Lecture 12. Galois extension

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

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

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

The Galois group of $K|_k$.

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

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

(ii) $K|_k$ 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 $k \subseteq K^H \subseteq K$ is again field extension!

Theorem (finite Galois correspondence)

Assume $k \subset K$ ($\subset \bar{k}$) to be finite, galois. Then

(i)

$$\{E \mid k \subseteq E \subseteq K\} \xleftrightarrow{1\text{-}1} \{H \mid \{e\} \subseteq H \subseteq G\}$$

$$E \longmapsto G(K|E)$$

$$K^H \longleftarrow H$$

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

$\forall \{e\} \in H \subseteq G$, $\quad G(K|_{K^H}) = H.$

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

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

Moreover, one has an isomorphism

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

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, $\exists \alpha \in K$, s.t.

$$K = k(\alpha).$$

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

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

The coeffs of $f(x)$ are

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

Then $\forall g \in H$,

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

$$= c_i(gg_1(\alpha), \ldots, g_n(\alpha))$$

c_i symmetric $\rightarrow$ $= c_i(g_1(\alpha), \ldots, g_n(\alpha))$.

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

Thus Since $f(\alpha) = 0$. it follows that

$$[K : K^H] = \text{deg of irred poly of } \alpha \text{ over } K^H$$

$$\leq \deg f(x) = n = |H|$$

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

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

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

Now:

$$G(K|E) = G\left(K|_{K^{G(K|E)}}\right)$$

Thus $[K:E] \overset{K|E \text{ Galois}}{=} |G(K|E)| = \left|G\left(K|_{K^{G(K|E)}}\right)\right|$

$$\overset{K|K^{G(K|E)} \text{ galois}}{=} [K : K^{G(K|E)}]$$

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 $\forall g \in G$,

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

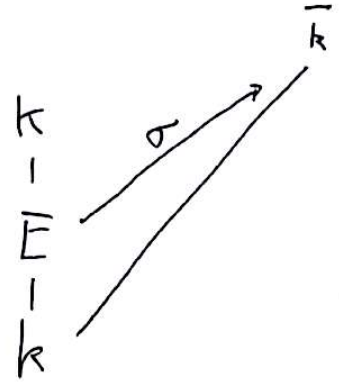
Thus. $E|k$ galois $\Rightarrow \forall g \in G,\ g(E) = E$

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

$$\Rightarrow H \lhd G.$$

Conversely, assume $H \lhd G$.

Consider



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

$K|k$ galois $\Rightarrow \quad \tau(K) = K. \Rightarrow$ ~~$\sigma(E) \subset K$~~.

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

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

that $\sigma(E) = E$.

Since σ is arbitrary, it follows that $E|k$ galois.

Assume: $E|k$ galois, Consider

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G(\bar{E}|k) \\ \wr & & \wr \\ \sigma & \longmapsto & \sigma|_{\bar{E}} \end{array}$$

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

that $\ker(\phi) = G(K|E) = H$. Thus $G/H \simeq G(E|k)$.

#.

Theorem (E. Artin)

K, field, $G \leq Aut(K)$, 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

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

Set $\{\underset{\text{id}}{\sigma_1}, \cdots \sigma_n\} = G$.

prove by contradiction: Assume the contrary that

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

Take $\alpha_1, \cdots, \alpha_{n+1} \in K$, k-lin. indep.

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

$$\begin{cases} v_1 = (\sigma_1(\alpha_1), \cdots, \sigma_n(\alpha_1)) \\ \vdots \\ v_{n+1} = (\sigma_1(\alpha_{n+1}), \cdots, \sigma_n(\alpha_{n+1})) \end{cases}$$

Since $\dim_K K^n = n$, $\exists$ non-trivial K-linear relations 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 $\forall i$

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

λ_1^{-1}

$$\Rightarrow \quad v_1 + \tilde{\lambda}_2 v_2 + \dots + \tilde{\lambda}_r v_r = 0, \quad \tilde{\lambda}_i \neq 0 \in K \quad (*)!$$

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,

$$\sigma(v_i) = v_i.$$

Thus, we can assume

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

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

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

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

or

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

Both are impossible !

Lemma:

pf 2. Step 1: Assume E/k seperable.

if $\forall \alpha \in E$, $[k(\alpha):k] \le n$,

then $[E:k] \le n$.

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

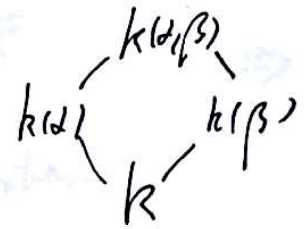
if $k(\alpha) = E$, then we're done.

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

Then $k(\alpha,\beta)/k$ seperable

Primitive Element Theorem

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



But $[k(\gamma):k] \not> [k(\alpha):k]$. ↯

#

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

$$G\{\alpha\} = \{\alpha_1, \cdots \alpha_d\} \qquad \alpha_i \neq \alpha_j.$$

Consider

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

Then $\forall \sigma \in G$, $\sigma(c_i(\alpha_1, \cdots \alpha_d)) = c_i(\alpha_1 \cdots \alpha_d)$, $\forall i$

$\Rightarrow c_i(\alpha_1 \cdots \alpha_d) \in k^G = k$

$\Rightarrow f(x) \in k[x]$.

$f_\alpha | f$

$\Rightarrow$ (1) the minimal f_α seperable $\Rightarrow K/k$ seperable

(2) ~~deg~~ f $[k(\alpha) : k] \leq d \leq n$

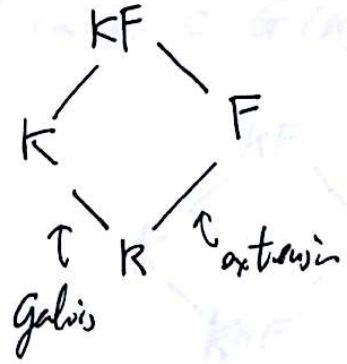
Step 1

$\Rightarrow [K : k] \leq n$.

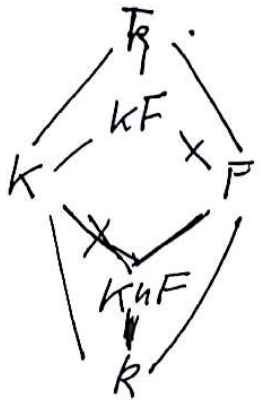
#

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

Prop 1. (1)



$\Rightarrow KF/F$ galois

(2) Moreover, if 

, then

$$G(KF/F) \cong G(K/K\cap F) \leq G(K/k)$$
$$\tilde{\sigma} \longmapsto \sigma|_K$$

Pf: (1) Obvious.

(2). Consider the natural restriction map

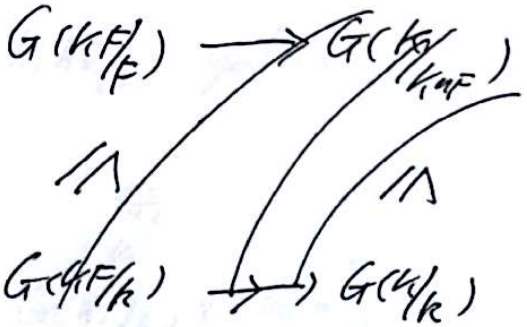
$$G(KF/F) \xrightarrow{\phi} G(K/k)$$
$$\sigma \longmapsto \sigma|_K$$

(this is defined. Since K/k is galois, particularly normal)

(i) ϕ is injective. This is obvious.

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

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



Assume KF/k finite ext. (for simplicity).

To see $im(\phi) = G(K/KF) \leq G(K/k)$, we

Consider $K^{im(\phi)}$:

Since $im(\phi) \subset G(K/KF)$, $K^{im(\phi)} \supset KF$.

Claim that: $K^{im(\phi)} = KF$.

Take $\alpha \in K^{im(\phi)} \subset K \subset KF$.

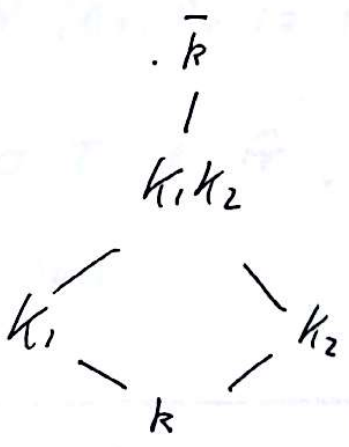
Use Galois correspondence for galois ext KF/F.

$\alpha \in \bar{F}$.

Thus $\alpha \in KF$. Done!

#

Prop 2:



K_i/k galois. $i=1,2$

$\Rightarrow K_1K_2/k$ galois

Moreover: $G(K_1K_2/k) \xrightarrow{\phi} G(K_1/k) \times G(K_2/k)$,

$\sigma \longmapsto (\sigma/K_1, \sigma/K_2)$

ϕ is an iso. if $k = K_1 \cap K_2$.

Pf: K_1K_2

$|$ gal is obvious.

k

ϕ is obviously injective.

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

$\exists\ \sigma \in G(K_1K_2/K_2) \leq G$, s.t $\sigma/_{K_1} = \sigma_1$

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

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

$\Rightarrow \phi$ is surj.

#

Definition: $f \in k[X]$, K = splitting field of f. $Gal(f) \triangleq G(K/k)$

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

it is not seperable.

Assume that $\mathrm{char}(k) \nmid n$.

$f_n'(x) = n x^{n-1} \neq 0$, $\quad f_n'(x) = 0 \Rightarrow x = 0$.

$f_n(0) = 1 \neq 0$ $\Rightarrow$

$f_n(x)$ is seperable.

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: $\mathrm{Gal}(f_n) = ?$

The splitting field of $f_n = x^n - 1$ is $k(\xi_n)$.

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: $\forall \tau \in G(k(\xi_n)|k)$

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

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 nece. surjective. (Take $k = \mathbb{R}$ or, $\mathbb{C}$)

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

$$G(\mathbb{Q}(\xi_n)|_{\mathbb{Q}}) \xrightarrow{\phi}_{\simeq} \left(\mathbb{Z}/n\right)^\times.$$

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 $n \cdot m$.

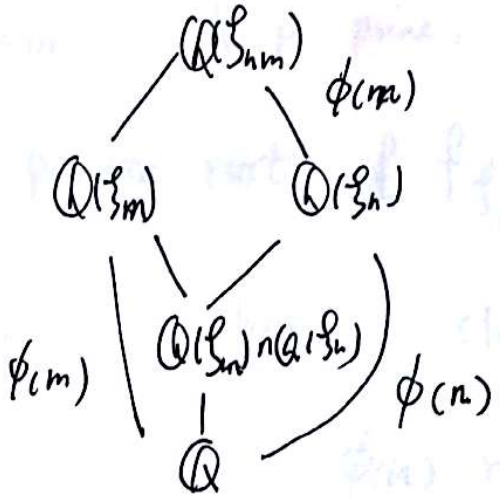
Thus $\mathbb{Q}(\xi_n) \cdot \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{nm})$

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

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

$\xi\left(\mathbb{Z}/n \cdot m \simeq \mathbb{Z}/n \times \mathbb{Z}/m\right.$, string isomorphism.

Chinese Remainder Theorem)



$$G(\mathbb{Q}(\xi_{nm})|_{\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m)})$$

$$\simeq G(\mathbb{Q}(\xi_n)|_{\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m)}) \times$$

$$G(\mathbb{Q}(\xi_m)|_{\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m)}).$$

prop 1 $\Rightarrow$ $G(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}(\zeta_n)) \simeq G(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n))$

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

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

#

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.

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

Gauß's 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_{ζ_n} contains at least $\phi(n)$ 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

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

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

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

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

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

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

(mod p reduction)

Now:
$$\begin{cases} \overline{x^n - 1} = \overline{f}_{\zeta_n} \cdot \overline{g} \\ \overline{g(x^p)} = (\overline{g}(x))^p \\ \overline{g(x^p)} = \overline{f}_{\zeta_n} \cdot \overline{h} \end{cases}$$

$\Rightarrow (\overline{f}_{\zeta_n}, \overline{g}) \neq 1$ $(\text{in } \overline{\pi}_p[x])$ $\Rightarrow$ $x^n - 1$ $\text{in } \overline{\overline{\pi}_p}$ has common roots. $\lightning$

$\vee (\overline{f}_{\zeta_n})$

#

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 a prime number.

Then one can use Compass and rule to draw regular

p-gon $\Leftrightarrow$ p is a Fermat prime. That is

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

Set-up:

Def: (Constructible point, line and circle)

~~$P \in \mathbb{C}$~~, 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 between constructible lines/circles.

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:

$F = \{a \in \mathbb{R} \mid (a,0) \text{ constructible number}\} \subset \mathbb{R}$

(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

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_m \subset \mathbb{R}, \text{ s.t.}$$

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

(ii) $K_i = K_{i-1}(\sqrt{r_i})$ for some $r_i \in K_{i-1}$.

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: $a \in F \overset{\text{Prop(2)}}{\Longrightarrow} [\mathbb{Q}(a):\mathbb{Q}] = 2^r$

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

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

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

$$+ i(\qquad\qquad)$$

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

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.

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

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

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & & \text{we know } [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1 \\ | \quad \diagdown\, \mathbb{Q}(\cos\frac{2\pi}{p}) & & \text{and since} \\ \mathbb{Q} \quad \diagup & & \zeta_p^2 - 2\cos\tfrac{2\pi}{p}\zeta_p + 1 = 0 \\ & & \Rightarrow [\mathbb{Q}(\zeta_p):\mathbb{Q}(\cos\tfrac{2\pi}{p})] = 2 \end{array}$$

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

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

$$\frac{p-1}{2} = 2^k \Rightarrow p = 2^m + 1.$$

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

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

$$\frac{\mathbb{Z}}{2^{2^n}} \simeq G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \twoheadrightarrow G(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\cos\tfrac{2\pi}{p}))$$

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

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

$$G(\mathbb{Q}(\cos\tfrac{2\pi}{p})/\mathbb{Q}) = G_0 \supset G_1 \supset \cdots \supset G_N = \{e\}.$$

s.t. $\dfrac{G_i}{G_{i+1}} = \dfrac{\mathbb{Z}}{2\mathbb{Z}}$

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

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_N = \mathbb{Q}(\cos\tfrac{2\pi}{p})$$

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

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

$\Rightarrow \cos\frac{2\pi}{p}$ is constructible.

#

Theorem: $\mathbb{C}$ is alg. closed.

pf: $\mathbb{C} := \{a+bi \mid i^2 = -1\} = \mathbb{R}(i)$

$$f_i = x^2 + 1. \in \mathbb{R}[x].$$

- $\forall\ x \in \mathbb{C},\ \exists\ y \in \mathbb{C}$, s.t $y^2 = x$.

  write $x = a+bi$.

  then $y = c + di$, with

  $$c^2 = \frac{a+\sqrt{a^2+b^2}}{2} > 0 \qquad d^2 = \frac{-a+\sqrt{a^2+b^2}}{2} > 0$$

- Char $\mathbb{R} = 0$,

  $E/\mathbb{R}$ finite, ext;

  $\tilde{E}$ = galois closure of $E/\mathbb{R}$

  Show: $\tilde{E} = \mathbb{C}$

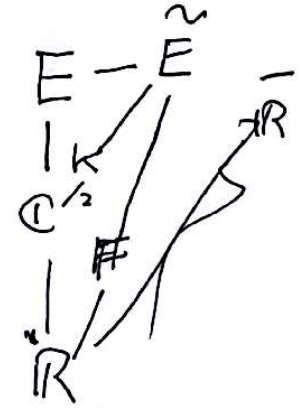
  $G = G(\tilde{E}/\mathbb{R})$

  Take $H \leq G$ a sylow 2-grp.

  $$F = \tilde{E}^H, \qquad G(\tilde{E}|F) = H$$

  $\| $

  $\mathbb{R}(\alpha)$. $\qquad \deg f_\alpha = [G:H] = \text{odd}$



But any odd poly in $\mathbb{R}[X]$ has a root in $\mathbb{R}[X]$,

hence, it is irred $\Leftrightarrow$ deg $= 1$

$\Rightarrow \quad F = \mathbb{R}$

$\Rightarrow$ G is a 2-group.

Let $G_1 = G(\tilde{E}/\mathbb{C}) \leq G$

If G_1 non-trivial, then G_1 is again 2-grp.

Take $G_2 \leq G_1$ to be a index 2-subgrp.

$K = \tilde{E}^{G_2}$, $K/\mathbb{C}$ quadratic ext

But ~~any~~ $\mathbb{C}$ has no quadratic-ext. !

$\Rightarrow$ G_1 must be trivial.

$\Rightarrow \quad \tilde{E} = \mathbb{C}$.

#

Lecture 14. Cyclic extensions.

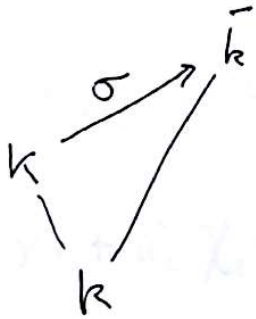
G = group / monoid, K = field

A <u>character</u> of G in K means a group homo

$$\chi : G \longrightarrow K^* \ (= GL_1(K))$$

χ is trivial if $\chi(G) = 1$.

In our situation:



G (in K^*)

$\sigma : k^\times \longrightarrow \bar{k}^\times$, σ is a character of k^* in to $\bar{k}$.

Let $\chi_1, \ldots, \chi_n : G \to K^\times$, be characters. They are

linearly indep over K, if

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \qquad a_i \in K$$

then $a_i = 0$, $\forall i$.

<u>Theorem (Artin)</u>. Let G be a group (monoid). Let

$\chi_1, \dots, \chi_n$ be distinct characters of G into a field K.

Then $\{\chi_1, \dots, \chi_n\}$ are linearly indep. over K.

pf: Let r be the minimal length of (non-trivial) K-lin. relation, say

$$a_1\chi_1 + \dots + a_r\chi_r = 0 \qquad a_i \neq 0 \in K.$$

assume $a_1 = 1$, get

$$\chi_1 + \tilde{a}_2\chi_2 + \tilde{a}_r\chi_r = 0 \qquad (*)$$

$\forall a, x \in G$.

$$\chi_1(ax) + \tilde{a}_2\chi_2(ax) + \dots + \tilde{a}_r\chi_r(ax) = 0$$

$$\Rightarrow \chi_1(a)\chi_1 + \tilde{a}_2\chi_2(a)\chi_2 + \dots + \tilde{a}_r\chi_r(a)\chi_r = 0$$

$$\Rightarrow \chi_1 + \left[\tilde{a}_2\frac{\chi_2(a)}{\chi_1(a)}\right]\chi_2 + \dots + \left[\frac{\tilde{a}_r\chi_r(a)}{\chi_1(a)}\right]\chi_r = 0 \qquad (*)'$$

Since $\chi_1, \dots, \chi_r$ distinct, it follows that

$$\exists\, a \in G, \text{ s.t } \chi_2(a) \neq \chi_1(a).$$

$$(*)' - (*) \Rightarrow \underbrace{\left(\tilde{a}_2\frac{\chi_2(a)}{\chi_1(a)} - \tilde{a}_2\right)}_{\neq 0}\chi_2 + \dots + \left(\tilde{a}_r\frac{\chi_r(a)}{\chi_1(a)} - \tilde{a}_r\right)\chi_r = 0$$

Then, we obtain a nontrivial k-lin relation among $\{\chi_1, \cdots \chi_n\}$ with smaller length. ↯.

#

Corollary (Artin).

Let $\sigma_1, \cdots, \sigma_n$ are n distinct embeddings of E into E'.

Let F be the fixed field of E, then

$$[E:F] \geq n.$$

Here, the fixed field means $\left\{ x \in E, \mid \sigma_1(x) = \cdots = \sigma_n(x) \right\}$.

pf: Suppose to the contrary that $[E:F] = r < n$

Take $w_1, \cdots, w_r$ be a basis. Consider

$$\sigma_1(w_1)\chi_1 + \sigma_2(w_1)\chi_2 + \cdots + \sigma_n(w_1)\chi_n = 0$$

$r < n$ ⎫

$$\sigma_1(w_r)\chi_1 + \sigma_2(w_r)\chi_2 + \cdots + \sigma_n(w_r)\chi_n = 0$$

$\Rightarrow \exists$ nontrivial solutions $(\chi_1, \cdots, \chi_n) \in E^n$

Now $\forall \alpha \in E$, $\exists a_1, \dots a_r \in F$, s.t

$$\alpha = a_1 w_1 + \cdots + a_r w_r$$

$$\sigma_1(a_1)\left[\sigma_1(w_1)\chi_1 + \sigma_2(w_1)\chi_2 + \cdots + \sigma_n(w_1)\chi_n\right] = \sigma_1(a_1)\cdot 0 = 0$$

$$\| $$

$$\sigma_1(a_1 w_1)\chi_1 + \sigma_1(a_1)\sigma_2(w_1)\chi_2 + \cdots + \sigma_n(a_1 w_1)\chi_n = 0$$

$$\| \; a_1 \in F$$

$$\sigma_2(a_1)\sigma_2(w_1)\chi_2$$

$$\|$$

$$\sigma_2(a_1 w_1)\chi_2$$

$$\sigma_2(a_2 w_2)\chi_2 + \sigma_2(a_2 w_2)\chi_2 + \cdots + \sigma_n(a_2 w_2)\chi_n = 0$$

$$\vdots$$

$$\sigma_n(a_r w_r)\chi_1 + \sigma_2(a_r w_r)\chi_2 + \cdots + \sigma_n(a_r w_r)\chi_n = 0$$

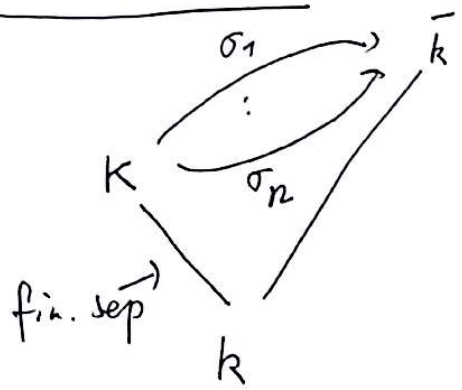
$$\Rightarrow \sigma_1(\underbrace{a_1 w_1 + \cdots + a_n w_r}_{\|\ \alpha})\chi_1 + \sigma_2(\underbrace{a_1 w_1 + \cdots + a_r w_r}_{\|\ \alpha})\chi_2 + \cdots$$

$$+ \sigma_n(\underbrace{a_1 w_1 + \cdots + a_r w_r}_{\|\ \alpha})\chi_n = 0$$

Since α is arbitrary,

$$\chi_1 \cdot \sigma_1 + \cdots + \chi_n \sigma_n = 0 \quad \lightning \quad \#$$

Norm and Trace:



$$\{\sigma_1 \dots \sigma_n\} = \mathrm{Hom}_k(K, \bar{k})$$

Define $N_{K/k}: K \longrightarrow k$, $N_{K/k}(\alpha) = \prod_{i=1}^{r} \sigma_i(\alpha)$

$Tr_{E/k}: K \longrightarrow k$, $Tr_{K/k}(\alpha) = \sum_{i=1}^{r} \sigma_i(\alpha)$

Theorem: (i) E/k finite separable.

Then $N_{E/k}: E^\times \to k^\times$ multiplicative homomorphism

$Tr_{E/k}: E \longrightarrow k$, additive homomorphism.

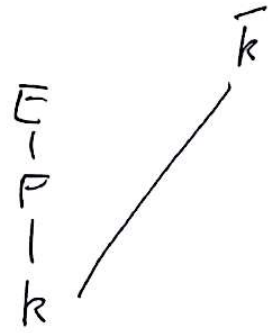
(ii) $E \supset F \supset k$ fin. sep.

Then $N_{E/k} = N_{F/k} \circ N_{E/F}$

$Tr_{E/k} = Tr_{F/k} \circ Tr_{E/F}$

(iii) E/k fin. sep. $\forall \alpha \in E$, $m_\alpha: E \longrightarrow E$, $x \mapsto \alpha \cdot x$

(ii)



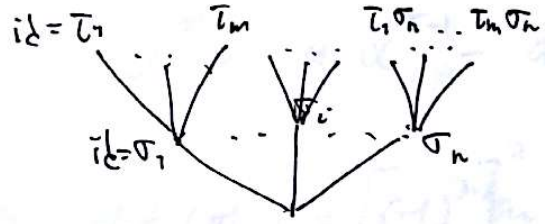
Let $\{\sigma_1, \ldots \sigma_n\} = \mathrm{Hom}_k^{id}(F, \bar{k})$

Let $\{\tau_1, \ldots \tau_m\} = \mathrm{Hom}_F^{id}(E, \bar{k})$

Then, for each $\sigma_i : F \hookrightarrow \bar{k}$.

Let $\{\tau_1\sigma_i, \ldots, \tau_m\sigma_i\}$ be the extensions of σ_i

to k-embeddings $\bar{E} \longrightarrow \bar{k}$.



$N_{E/F}(N_{F/k}(\alpha))$

Then $\mathrm{Hom}_k(E, \bar{k}) = \{\tau_i\sigma_j\}$. "

Then $N_{E/k}(\alpha) = \prod_{i,j}(\tau_i\sigma_j)(\alpha) = \prod_i\left(\prod_j \sigma_j(\alpha)\right)$

The same proof holds for $\overline{\Pi}$.

(iii). $F = k(\alpha)$

$$\begin{array}{c} \overline{E} \\ | \\ k(\alpha) = F \\ | \\ k \end{array} \qquad \alpha \begin{pmatrix} \alpha \\ | \\ k(\alpha) = F \\ | \\ k \end{pmatrix} r$$

α ~~$f_\alpha(x) = \overline{\Pi}(x-$~~

$\mathrm{Hom}_k(F, \overline{k}) \xleftrightarrow{1-1}$ roots of f_α

$\{\sigma_1 \cdots \sigma_r\}$

$f_\alpha(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_r(\alpha))$

$(x - \alpha)$

$= x^r - \left[\left(\sum_i \sigma_i\right)(\alpha)\right] x^{r-1} + \cdots + (-1)^r \left(\prod_i \sigma_i\right)(\alpha)$

$= x^r \pm a_1 x^{r-1} + \cdots + (-1)^r a_r$

$m_\alpha : k(\alpha) \longrightarrow k(\alpha)$

$k\{1, \alpha, \ldots, \alpha^{r-1}\} \quad k\{1, \alpha, \cdots \alpha^{r-1}\}$

$$m_\alpha\{1, \alpha, \cdots \alpha^{r-1}\} = \{1, \alpha, \ldots \alpha^{r-1}\} \begin{pmatrix} 0 & 0 & & (-1)^{r-1} a_r \\ 1 & 0 & & \vdots \\ \cdot & 1 & \ddots & \\ 0 & & \ddots & a_1 \end{pmatrix}_{r \times r}$$

$$\alpha^r = a_1 \alpha^{r-1} - a_2 \alpha^{r-2} + \cdots + (-1)^{r-1} a_r$$

$$\Rightarrow \det(m_\alpha) = \left[(-1)^{r-1}\right]^2 a_r = a_r = \left(\prod_i \sigma_i\right)(\alpha)$$

$$= N_{k(\alpha)/k}(\alpha)$$

$$\left.\begin{array}{l} \\ \\ \end{array}\right\} \quad tr(m_\alpha) = a_1 = \left(\sum_i \sigma_i\right)(\alpha) = \mathrm{Tr}_{k(\alpha)/k}(\alpha).$$

Now take any F-basis $\{w_1, \dots, w_d\}$ of E/F.

Then

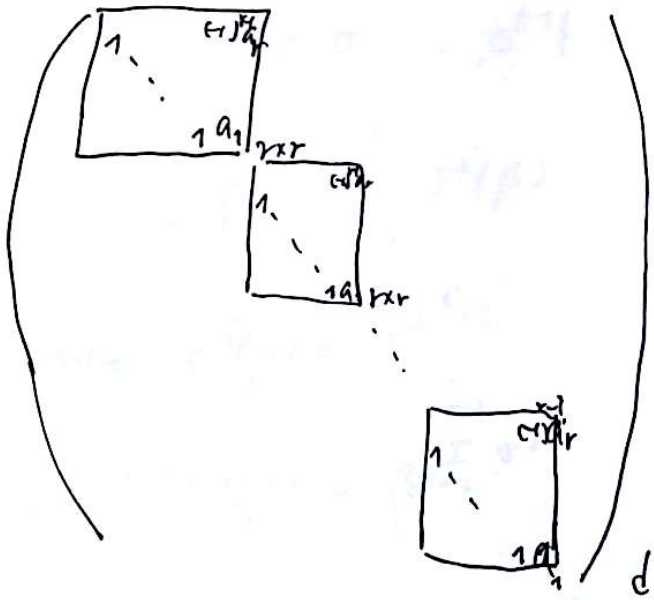
$$\{w_1 \dots w_d,\ w_1\alpha, \dots w_d\alpha, \dots,\ w_1\alpha^{r-1} \dots w_d\alpha^{r-1}\}$$

k-basis of E/k.

Then

$$m_\alpha\{w_1, w_1\alpha, \dots, w_1\alpha^{r-1}, \dots, w_d, w_d\alpha, \dots, w_d\alpha^{r-1}\}$$

$$= \{w_1, w_1\alpha, \dots w_1\alpha^{r-1}, \dots; w_d, w_d\alpha, \dots w_d\alpha^{r-1}\}$$



Clearly: $\det(m_\alpha) = a_r^d = N_{k(\alpha)/k}(\alpha)^d = N_{k(\alpha)/k}\left(N_{E/k(\alpha)}(\alpha)\right)$

$$\operatorname{tr}(m_\alpha) = d a_1 = \operatorname{Tr}_{k(\alpha)/k}\left(\operatorname{Tr}_{E/k(\alpha)}(\alpha)\right). \quad \#$$

Theorem (Hilbert 90.) K/k cyclic of order n, $G = \langle \sigma \rangle$

(I) (multiplicative form).

$\beta \in K$

$N_{K/k}(\beta) = 1 \iff \beta = \frac{\alpha}{\sigma\alpha}$ for some $\alpha \in K$.

(II) (additive form)

$\beta \in K$,

$Tr_{K/k}(\beta) = 0 \iff \beta = \alpha - \sigma\alpha$ for some $\alpha \in K$

Pf: (I) ($\Leftarrow$) easy.

($\Rightarrow$). $G = \{1, \sigma, \ldots, \sigma^{n-1}\}$

$$N_{K/k}(\beta) = \prod_{i=0}^{n-1} \sigma^i(\beta)$$

write $\sigma^i(\beta) = \beta^{\sigma^i}$.

write $\prod_i \sigma^i(\beta) = \beta^{\sum_{i=0}^{n-1} \sigma^i}$

we want to solve α for

$$\beta \cdot \alpha^{\sigma} = \alpha \qquad (*)$$

we write $\alpha = \sum_{i=0}^{n-1} a_i(\beta)\sigma^i$, put into (*), get

$$\sum \beta\sigma(a_i(\beta))\cdot\sigma^{i+1} = \sum a_i(\beta)\sigma^i$$

get Thus get

$$\left.\begin{aligned} a_0(\beta) &= \beta\,\sigma(a_{n-1}(\beta)) \\ a_1(\beta) &= \beta\cdot\sigma(a_0(\beta)) \\ &\vdots \\ a_{n-1}(\beta) &= \beta\cdot\sigma(a_{n-2}(\beta)) \end{aligned}\right\} \Rightarrow a_{n-1}(\beta) = \beta^{\sum_{i=0}^{n-1}\sigma^i}\sigma^n(a_{n-1}(\beta))$$

No contradiction, since $\beta^{\sum_{i=0}^{n-1}\sigma^i} = 1$

$\{\sigma^n = id$

Thus, for simplicity, let

$$a_{n-1}(\beta) = 1. \Rightarrow$$

$$a_0(\beta) = \beta \Rightarrow$$

$$a_1(\beta) = \beta^{1+\sigma} \Rightarrow$$

$$\vdots$$

$$a_{n-2}(\beta) = \beta^{\sum_{i=0}^{n-2}\sigma^i}$$

Now apply Artin's thm on character, $\exists\,\theta \in K$, s.t

$$\alpha = \beta\cdot\theta + \beta^{1+\sigma}\sigma(\theta) + \cdots + \beta^{\sum_{i=0}^{n-2}\sigma^i}\sigma^{n-2}(\theta) + \sigma^{n-1}(\theta) \neq 0$$

Certainly α^{ϵ^k} satisfies the eqn (*).

(II) ($\Leftarrow$) easy

($\Rightarrow$). Take θ, $tr\theta \neq 0$. set $\alpha = \frac{1}{tr\theta}[\beta\theta^{\sigma} + (\beta+\sigma\beta)\theta^{\sigma^2} + \cdots + (\beta+\sigma\beta+\cdots+\sigma^{n-2}\beta)\theta^{\sigma^{n-1}}]$

Again, set $\alpha = \sum b_i(\beta)\sigma^i$, solve. Then check.

$\sigma(\alpha)+\beta = \alpha$ (**) $\beta = \alpha - \sigma\alpha$

#

$\Rightarrow \sum \sigma(b_i(\beta))\sigma^{i+1} + \beta = \sum b_i(\beta)\sigma^i$

$b_0(\beta) = \beta + \sigma(b_{n-1}(\beta))$

$b_1(\beta) = \sigma(b_0(\beta)) \Rightarrow b_1(\beta) = \beta^{\sigma} + \sigma^2(b_{n-1}(\beta))$

$\vdots$ $\vdots$

$b_{n-1}(\beta) = \sigma(b_{n-2}(\beta)) \Rightarrow b_{n-1}(\beta) = \beta^{\sigma^{n-1}} + \sigma^n(b_{n-1}(\beta))$

Again: $\Rightarrow b_{n+1}(\beta) = \beta^{\sigma^{n-1}} + b_{n-1}(\beta) \Rightarrow \beta^{\sigma^{n-1}} = 0 \Rightarrow \beta = 0$ ↯.

Notice that $Tr(\beta) = \beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-1}} = 0$

$\Rightarrow$ ...

Theorem 1: $(\operatorname{char} k, n) = 1$. or $\operatorname{char} k = 0$.

Assume k contains a primitive $n^{\text{-th}}$ root of unity

($\Leftrightarrow$ $x^n = 1$ has n solutions in k)

(i). Let K be a cyclic extension of deg n.

Then $\exists\ \alpha \in K$, s.t $K = k(\alpha)$. and α satisfies

$$x^n - a = 0 \quad \text{for some } a \in k$$

(ii) Conversely, let $a \in k$. Let α be a root of $x^n = a$.

The $k(\alpha)$ is cyclic over k, of degree d/n

and $\alpha^d \in k$.

Theorem 2: (Artin–Schreier) $\operatorname{char} k = p > 0$

(i) Let K be a cyclic extension of k of deg p. Then $\exists \alpha \in K$,

s.t $K = k(\alpha)$, and α satisfies an eqn of form

$$x^p - x - a = 0, \quad \text{for some } a \in k$$

(ii) Conversly, given $a \in k$, the poly $x^p - x - a$ either has

one root in k, in which case all its roots are in k, or it

is irreducible. In the latter case $k(\alpha)/k$ is cyclic of deg p. for any

α a root of $x^p - x - a$.

Pf of Thm 1:

(i) Let ζ be a primitive n^{th} root of 1.

Then $\zeta \in k, \Rightarrow N_{k/k}(\zeta)^{-1} = (\zeta^{-1})^n = 1.$

Hilbert 90 $\Rightarrow$ $\exists \alpha \in k$, s.t

$$\zeta^{-1} = \frac{\alpha}{\sigma(\alpha)}$$

$$\Leftrightarrow \sigma(\alpha) = \zeta \cdot \alpha$$

$$\Rightarrow \sigma^i(\alpha) = \zeta^i \alpha, \quad \forall\ 0 \le i \le n-1$$

$\zeta^i \alpha + \zeta^j \alpha$ if $i \neq j$

Thus $[k(\alpha) : k] \ge n$

$$\Rightarrow [k(\alpha) : k] = n.$$

Note $\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta\alpha)^n = \alpha^n$

Thus $\alpha^n \in k^G = k$

i.e. $\alpha^n = a \in k$.

(ii) ~~Let d be the minimal power, s.t~~

As $\zeta \in k$, $k(\alpha)/k$ is galois

$G = G(k(\alpha)/k)$. Define a map $G \xrightarrow{\phi} \mathbb{Z}/n\mathbb{Z}$, by

$$\sigma \longmapsto \frac{\sigma(\alpha)}{\alpha}$$

Note

$\sigma(\alpha) = \xi^{i(\sigma)} \cdot \alpha$, $\xi \in k$

$\tau(\sigma(\alpha)) = \tau(\xi^{i(\sigma)} \cdot \alpha) = \xi^{i(\sigma)} \cdot \xi^{i(\tau)} \cdot \alpha = \xi^{i(\sigma)+i(\tau)} \cdot \alpha$

$\Rightarrow \phi$ is a gp homo, and obviously injective.

Thus G is cyclic. Assume $|G| = d \mid n$

Then $G = \langle \sigma \rangle$, $\sigma(\alpha^d) = (\sigma(\alpha))^d = \xi^{\frac{n}{d} \cdot d} \cdot \alpha^d = \alpha^d$

with $\sigma(\alpha) = \xi^{\frac{n}{d}} \cdot \alpha$.

$\Rightarrow \alpha^d \in k(\alpha)^G = k$ (Thus the min. poly of α is of the form $x^d - b$, $b \in k$)

#

Pf of Thm 2: (i). $\operatorname{Tr}_{K/k}(1) = p \cdot 1 = 0$. Thm Hilbert 90 $\Rightarrow$

$\exists \alpha \in K$ s.t. $1 = \sigma\alpha - \alpha$

$\Rightarrow \sigma^i(\alpha) = \alpha + i$, $i = 0, \dots, p-1$.

$\Rightarrow [k(\alpha) : k] \geq p \Rightarrow k(\alpha) = K$.

Note: $\sigma(\alpha^p - \alpha) = (\sigma(\alpha))^p - \sigma(\alpha)$

$= (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha$

$\Rightarrow \alpha^p - \alpha \in K^G = k$

(ii) Given $x^p - x - a = 0$, $a \in k$.

if $\alpha \in$ is a root, then

$\{\alpha, \alpha+1, \ldots \alpha+p-1\}$ are roots of $x^p - x - a$.

Thus, if $\alpha \in k$, then all root are in k.

Now, assume $\nexists\ \alpha \in k$, s.t α is a root of $x^p - x - a$.

But then claim: $f(x) = x^p - x - a$ irreducible.

If not, $f = g \cdot h$, $\deg g < p$, $\deg h < p$

with $g, h \in k[x]$

But $g(x) = (x - \alpha - i_1) \cdots (x - \alpha - i_d), \in k[x]$

$\{i_1 \ldots i_d\} \subsetneq \{0, 1, \ldots, p-1\}$.

Then: $d\alpha + \sum_{\ell=1}^{d} i_\ell \in k$ (it is the coeff of x^{d-1} in g)

$\Rightarrow \alpha \in k$ $\lightning$.

Then $k(\alpha)/k$ galois (it is the splitting field of the sep. poly $x^p - x - a$)

Then $G(k(\alpha)/k) \xrightarrow{\phi} \mathbb{Z}/p\mathbb{Z}$ is a grp hom

$\sigma \longmapsto \phi(\sigma) = \sigma(\alpha) - \alpha$

$\Rightarrow G(k(\alpha)/k) \cong \mathbb{Z}/p\mathbb{Z}$. $\#$

Complement to the proofs of Thm 1, (i), Thm 2 (i):

In Thm 1, (i), one used Hilbert 90. to get
(multiplicative form)

$$\alpha \in K, \text{ s.t } \sigma(\alpha) = \xi_i \alpha.$$

This can be also proven without Hilbert 90.:

Take any $\tilde{\alpha} \in K$, s.t $K = k(\tilde{\alpha})$.

Let $\{1, \tilde{\alpha}, \dots, \tilde{\alpha}^{n-1}\}$ be a k-basis of K.

Write $\sigma\{1, \tilde{\alpha}, \dots, \tilde{\alpha}^{n-1}\}$

$$= \{\sigma(1), \sigma(\tilde{\alpha}), \dots (\sigma(\tilde{\alpha}))^{n-1}\}$$

$$= \{1, \tilde{\alpha}, \dots, \tilde{\alpha}^{n-1}\} \cdot A_\sigma \quad \text{with } A_\sigma \in GL_n(k).$$

It is to find a

$$\alpha = \sum \lambda_i \tilde{\alpha}^i \in K, \text{ s.t } \sigma(\alpha) = \xi \cdot \alpha$$

Note $\sigma^n = 1 \Rightarrow$ the char. poly of A_σ is equal to

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \xi^i)$$

Consider $\sigma - \xi^i \mathrm{Id} : K \longrightarrow K \quad \forall i$

Put, $K_{\xi^i} = \ker(\sigma - \xi^i \mathrm{Id})$. Then it is

stand to show that $K_{\xi^i} \neq \{0\}$, and $K = \bigoplus_{i=0}^{n-1} K_{\xi^i}$

Then, $\dim_k K_{g^i} = 1$.

Take $\alpha \in K_{g^1}$. we get the result..

(Note that $K_{g^i} = k\{\alpha^i\}$, $i = 0, \ldots, n-1$.

In Thm 2, (i), one used Hilbert 90, add. form to get

$\alpha \in K$, s.t $\sigma(\alpha) = \alpha + 1$.

This can be also obtained without using Hilbert 90. :

Note in char p.

$$x^p - 1 = (x-1)^p.$$

Then, we consider k-lin. maps:

$$(\sigma - id)^i : K \longrightarrow K, \quad i = 0, \ldots p-1.$$

Put $V_i = \ker(\sigma - id)^i$,

$W_i = \operatorname{im}(\sigma - id)^i$

then $K = V_p \supset V_{p-1} \supset \cdots \supset V_0 = \{0\}$

$\{0\} = W_p \subset W_{p-1} \subset \cdots \subset W_0 = K$

one has $K = V_i \oplus W_i$, $\forall i$

$W_i \subsetneq W_{i-1} \Rightarrow \dim W_i = p - i$ $i = 0 \ldots p$

$\Rightarrow \dim V_i = i$

Thus $\dim V_{n-1} = 1$.

Take $\alpha \in V_1$. Then

$(\sigma - id)\alpha = 0$.

Clearly $V_1 = \{1\}$.

and $V_2 = \{1, \tilde{\alpha}\}$. with

$0 \neq \sigma(\tilde{\alpha}) - \tilde{\alpha} \in V_1 \Rightarrow \sigma(\tilde{\alpha}) = \tilde{\alpha} + i$.

$(\sigma - i\mathrm{id})(\tilde{\alpha}) \Rightarrow \sigma(\frac{1}{i}\tilde{\alpha}) = \frac{1}{i}\tilde{\alpha} + 1$

$\frac{1}{i}\tilde{\alpha} = \alpha$, $\frac{1}{i}\tilde{\alpha} = \alpha$.

Note, we are able to find a basis of K

$\{1, \alpha, e_2, \dots e_p\}$.

$\alpha = e_1$, e_2

s.t

$$\sigma\{e_1, e_2 \dots, e_p\} = \{e_1 \dots e_p\} \begin{pmatrix} 1 & 1 & & 0 \\ & 1 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix}.$$

#

Lecture 15. Solvable and radical extensions

Def 1: E/k. finite, separable. is said to be solvable if

$G(\tilde{E}/k)$ is solvable group, where $\tilde{E}$ = galois closure of E over k.

Def 2: F/k fin. sep is said to be solvable by radicals if $\exists$ finite ext $\bar{E}/F$ admitting a tower

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$$

such that each step E_{i+1}/E_i is one of the following types

(1) it is obtained by adjoining a root of unity

(2) it is obtained by adjoining a root of a polynomial $x^n - a$ with $a \in E_i$, and n prim to $\operatorname{char} k$.

(3) it is obtained by adjoining a root of $x^p - x - a$ with $a \in E_i$, if $p = \operatorname{char} k > 0$.

Theorem: E/k fin. sep. Then

E/k is solvable iff E/k is radically solvable by

Corollary (E. Galois). Let $f \in k[x]$, seperable poly. That E be the splitting field of f ovr k. Then

E/k solvable by radicals $\iff$ $\mathrm{Gal}(f)$ is solvable group.

Corollary: $k = k[c_1, \dots, c_n]$.

$$f(x) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n \in k[x]$$

Then $\{x_1, \dots, x_n\}$ be roots of f in an alg. closure of k.

$$E = k(x_1, \dots, x_n).$$

Then E/k is solvable by radicals iff $n \leq 4$.

Pf: it suffices to show

$$G(E/k) = S_n.$$

$$(x - x_1) \cdots (x - x_n) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n$$

$$\Rightarrow \quad c_1 = c_1(x_1, \dots, x_n) = x_1 + \cdots + x_n$$

$$\vdots$$

$$c_n = c_n(x_1, \dots, x_n) = x_1 \cdots x_n$$

Thus $E = k(x_1, \dots, x_n)$

Clearly $S_n \times k(x_1, \dots, x_n) \longrightarrow k(x_1, \dots, x_n)$

$$\sigma, f(x_1, \dots, x_n) \longmapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

$$\Rightarrow \quad S_n \leq \mathrm{Aut}(k(x_1, \dots, x_n))$$

By Galois's theorem, we know

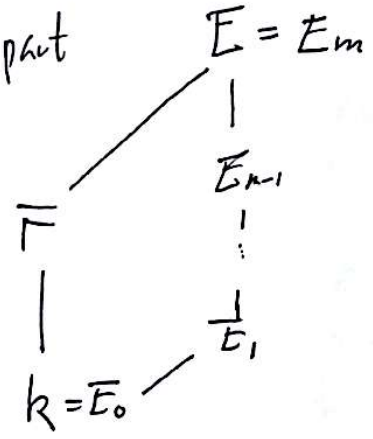
$$K(x_1 \dots x_n)^{S_n} = K(\sigma_1 \dots \sigma_n).$$

By Artin's thm, we know that

$$G(\underbrace{K(x_1 \dots x_n)}_{E} \mid \underbrace{K(\sigma_1 \dots \sigma_n)}_{k}) = S_n. \qquad \#.$$

Pf of theorem:

($\Rightarrow$) if part



(1) $E_{i+1} = E_i(\xi)$. $\xi^n = 1$. (primitive).

$G(E_{i+1}/E_i)$ galois

$G(E_{i+1}/E_i) \leq (\mathbb{Z}/n)^\times$. hence abelian.

(2) easy case: if E_i contains a primitive n^{th} root.

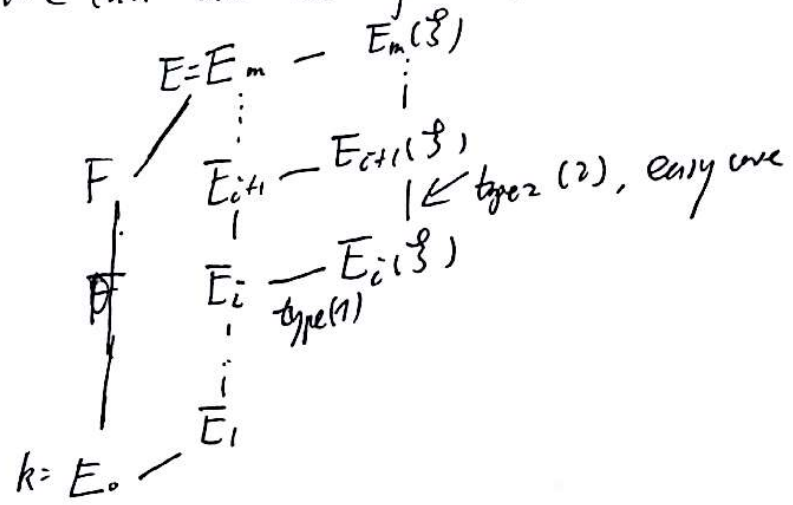
then we know that $G(E_{i+1}/E_i)$ is cyclic

General case:

If E_i does not contain a primitive n^{th} root of unity,

then $\bar{E}_{i+1}/\bar{E}_i$ is not galois.

We can do as follows:



Replace the old tower by the new one,

(3) E_{i+1}/E_i is either trivial or galois and of cyclic ext.

$(1)+(2)+(3) \Rightarrow \exists$

$\tilde{E}$ s.t $G(\tilde{E}/k)$ solvable

(i.e $G(\tilde{E}/k) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_N \triangleright \{e\}$

s.t G_i/G_{i+1} abelian)

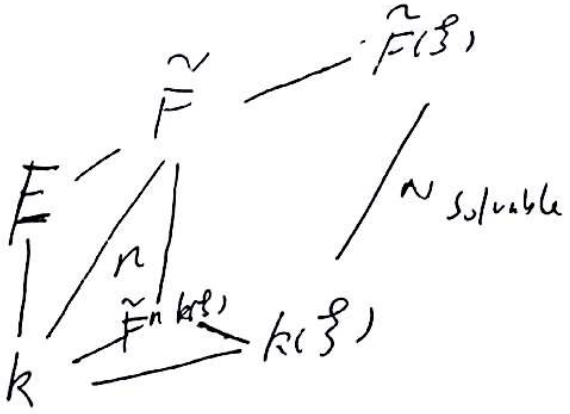
F

k

$\Rightarrow$ $G(\tilde{E}/k) \twoheadrightarrow G(F/k)$ is also solvable.

($\Leftarrow$) only if part.

Assume E/k solvable.



$\tilde{F}$ = galois closure of F/k.

$[\tilde{F}:k]=n$. Let ζ be a primitive n^{th} root of unity.

Then $G(\tilde{F}(\zeta)/k(\zeta)) \cong G(\tilde{F}/\tilde{F}\cap k(\zeta)) \leq G(\tilde{F}/k)$

$\Rightarrow$ ~~$[\tilde{F}:k]$~~ $[\tilde{F}(\zeta):k(\zeta)]\,|\,n$ & $G(\tilde{F}(\zeta)/k(\zeta))$ solvable

$G(\tilde{F}(\zeta)/\tilde{F}) \simeq G(k(\zeta)/k(\zeta)\cap F) \leq G(k(\zeta)/k)$

$G(\tilde{F}(\zeta)/\tilde{F}) \hookrightarrow G(\tilde{F}(\zeta)/k) \twoheadrightarrow G(\tilde{F}/k)$

$\Rightarrow G(\tilde{F}(\zeta)/k)$ solvable

$\Rightarrow \exists$ cyclic tower

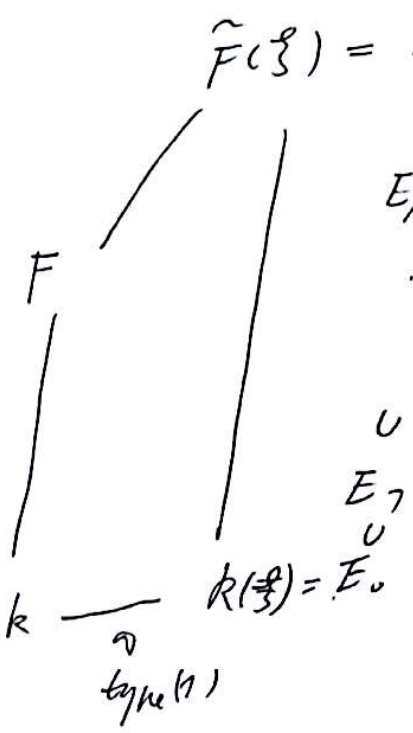
$G(\tilde{F}(\zeta)/k(\zeta)) = G_0 \rhd G_1 \rhd \cdots \rhd G_r \rhd \{e\}$.

s.t G_i / G_{i+1} cyclic of order p_i. p_i : prime number.

Note $p_i \mid [\tilde{F}(\zeta) : k(\zeta)]$, hence $p_i \mid n$.

Thus $k(\zeta)$ contains p_i-th roots of unity.

Now by the galois correspondence., and results we proved last lecture, we know



E_i / E_{i-1} is of type (2) or (3)

and E_0 / k is of type (1)

$\Rightarrow F/k$ is solvable by radicals.

#

END OF LECTURE.