fact: $a \in \bar{F} \xRightarrow{\text{Prop(2)}} [\mathbb{Q}(a) : \mathbb{Q}] = 2^r$

But for $a_0 = \cos 20^\circ$, we get

$$(\cos 20^\circ + i \sin 20^\circ)^3 = \cos 60^\circ + i \sin 60^\circ$$

$$(\cos 20^\circ)^3 - 3 \cos 20^\circ (1 - \sin^2 20^\circ)$$

$$+ i(\quad)$$

$$\Rightarrow 4a_0^3 - 3a_0 = \frac{1}{2} \Rightarrow [\mathbb{Q}(a_0) : \mathbb{Q}] = 3 \neq 2^r.$$

Thus, $\cos 20^\circ$ is not constructible.

Pf of Thm 2: (\Rightarrow)

If regular p -gon can be drawn by Compass & Rule, then $\cos \frac{2\pi}{p}$ is

a constructible number.

$$\zeta_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$$

$$\text{then } \cos \frac{2\pi}{p} = \frac{1}{2} (\zeta_p + \zeta_p^{-1})$$

$$\mathbb{Q}(\zeta_p)$$

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ | \quad \swarrow \mathbb{Q}(\cos \frac{2\pi}{p}) \\ \mathbb{Q} \quad \searrow \end{array}$$

$$\text{we know } [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$$

and since

$$\zeta_p^2 - 2 \cos \frac{2\pi}{p} \zeta_p + 1 = 0$$

$$\Rightarrow [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\cos \frac{2\pi}{p})] = 2$$

$$\Rightarrow [\mathbb{Q}(\cos \frac{2\pi}{p}) : \mathbb{Q}] = \frac{p-1}{2}$$

Since $\cos \frac{2\pi}{p}$ is constructible, it follows.

$$\frac{p-1}{2} = 2^k \Rightarrow p = 2^{m+1} \left. \begin{array}{l} \\ \rho \text{ prime} \end{array} \right\} \Rightarrow p = 2^{2^n} + 1.$$

(\Leftarrow) assume $p = 2^{2^n} + 1$. then

$$\frac{\sqrt{p}}{2^{2^n}} \simeq G(\mathbb{Q}(\zeta_p) | \mathbb{Q}) \rightarrow G(\mathbb{Q}(\zeta_p, \frac{2\pi}{p}) | \mathbb{Q})$$

$$\Rightarrow G(\mathbb{Q}(\cos \frac{2\pi}{p}) | \mathbb{Q}) \simeq \frac{\sqrt{p}}{2^{2^n-1}}$$

Thus, it exists a tower of (normal) subgrps.

$$G(\mathbb{Q}(\omega^{\frac{22}{p}}) | \mathbb{Q}) \supset G_0 \supset G_1 \supset \dots \supset G_N = \{e\}.$$

$$G(\mathbb{Q}(\omega^{\frac{22}{p}}) | \mathbb{Q}) \quad \text{s.t.} \quad \frac{G_i}{G_{i+1}} = \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Then, by Galois correspondence, \exists tower of subfields.

$$\mathbb{Q} \subset K_1 \subset \dots \subset K_N = \mathbb{Q}(\omega^{\frac{22}{p}})$$

s.t. $K_{i+1} | K_i$ is a double extension

thus, $K_{i+1} = K_i(\sqrt{r_i})$ for some $r_i \in K_i$, $r_i^2 \notin K_i$.

$\Rightarrow \omega^{\frac{22}{p}}$ is constructible.

#.