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~~ $\Leftrightarrow$ 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 $\Leftrightarrow$ $|G(K|k)| = [K:k]$

Note: we have the natural group action:

$$G \times K \longrightarrow K$$
$$(\sigma, x) \longmapsto x^\sigma$$

For $H \leq G$, ~~et~~ 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)

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

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

$$K^H \longleftarrow H$$

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

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

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

Then $E|k$ Galois $\iff H \trianglelefteq G$

Moreover, one has an isomorphism

$$\begin{array}{ccc} G/H & \xrightarrow{\sim} & G(E|k) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ [\sigma] & \longmapsto & \sigma|_E \end{array}$$

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 $H = \{g_1, \ldots, g_n\} \leq G$. Consider

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

The coeffs of $f(x)$ ~~are~~ 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

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

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

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

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

$$\underline{\le} \deg f(x) = n = \underline{|H|}$$

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

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

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

Now:

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

Thus,

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

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 $\Rightarrow \forall g \in G,\ g(E) = E$

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

$\Rightarrow H \triangleleft G$.

Conversely, assume $H \triangleleft G$.

Consider

$$\begin{tikzcd}
 & & \bar{k} \\
K \arrow[d, dash] & & \\
E \arrow[d, dash] \arrow[uurr, "\sigma"] & & \\
k \arrow[uuurr, dash] & &
\end{tikzcd}$$

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

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

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

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

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

Assume: $E|k$ galois. Consider

$$\begin{array}{ccc} G & \xrightarrow{\ \phi\ } & G(E|k) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \sigma & \longmapsto & \sigma|_E \end{array}$$

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

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

Set $\{\underset{\overset{\parallel}{id}}{\sigma_1}, \dots \sigma_n\} = G$.

prove by contradiction: Assume the contrary that

$[K:k] > n$.

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

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

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

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

$$\lambda_1 v_1 + \dots + \lambda_r v_r = 0 \quad , \quad \underset{\lambda_i \in K}{\overset{0 \ \forall i}{\not\parallel}}$$

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

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

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

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

$$\left[\sigma(\tilde{\lambda}_2) - \cancel{\sigma(\lambda_2)}\,\tilde{\lambda}_2\right] v_2 + \cdots + \left[\sigma(\tilde{\lambda}_r) - \tilde{\lambda}_r\right] v_r = 0.$$

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

or

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

Both are impossible!

Lemma:

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

If $\forall \alpha \in E$, $[k(\alpha):k] \leq n$,

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

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

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

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

$$\begin{tikzcd} & k(\alpha,\beta) \arrow[dl, dash] \arrow[dr, dash] & \\ k(\alpha) \arrow[dr, dash] & & k(\beta) \arrow[dl, dash] \\ & k & \end{tikzcd}$$

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

Primitive Element Theorem

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

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

#

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

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

σ

Consider

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

Then $\forall \sigma \in G$, $\sigma(C_i(\alpha_1, \dots \alpha_d)) = C_i(\alpha_1 \dots \alpha_d)$, $\forall i$

$\Rightarrow C_i(\alpha_1 \dots \alpha_d) \in K^G = k$

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

$f_\alpha \mid f$

$\Rightarrow \begin{cases} (1) & \cancel{\text{the minimi}}\ f_\alpha \text{ seperable} \Rightarrow K/k \text{ seperable} \\ (2) & \cancel{\deg f}\ [k(\alpha):k] \le d \le n \end{cases}$

$\xRightarrow{\text{step 1}} [K:k] \le n.$ #

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

Prop. (1)
$$\begin{tikzcd} & KF \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash, "\text{galois}"'] & & F \arrow[dl, dash, "\text{extension}"] \\ & k & \end{tikzcd} \Rightarrow KF/F \text{ galois}$$

(2)
Moreover, if
$$\begin{tikzcd}[column sep=small]
 & \bar{k} \arrow[dl, dash] \arrow[dr, dash] & \\
 & KF & \\
K \arrow[ur, dash] \arrow[dr, dash] & & F \arrow[ul, dash] \arrow[dl, dash] \\
 & K\cap F \arrow[d, dash] & \\
 & k &
\end{tikzcd}$$
, then

$$G(KF/F) \simeq G(K/K\cap F) \leq G(K/k)$$
$$\sigma \longmapsto \sigma|_K$$

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

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

$$\begin{tikzcd}
G(KF/F) \arrow[r] \arrow[d, phantom, "\leq" rotate=90] & G(K/K\cap F) \arrow[d, phantom, "\leq" rotate=90] \\
G(KF/k) \arrow[r] & G(K/k)
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
 & KF & \\
K \arrow[ur, dash] & & F \arrow[ul, dash] \\
 & K\cap F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

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

To see $\operatorname{im}(\phi) = G(K/_{K\cap F}) \leq G(K/_k)$, we

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

Since $\operatorname{im}(\phi) \subset G(K/_{K\cap F})$, $K^{\operatorname{im}(\phi)} \supset K\cap F$.

Claim that: $K^{\operatorname{im}(\phi)} = K\cap F$.

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

Use Galois correspondence for galois ext $KF/_F$.

$\alpha \in F$.

Thus $\alpha \in K\cap F$. Done.!

#

Prop 2:

$$\begin{tikzcd}[column sep=small]
 & \bar{k} \arrow[d, dash] & \\
 & K_1K_2 & \\
K_1 \arrow[ur, dash] & & K_2 \arrow[ul, dash] \\
 & k \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

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

$\Rightarrow K_1K_2/_k$ galois

Moreover:

$$\begin{array}{ccccc}
G & & G_1 & & G_2 \\
\wr\wr & & \wr\wr & & \wr\wr \\
G(K_1K_2/k) & \overset{\phi}{\hookrightarrow} & G(K_1/_k) & \times & G(K_2/_k), \\
\sigma & \longmapsto & (\sigma/_{K_1} & ; & \sigma/_{K_2})
\end{array}$$

ϕ is an iso, if $k = K_1\cap K_2$.

Pf: K_1K_2
$|$ galois 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 $\mathrm{char}(k) \nmid n$.

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

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

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

Note: $\forall \sigma \in G(k(\zeta_n)|k)$,

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

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

This is easy: $\forall \tau \in G(k(\zeta_n)|k)$

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

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:

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

clearly, ϕ is inj.

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

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

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

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

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

pf: $(n,m)=1$, then $\zeta_n \cdot \zeta_m$ is a primitive root of order $n \cdot m$.

Thus $\mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$

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

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

& ($\mathbb{Z}/n \cdot m \simeq \mathbb{Z}/n \times \mathbb{Z}/m$, ring isomorphism. Chinese Remainder Theorem)

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{nm}) \arrow[dl, dash] \arrow[dr, dash, "\phi(nm)"] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash] \arrow[ddr, dash, bend right, "\phi(m)"'] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[ddl, dash, bend left, "\phi(n)"] \\
 & \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$G(\mathbb{Q}(\zeta_{nm}) | \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m))$$

$$\simeq G(\mathbb{Q}(\zeta_n) | \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) \times$$

$$G(\mathbb{Q}(\zeta_m) | \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)).$$

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

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

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

#

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 $\deg f_{\zeta_n} = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$

$$= \left| G(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \right| \le \phi(n).$$

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. $g(x^p) = f_{\zeta_n}(x)\, h(x)$ (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)

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

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

$\supset (\bar{f}_{\zeta_n})$

#

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: $p \in$ prime number.

Then one can use compass and rule to draw regular p-gon $\Longleftrightarrow$ 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 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: ~~Ab~~

$F = \{ a ~~(a\neq 0)~~ \text{ constructible number} \} \subset \mathbb{R}$

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

(2) $\forall$ finitely many $a_1, \ldots, a_n \in F$, there exists a tower

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

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

(ii) $K_i = K_{i-1}(\sqrt{r_i})$. for some $r_i \in \mathbb{R}_{\geq 0}$ 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: $a \in F \xRightarrow{\text{Prop.(2)}} [\mathbb{Q}(a) : \mathbb{Q}] = 2^r$

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

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

$$\parallel$$

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

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

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

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.

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

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

$$\begin{tikzcd}
\mathbb{Q}(\xi_p) \arrow[dd, no head] \arrow[dr, no head] & \\
& \mathbb{Q}(\cos\frac{2\pi}{p}) \arrow[dl, no head] \\
\mathbb{Q} &
\end{tikzcd}$$

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

and since

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

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

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

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

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

p prime

$$\Rightarrow p = 2^{2^n} + 1.$$

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

$$\frac{\mathbb{Z}}{2^{2^n}} \simeq G(\mathbb{Q}(\xi_p)|\mathbb{Q}) \twoheadrightarrow G(\mathbb{Q}(\cos\frac{2\pi}{p})|\mathbb{Q})$$

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

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

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

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

Thus, 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 $r_i \in K_{i+1}$, $r_i^2 \notin K_i$.

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

#