30th Jan:

Def: A field extension M/K is basic if $M = K(\alpha)$ for some $\alpha \in M$

Let $M = K(\alpha)$ be a basic extension of K

then

If α is transcendental over K, then

$K(\alpha) \cong K(t)$ is a K-isomorphism

$$\frac{f(\alpha)}{g(\alpha)} \longrightarrow \frac{f(t)}{g(t)}$$

Cor: upto K-isomorphism, $\exists$ unique basic extension $K(\alpha)$ with α transcendental over K

Eg: $\mathbb{Q}(\sqrt{\pi}) \cong \mathbb{Q}(\pi^5)$ as $\mathbb{Q}$-isomorphism

Basic extension generated by π^5

$\mathbb{Q}(\sqrt{\pi}), \mathbb{Q}(\pi^5)$ are both extn of $\mathbb{Q}(\pi^{10})$

Note: above is not isomorphic as extensions of $\mathbb{Q}(\pi^{10}) \subset \mathbb{Q}(\sqrt{\pi})$

but $\mathbb{Q}(\sqrt{\pi}), \mathbb{Q}(\pi^5)$ $\mathbb{Q}(\pi^{10}) \subset \mathbb{Q}(\pi^5)$ not $\mathbb{Q}(\pi^{10})$ isomorphic

$\mathbb{Q}(\sqrt{\pi}) = K(\sqrt{\pi})$ $\quad K = \mathbb{Q}(\pi^{10})$

↑ over K $\exists$ generator $\sqrt{\pi}$

but $\sqrt{\pi}$ is algebraic over K as

$t^{20} - \pi^{10} \in K[t]$ has

$(\sqrt{\pi})^{20} - \pi^{10} = 0$

$$\min_K \sqrt{\pi} = t^{20} - \pi^{10} \Rightarrow \mathbb{Q}(\sqrt{\pi}) \cong \frac{K[t]}{\langle t^{20} - \pi^{10} \rangle}$$

Note: that $\min_K \sqrt{\pi} = t^{20} - \pi^{10}$ → will come later in course

$\mathbb{Q}(\pi^5) = K(\pi^5) \cong \dfrac{K[t]}{\langle t^2 - \pi^{10} \rangle}$ $\quad \min_K (\pi)^5 = t^2 - \pi^{10}$

Note: that $\min_K (\pi)^5 = t^2 - \pi^{10}$ → will come later in course

$$\frac{K[t]}{\langle t^{20} - \pi^{20} \rangle} = \text{span}\{1, t, t^2, \ldots t^{19}\}$$

↳ dim = 20

$$\frac{K[t]}{\langle t^2 - \pi^{10} \rangle} = \text{span}\{1, t\}$$

↳ dim = 2

not vector space isomorphism ⇒ not isomorphic as fields

now let $M = K(\alpha)$, α: algebraic over K then

$m(t) = \min_K \alpha \in K[t]$ of deg $\neq 1$

and $K(\alpha) \cong \frac{K[t]}{\langle m(t) \rangle}$

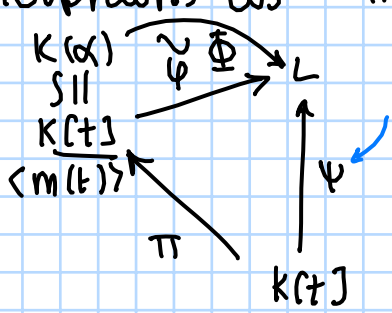
↑ monic and irreducible (unique)

$L|_K$ be any field extension, $\beta \in L$ (algebraic / K)

$\min_K \beta = m(t)$ then

$\exists$ unique K-homomorphism $\varphi: K[\alpha] \longrightarrow L$ $\quad \varphi_K = id$, $\varphi(\alpha) = \beta$
$\alpha \longmapsto \beta$

this map is Homomorphism as $K[\alpha] \cong \frac{K[t]}{\langle m(t) \rangle} \longrightarrow L$, π: $K(t) \to L$, $t \to \beta$



$\psi(t) = \beta$
$\ker(\psi) = \langle m(t) \rangle$

$\tilde{\varphi}$ is well defined and so, $\frac{K[t]}{\langle m(t) \rangle} \cong K(\alpha) \Rightarrow \bar{\Phi}: K(\alpha) \longrightarrow L$

as ψ is unique $\Rightarrow \tilde{\varphi}$ is unique ($\because$ composition)

$\text{img}(\bar{\Phi}) = K[\beta] \cong K[\alpha]$ K-isomorphism

Note: If we have a basic extension $K(\alpha)$, α algebraic / K then it is unique upto K-isomorphism

Theorem: K fields, $\{$ Basic extension $K(\alpha)$ of K upto K-isomorphism $\} \leftrightarrow \{$ monic irreducible polynomial in $K[t] \} \cup \{K(t)\}$

proof: $K(\alpha) \xrightarrow[\bar{\Phi}]{} \min_K \alpha$

$\frac{K[t]}{\langle m(t) \rangle} \leftarrow m(t)$

Note: Not a bijection, but fiber exist as $m(0) \neq m(1)$ but $K(0) \cong K(1)$

So, for $\mathbb{Q}$: $\{$ Basic extensions of $\mathbb{Q}$ upto $\mathbb{Q}$-isomorphism $\} \leftrightarrow \{$ monic polynomials of $\mathbb{Q}[t] \} \cup \{\mathbb{Q}(t)\}$

for $\mathbb{R}$: $\{$ Basic extensions of $\mathbb{R}$ upto $\mathbb{R}$-isomorphism $\} \leftrightarrow \{$ deg 1, deg 2 monic polynomial irreducibles $\} \cup \{\mathbb{R}(t)\}$

as if $f(t) \in \mathbb{R}[t]$ irred, $\deg f > 2$
$\Rightarrow \exists\, \alpha \in \mathbb{C}$ s.t
$f(\alpha) = 0$ in $\mathbb{C}[t] \Rightarrow f(\bar{\alpha}) = 0$ ($\because$ complex conjugate theorem)
$\Rightarrow f(t) = \underbrace{(t-\alpha)(t-\bar{\alpha})}_{\in \mathbb{R}[t]} f'(t)$ & monic, $\deg = 2 \rightarrow \deg > 0$
$\Rightarrow f$ is reducible

Note: $\mathbb{Q}(\underbrace{\sqrt{2}}_{\alpha}) \not\cong \mathbb{Q}(\underbrace{\sqrt{2}+1}_{\beta})$ $\mathbb{Q}$-isomorphism not possible
$\alpha \longmapsto \beta$ diffet minimal polynomial

similarly $\mathbb{R}(i) \not\cong \mathbb{R}(\omega)$ $\mathbb{R}$-isomorphism
$i \longmapsto \omega$ diffet minimal polynomial

Defn: L is a field obtained from k by adjoining a root of $m(t)$ where $m(t)$ is monic irreducible over $k[t]$

then $L = k[\alpha]$, $m(\alpha)=0$
$\cong \frac{k[t]}{\langle m(t)\rangle}$, $t = \alpha$

Note: Above if $m(t)$ is 3 degree in $\mathbb{C}[t]$, then upto isomorphism

$$k[\alpha_1] \cong k[\alpha_2] \cong k[\alpha_3] \cong \frac{k[t]}{\langle m(t)\rangle}$$

Eg: $k=\mathbb{Q}$, $m(t) = t^3-2$

$\alpha_1, \alpha_2, \alpha_3 = 2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}$

then $\mathbb{Q}(\alpha_1) \cong \mathbb{Q}(\alpha_2) \cong \mathbb{Q}(\alpha_3) \cong \frac{\mathbb{Q}[t]}{\langle t^3-2\rangle}$ as $\mathbb{Q}$-isomorphism

Eg: $t^3+t+1 \in (\mathbb{Z}/2\mathbb{Z})[t]$

$(0)+0+1 \neq 0$
$(1)+(1)+1 \neq 0$

So, $t^3+t+1 \in \mathbb{F}_2[t]$ irreducible
let $\alpha^3+\alpha+1 = 0$ root, $|\mathbb{F}_2(\alpha)| = 8$ elements

Eg: $t^2-2 \in \mathbb{F}_3[t]$ irreducible, $\mathbb{F}_3(\alpha)$, $\alpha^2-2=0$

$|\mathbb{F}_3(\alpha)| = 9$ elements

Defn: $M|_K$ field extension, M: vectorspace over K, then $\dim_K M$ or dimension of M over K

$$\dim_K M = [M:K] = \deg \text{ of } M|_K$$

Theorem: $[M:K]=1$ iff $M=K$

proof:
($\Leftarrow$) trivial
($\Rightarrow$) as $K \subseteq M$ and M is vector space over M, basis $= \{e\}$
then $\alpha e = M \Rightarrow M = K$ as $\alpha e \in K$ iff $\alpha e \in M$

Note: All vector space have 0 dim vector space basis $= \phi$

Eg: $[\mathbb{Q}(t):\mathbb{Q}] = \infty$ as $\{1, t, t^2, \ldots\}$ is linearly independent over $\mathbb{Q}$

Exe: find basis of $\mathbb{Q}(t)$ over $\mathbb{Q}$ → done down

Note: $\mathbb{Q}(t)$ is countable, so $[\mathbb{Q}(t):\mathbb{Q}] = |\mathbb{N}|$
as

$$\mathbb{Q}[t] \times \mathbb{Q}[t] \setminus 0 \longrightarrow \mathbb{Q}(t) \text{ is surjective}$$
$$(f, g) \longrightarrow f/g$$

$\Rightarrow |\mathbb{Q}(t)| \leq |\mathbb{Q}[t] \times \mathbb{Q}[t] \setminus 0|$

$\Rightarrow \mathbb{Q}(t)$ is countable

now, $\mathbb{Q}[t]$ is countable as, $\bigcup_{n \geq 0}$ deg n polynomials in $\mathbb{Q}[t] = \mathbb{Q}[t]$

↑ countable as $\cong \mathbb{Q}^{n+1}$ and so countable union of countable sets

Exe: show that $[\mathbb{R}(t) : \mathbb{Q}]$ is uncountable, and $[\mathbb{R}(t) : \mathbb{R}]$ is uncountable → done down

Defn: M/K is finite extension if $[M:K] < \infty$

Defn: M/K is finitely generated if $\exists \alpha_1, \alpha_2 \ldots \alpha_n \in M$ s.t $M = K(\alpha_1 \ldots \alpha_n)$

Eg: $\mathbb{C}/\mathbb{R}$ finite extension

$[\mathbb{C}:\mathbb{R}] = 2$ $\{1, i\}$ = Basis

Theorm: M/K finite extension $\Rightarrow M/K$ is finitely generated

proof: let $\{\alpha_1 \ldots \alpha_n\}$ be basis, then $M = \sum_{i=1}^{n} K\alpha_i$

$\Rightarrow M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$

but, M: f.g field ext $/K \not\Rightarrow M/K$ is finite

$M = K(t)$ but M/K not finite $M = \mathbb{Q}(t)$, $K = \mathbb{Q}$

Defn: $M = K(\alpha)$, α: algebraic over K, $K(\alpha) \cong \frac{K[t]}{\langle m(t) \rangle}$ $m(t) = \min_K \alpha$

deg $m(t) = n$ $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$

i.e $m(\alpha) = 0$

$[K(\alpha):K] = n$ as spanning set $= \{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$ over $K(\alpha)/K$

Exe: show that $\{1, \alpha, \ldots \alpha^{n-1}\}$ is linearly independent over K → done down

Eg: $\alpha = e^{2\pi i/p}$ (p-prime) $K = \mathbb{Q}$

$\alpha - 1 = 0$

$(\alpha - 1)(\alpha^{p-1} + \cdots + \alpha + 1) = 0$

irreducible (done before)

$\Rightarrow m(t) = \alpha^{p-1} + \cdots + \alpha + 1$

deg $p-1$

$\Rightarrow [\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p-1$ for primes

if $p=1$, then $\alpha = e^{2\pi i} = 1 \Rightarrow [\mathbb{Q} : \mathbb{Q}] = 1$

if $p=4$: $[\mathbb{Q}(e^{2\pi i/4}) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2 \neq 4-1$

if $p=15$: $[\mathbb{Q}(e^{2\pi i/15}) : \mathbb{Q}]$

then $\alpha = e^{2\pi i/15}$

$\alpha^{15} - 1 = 0$

minimal polynomial irreducible factor of $t^{15}-1$

$15 = 3 \cdot 5 = (t^3 - 1)(t^{12} + t^9 + t^6 + t^3 + 1)$

$= (t^5 - 1)(t^{10} + t^5 + 1)$

minimal polynomial irreducible factor of both fails

$t^5 - 1 = (t-1)(\deg 4)$ → divide to factor

$t^3 - 1 = (t-1)\ \deg 2$ → divide to factor

deg 8 → final

Note: $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$ $\quad n = \prod_{i=1}^{M} p_i^{e_i}$

$= \prod_{i=1}^{M} \varphi(p_i^{e_i})$

$\varphi(n)$ = no. of generators of $\mathbb{Z}/n$

$\varphi(n) = n \prod_{i=1}^{K} \left(1 - \frac{1}{p_i}\right)$ $\quad n = \prod_{i=1}^{N} p_i^{e_i}$

Exe: show that $\{1, \alpha, \ldots \alpha^{n-1}\}$ is linearly independent over k

Ans:

for $\sum_{i=0}^{n-1} a_i \alpha^i = 0$

diff $n-1$ times $\Rightarrow a_{n-1} = 0$ (wrt α)

similarly $a_0 = 0$ $\forall \varphi$

Exe: find basis of $\mathbb{Q}(t)$ over $\mathbb{Q}$

Ans:

$\text{Basis} = \left\{ t^n \mid n \geq 0 \right\} \cup \left\{ \frac{t^r}{p^k} \;\middle|\; r < \deg(p),\ p \text{ irreducible monic}, k \in \mathbb{N} \right\}$

as ① spans, this is trivial

$\frac{f(t)}{p(t)} = \frac{Q(t)p(t) + r(t)}{p(t)}$

$= Q(t) + \frac{r(t)}{p(t)}$ → turn into irreducibles

$\left(\frac{r^{k-1}}{p^k(t)} + \frac{1}{\ldots} + \frac{1}{\ldots} = \frac{r(t)}{p(t)} \right)$ By partial fraction

② lin independent

as $\sum a_i t^i + \sum B_i \frac{t^r}{p^k} = 0$

now if $\exists \frac{1}{(x-\alpha)}$ in some factor → we make this power 1 by multiplying and then we put $x \to \alpha$ so this blows up

$\Rightarrow$ this has to be 0

so, all terms with $(x-\alpha)$ have to sum to 0

then $\alpha_1 \left(\frac{1}{f(x-\alpha)}\right) + \alpha_2 \left(\frac{1}{g(x-\alpha)}\right)$ s.t $\alpha_1 + \alpha_2 = 0$ then we multiply by $(x-\alpha)$ and do for smaller f, g functions

as all are different, we can get all denominates prior 1 and different, and some nothing in denominator

We blow up by making unique denominator terms 0
⇒ all do same from start
all denominator terms 0
all as $\{1, x, x^2, \ldots\}$ lin ind ⇒ all terms 0

Exe: Show that $[\mathbb{R}(t):\mathbb{Q}]$ is uncountable, and $[\mathbb{R}(t):\mathbb{R}]$ is uncountable

Ans: $[\mathbb{R}(t):\mathbb{Q}]$ uncountable as

$\mathbb{R}\setminus\mathbb{Q}$ in basis which is uncountable (trivially lin ind)

and $[\mathbb{R}(t):\mathbb{R}]$ uncountable as

$\frac{1}{t-\alpha}$ in basis $\forall \alpha \in \mathbb{R}$, so uncountable (lin ind by putting $t \to \alpha$)

3rd Feb:

Theorem: K field

① $m(t) \in K[t]$ monic irreducible, then $\exists$ a pair (M, α) where M/K is field extension

$$M = K(\alpha) \quad \min_K \alpha = m(t)$$

Further, the pair (M, α) is unique upto K-isomorphism

i.e if $\exists (M', \alpha')$ another pair s.t

$$M' = K(\alpha') \quad \min_K \alpha' = m(t)$$ then $\exists$ unique K-isomorphism

$$M \xrightarrow{\varphi} M', \quad \varphi(\alpha) = \alpha'$$

$$\frac{K[t]}{\langle m(t) \rangle} \cong K(\alpha) \cong K(\alpha')$$

② $\exists (M, \alpha)$ s.t α is transcendental $/K$

$$M = K(\alpha) \cong K(t)$$

further, if (M', α') s.t M'/K, α' transcendental $/K$, $M' = K(\alpha')$ then $\exists$ unique K-isomorphism b/w

$$\begin{array}{ccc} K(\alpha) & & K(\alpha') \\ \| & & \| \\ M & \longrightarrow & M' \\ \alpha & \longmapsto & \alpha' \end{array}$$

Eg: $\mathbb{Q}(\sqrt{\pi})$, $\mathbb{Q}(\pi^5)$

M $\quad$ M'

$K(\pi^{10}) = K$

M, M' are basic extensions of $\mathbb{Q}$, by transcendental elements

$\Rightarrow M \cong M'$ $\mathbb{Q}$-isomorphism $\sqrt{\pi} \longrightarrow \pi^5$

M, M' are also extensions of $K = \mathbb{Q}(\pi^{10})$ they are basic over K, but

$\nexists$ K-isomorphism $M \longrightarrow M'$ as if $\exists$ a K-isomorphism $\varphi: M \longrightarrow M'$ then φ is K-linear $\Rightarrow [M:K] = [M':K]$

$\pi^{10} = t$ $\quad$ $\mathbb{Q}(t^{1/20})$ $\quad$ $\mathbb{Q}(t^{1/2})$

$K = \mathbb{Q}(t)$

$\mathbb{Q}(t^{1/2})$: $\dim = 2$ ($\because \min_K t^{1/2} = x^2 - t$)

$\mathbb{Q}(t^{1/20})$: $\dim = 20$ ($\because \min_K t^{1/20} = x^{20} - t$)

but $[M:K] \neq [M':K]$, so they are not K-isomorphic

Eg:

$\mathbb{Q}(\sqrt{t}) = M'$

$\mathbb{Q}(t) = M$

isomorphic over $\mathbb{Q}$ but not isomorphic M

$x^{20} - t$ irreducible in $\mathbb{Q}(t)[x]$:

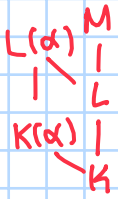
$x^{20} - t$ irreducible in $\mathbb{Q}(t)[x] \in$ irreducible in $\underbrace{\mathbb{Q}[t]}_{\text{UFD}}[x]$ ($\because$ gauss)

$t \in \mathbb{Q}[t]$ irreducible $\Rightarrow$ t is prime ($\because$ UFD)
then $t \nmid 1$, $t \mid -t$ but $t^2 \nmid -t$

then by Eisenstein

$x^{20} - t$ is irreducible in $\mathbb{Q}[t][x]$
$\Rightarrow x^{20} - t$ is irreducible in $\mathbb{Q}(t)[x]$

lemma: $\alpha \in M$,



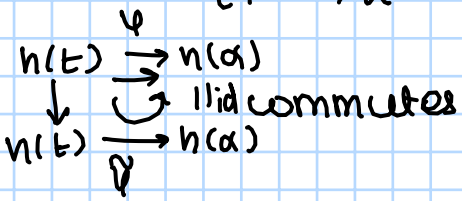
$[L(\alpha):L] = \deg \min_{L} \alpha$ (g) $[K(\alpha):K] = \deg \min_{K} \alpha$ (f)

then $[L(\alpha):L] \leq [K(\alpha):K]$

proof:

$\varphi: K[t] \to M$, $t \mapsto \alpha$ — K-homomorphism, $\ker \varphi = \langle f(t) \rangle$

$\tilde{\varphi}: L[t] \to M$, $t \mapsto \alpha$ — L-homomorphism, $\ker \tilde{\varphi} = \langle g(t) \rangle$



$\Rightarrow \ker \varphi \subset \ker \tilde{\varphi}$

$\| $

$\langle f(t) \rangle \subseteq \langle g(t) \rangle$

$\Rightarrow f(t) = g(t) h(t)$
$\Rightarrow g \mid f$

$\Rightarrow \deg(g) \leq \deg(f)$

so, $[L(\alpha):L] \leq [K(\alpha):K]$

ex: give example where strict inequality holds → done down

M/K, $\alpha_1, \alpha_2, \ldots \alpha_n \in M$: algebraic/K then $K[\alpha_i^\circ] = K(\alpha_i)$

$K[\alpha_1, \alpha_2, \ldots \alpha_n] = K(\alpha_1, \alpha_2, \ldots \alpha_n)$
$\|$
$K(\alpha_1)(\alpha_2, \ldots \alpha_n)$
$\|$
$K[\alpha_1](\alpha_2, \ldots \alpha_n)$
$\|$
$K[\alpha_1](\alpha_2)(\alpha_3, \ldots \alpha_n)$
$\|$
$K[\alpha_1][\alpha_2](\alpha_3, \ldots \alpha_n)$
$\vdots$
$K[\alpha_1][\alpha_2] \cdots [\alpha_n]$
$\|$
$K[\alpha_1, \alpha_2 \ldots \alpha_n]$

if $[K(\alpha_i):K] = d_i^\circ$
then, $K(\alpha_i) = \{ a_0 + a_1 \alpha_i^\circ + \cdots + a_{d_i^\circ - 1} \alpha_i^{d_i - 1},\ a_i \in K \}$

so, $K(\alpha_1, \alpha_2 \ldots \alpha_n) = \operatorname{span} \{ \alpha_1^{m_1} \cdot \alpha_n^{m_n} \mid 0 \leq m_i^\circ < d_i^\circ \}$

for each variable $= d_i \Rightarrow$ total $d_1 \dots d_n$

so, $[K(\alpha_1 \dots \alpha_n) : K] \leq \prod_{i=1}^{n} d_i$

if span also lin ind, then done

ex: find example with strict inequality → done down

now, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \operatorname{span}_{\mathbb{Q}} \{ (\sqrt{2})^i (\sqrt[3]{2})^j \mid i = 0,1,\ j = 0,1,2 \}$

$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$ in this case $= 6$ (trivial)

Theorem: (Tower)



$[L:K] = [L:M][M:K]$

$|I|$ cardinality of basis

proof: $\{e_i : i \in I\}$ basis of $M|K$

$\{f_j : j \in J\}$ basis of $L|M$

$S = \{e_i f_j,\ i \in I,\ j \in J\}$ is basis of $L|K$

as ① $\operatorname{span}_K(S) = L$ ($\because \forall \alpha \in L$, $\alpha = \sum c_i f_j$ $c_i \in M$ $= \sum\sum a_j e_j f_i$ $c_i = \sum a_j e_j$)

② $\sum_{\text{finite}} e_i f_j a_{ij} = 0$ $a_{ij} \in K$

then

$\sum_j \sum_i \underbrace{(a_{ij} e_i)}_{\in M} f_j = 0$

but f_j lin ind over M

$\Rightarrow \sum_i a_{ij} e_i = 0$

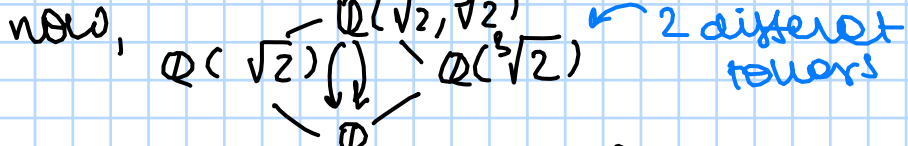
$\Rightarrow a_{ij} = 0$ as $\{e_i \mid i \in I\}$ are lin ind

$\forall i,j$ $a_{ij} = 0$

so, $|S| = |I||J|$

$\Rightarrow [L:K] = [L:M][M:K]$

now,



2 different towers

$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}), \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$

n $\qquad\qquad$ $\underbrace{\qquad}_{2}$

$\Rightarrow 2 \mid n$

similarly $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \Rightarrow 3 \mid n$

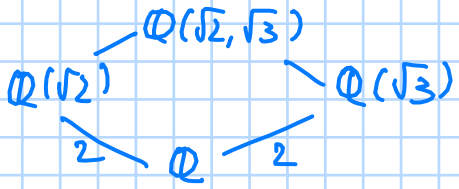
so, $6 \mid n \Rightarrow$ but $n \leq 6$

$\Rightarrow n = 6$

generally, $[M_0 : K] = \prod_{i=0}^{n-1} [M_i : M_{i-1}]$

M_0
|
M_1
|
⋮
|
$M_n = K$

Eg:



$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})] = n$
then $n \leq 2$
↓
deg of minimal polynomial of $\sqrt{2}$ / $\mathbb{Q}(\sqrt{3})$
$t^2 - 2$ → irreducible over $\mathbb{Q}$

Exe: show that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$
Ans:
if $\sqrt{2} = a + b\sqrt{3}$ $a, b \in \mathbb{Q}$
$2 = a^2 + b^2(3) + 2ab\sqrt{3}$
Rational irrational
this is a contradiction, so $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$

so, $\sqrt{2} \notin \mathbb{Q}(\sqrt{3}) \Rightarrow n = 2$ as minimal polynomial $t^2 - 2$

Exe: show $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 8$, i.e $\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$ → done down

Defn: M/K is a finite extension if $[M:K] < \infty$

Defn: M/K is f.g if $M = K(\alpha_1 \dots \alpha_n)$ $\alpha_i \in M$

we have seen f.e ⇒ f.g

Defn: M/K is algebraic if every $\alpha \in M$ is algebraic over K

now, M/K f ⇒ M/K f.g is seen
f ⇒ M/K is algebraic as $\forall \alpha \in M$
$[K(\alpha) : K] = \deg \min_K \alpha$

as
M
|
$K(\alpha)$) finite ⇒ $[K(\alpha) : K] < \infty$ ($\because [M:K] < \infty$ $= [M : K(\alpha)][K(\alpha) : K]$)
|
K
⇒ α is algebraic over K

also, M/K f.g ⇏ M/K algebraic as $M = K(t)$

$M|_K$ f.g $\not\Rightarrow$ $M|_K$ algebraic as $M = \mathbb{Q}(\sqrt{p} : p \text{ is prime})$ ← not f
$M|_{\mathbb{Q}}$ is algebraic ↳ same for $\bar{\mathbb{Q}}$ ← not f

Exe: show that $M|_{\mathbb{Q}}$ $M = \mathbb{Q}(\sqrt{p} : p \text{ is prime})$ is algebraic → done down

$\bar{\mathbb{Q}}$ is a field, as for $\alpha, \beta \in \bar{\mathbb{Q}}$

$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$

$\Rightarrow [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] < \infty$ so, $\mathbb{Q}(\alpha,\beta)$ is a field with finite degree

$\Rightarrow \alpha \pm \beta \in \bar{\mathbb{Q}}$, $\alpha\beta \in \bar{\mathbb{Q}}$, $\frac{1}{\alpha} \in \bar{\mathbb{Q}}$

$\alpha\beta, \alpha \pm \beta, \frac{1}{\alpha}$ is a root of $f(t) \in \mathbb{Q}(\alpha,\beta)[t]$

Exe: $M|_K$, $\bar{K} = \{\alpha \in M \mid \alpha \text{ algebraic over } K\}$ → done down

$\bar{K}$ is field, $\bar{K}|K$: algebraic, any $\alpha \in M \setminus \bar{K}$ is transcendental

$[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$ as $t^n - 2$ has root $2^{1/n}$ is irreducible

$[\mathbb{Q}(2^{1/n}) : \mathbb{Q}] = n$ contains subfield $\forall n \in \mathbb{N}$

$\Rightarrow [\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$

THEOREM: $M|K$ field ext^n, FAE

① $M|K$ finite ext^n

② $M|K$: f.g & $M|K$ algebraic

③ $M = K(\alpha_1, \dots \alpha_n)$, $\alpha_i \in M$ algebraic $/K$

proof:

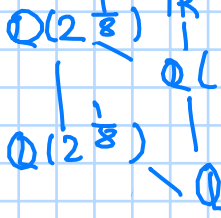
① ⇒ ② ⇒ ③ is trivial,

as $[M : K] \leq \prod_i [K(\alpha_i) : K] < \infty$

$\Rightarrow [M : K]$ is finite extension

Exe: give example where strict inequality holds

Ans: $\alpha = 2^{1/8} \in \mathbb{R}$



$[\mathbb{Q}(2^{\frac{1}{8}}) : \mathbb{Q}(2^{\frac{1}{2}})] = 4$

as $t^4 - (2)^{\frac{1}{2}}$ will be irreducible as $2^{\frac{1}{2}}$ prime

$2^{\frac{1}{2}} \nmid 1$ but $2^{1/2} \mid -(2)^{\frac{1}{2}}$, $2^{1/2} \nmid -(2)$

(∵ existing) $t^4 - (2)^{1/2}$ in $\mathbb{Q}[2^{\frac{1}{2}}][t]$

$\Rightarrow t^4 - (2)^{1/2}$ irred in $\mathbb{Q}(2^{1/2})(t)$

$[\mathbb{Q}(2)^{\frac{1}{8}} : \mathbb{Q}] = 8$ as $t^8 - 2$ is irreducible (∵ Eisenstein)

so, $[\mathbb{Q}(2^{\frac{1}{8}}) : \mathbb{Q}(2^{\frac{1}{2}})] < [\mathbb{Q}(2^{\frac{1}{8}}) : \mathbb{Q}]$

strict inequality

Exe: find example with strict inequality

Ans:

let $M=\mathbb{R}$

$K=\mathbb{Q}$ then $\alpha_1 = 2^{\frac{1}{4}}$ $\alpha_2 = 2^{\frac{1}{2}}$

$[K(\alpha_1,\alpha_2):K] = [\mathbb{Q}(2^{\frac{1}{4}}):\mathbb{Q}] = 4$

($\because t^4-2$ is ind by eisnstein)

and $\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}}) = \mathbb{Q}(2^{\frac{1}{4}})$ ($\because$ trivially $(2)^{\frac{1}{4}})^2 = 2^{\frac{1}{2}}$)

now, $d_1=4$, $d_2=2$ ($\because t^2-2$ is ind by eisnstein

so, $[K(\alpha_1,\alpha_2):K] \leq d_1 d_2 = 8$

$4 < 8$

↑ strict inequality

Exe: show $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] = 8$, i.e $\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$

Ans:

$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$

|

$\mathbb{Q}(\sqrt{2},\sqrt{3})$

|

$\mathbb{Q}$

$\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$

as if so

then $b\sqrt{2} + c\sqrt{3} = \sqrt{5} + a$

some $a,b,c \in \mathbb{Q}$

$2b^2 + 3c^2 + 2bc\sqrt{6} = 5 + a^2 + 2a\sqrt{5}$

$2b^2 + 3c^2 - 5 - a^2 = 2a\sqrt{5} + 2bc\sqrt{6}$

$d = e\sqrt{5} + f\sqrt{6}$

$d^2 = 5e^2 + 6f^2 + 2ef\sqrt{30}$

$\Rightarrow d^2 = 6e^2 + 6f^2$ $ef=0$

($\because 1, \sqrt{30}$ lin ind) $e=0 \Rightarrow a=0$

$f=0 \Rightarrow b=0, c=0$

$\Rightarrow d=0$

this is a contradiction

so, $\sqrt{5} \notin \mathbb{Q}(\sqrt{2},\sqrt{3})$

so, t^2-5 minimal ($\because$ eisnstein)

$\therefore [\mathbb{Q}(\sqrt{5},\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2},\sqrt{3})] = 2$

and $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ already seen

$\Rightarrow [\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 8$ by tower property

Exe: show that $M/\mathbb{Q}$ $M = \mathbb{Q}(\sqrt{p} : p \text{ is prime})$ is algebraic

Ans:

any $\alpha \in M$, $\exists \{p_1, p_2, \ldots p_n\}$ s.t

$\alpha \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots \sqrt{p_n})$

so, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{p_1}, \ldots \sqrt{p_n}) : \mathbb{Q}]$

$\leq 2 \times 2 \times \cdots \times 2 = 2^n$

so, $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\Rightarrow \alpha$ is algebraic

so, $\forall \alpha \in M$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty \Rightarrow \alpha$ is algebraic

$\Rightarrow M$ is algebraic

Exe: M/K, $\bar{K} = \{\alpha \in M \mid \alpha$ algebraic over $K\}$

$\bar{K}$ is field, $\bar{K}/K$: algebraic, any $\alpha \in M \setminus \bar{K}$ is transcendental

Ans: $\bar{K} = \{\alpha \in M \mid \alpha$ algebraic $/K\}$

$\bar{K}$ is field is trivial as $\forall \alpha, \beta \in \bar{K}$

$[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K] < \infty$

so, $K(\alpha, \beta)$ is a field with finite degree

so, $\alpha\beta \in \bar{K}$, $\alpha + \beta \in \bar{K}$, $\frac{1}{\alpha} \in \bar{K}$ as these are roots of $f(t) \in \mathbb{Q}(\alpha, \beta)[t]$

$\bar{K}$

$K(\alpha, \beta)$

$K(\alpha\beta)$

K

$\Rightarrow [K(\alpha\beta) : K] < \infty$

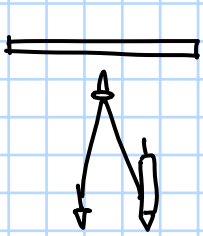
$\Rightarrow \alpha\beta \in \bar{\mathbb{Q}}$ similarly for others

trivially any $\alpha \in M \setminus \bar{K}$ as $\bar{K}$ is all algebraic $/K$

$\bar{K}/K$ algebraic also trivial

6th Feb:

Construction by ruler and compass (R and C):

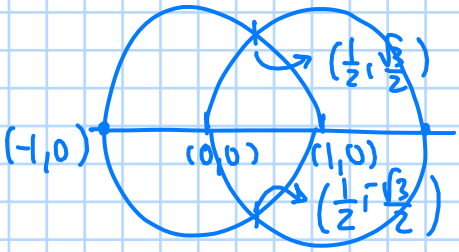


Ruler without marking

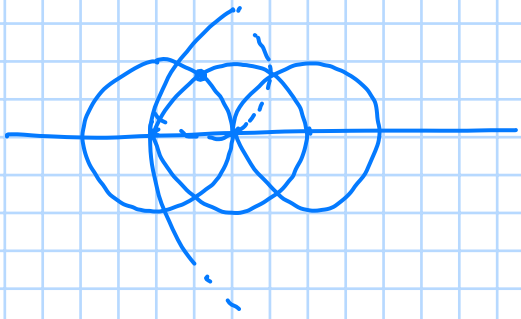
eg: $C_0 = \{(0,0), (1,0)\}$

start

$(0,0)$ $(1,0)$



$\rightarrow C_1 = \{(-1,0), (2,0), (\frac{1}{2}, \pm\frac{\sqrt{3}}{2})\} \cup C_0$



$\rightarrow C_2 = C_1 \cup \{\text{new points}\}$

$\vdots$

$\tilde{C} = \bigcup_{i \geq 0} C_i \in \mathbb{R} \times \mathbb{R}$

R $(x-a)^2+(y-b)^2=r^2$
S $(x-a')^2+(y-b')^2=r^2$
$\equiv$ $(x-a)^2+(y-b)^2=r^2$ & $a''x+b''y=r''$

we are adding points which solve both

as $(R=0, S=0) \Leftrightarrow (R=0, S-R=0)$

Let $\tilde{C} = \bigcup_{i \geq 0} C_i \subseteq \mathbb{R} \times \mathbb{R}$ be set of constructable points in $\mathbb{R}^2$

as $\pi_1(\tilde{C}) = \pi_2(\tilde{C})$ also

$C = \pi_1(\tilde{C})$ set of constructable numbers in $\mathbb{R}$

We want to find the following:

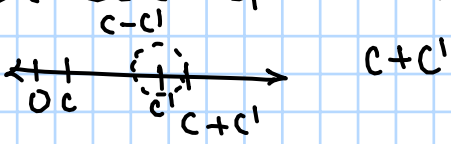
1. Given a constructable angle θ, can we bisect it ($\theta/3$ construction)
2. Can we duplicate a unit cube (i.e $2^{1/3} \in C$)
3. Can we square a unit circle (i.e $\sqrt{\pi} \in C$ or area of unit circle as a square)
4. Find $n \geq 3$ s.t regular n-gons is constructable
   $\triangle, \square, \ldots$ (angle $\frac{2\pi}{n}$ is constructable)
5. We want smallest $n \geq 1$ s.t $n°$(angle) is constructable

Lemma: ① $\mathbb{C}$ is a subfield of $\mathbb{R}$

② If $c>0 \in \mathbb{C}$ then $\sqrt{c} \in \mathbb{C}$

proof:

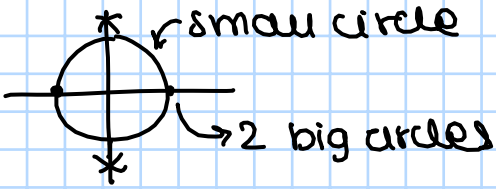
① we have $c, c' \in \mathbb{C}$ we want to construct



trivial by taking circle c' and radius $0-c$

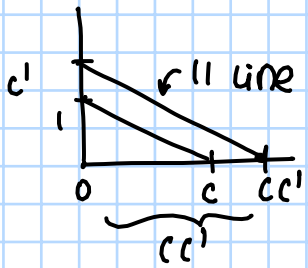
similarly for subtraction, so, $c-c', c+c' \in \mathbb{C}$

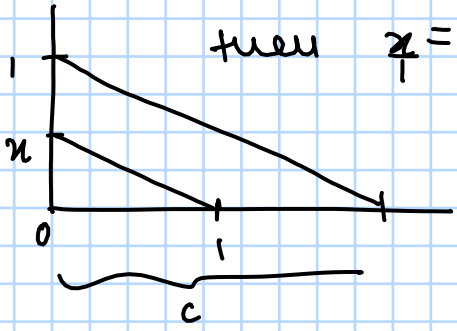
we can also draw a $\perp$ line from point to a line



we can draw $\parallel$ to a given line, by first taking $\perp$, and then taking $\perp$ again

now,

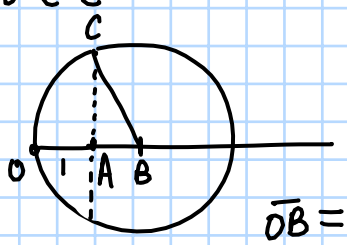




then $\frac{x}{1} = \frac{1}{c} \Rightarrow x = \frac{1}{c}$

so, $\mathbb{C}$ is a subfield of $\mathbb{R}$

② $c>0 \in \mathbb{C}$



$\overline{OB} = \frac{c+1}{2}$

$\overline{OA} = 1$

$BC = \frac{c+1}{2}$ $AB = \frac{c-1}{2}$ $AC = \sqrt{\left(\frac{c+1}{2}\right)^2 - \left(\frac{c-1}{2}\right)^2} = \sqrt{c}$

Def: $K \subset \mathbb{R}$ subfield $K/\mathbb{Q}$: iterated quadratic if $\exists$ a sequence of subfields

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n = K$$

$$[K_i : K_{i-1}] = 2$$
$$[K : \mathbb{Q}] = 2^n, \; n = 0 \text{ is also fine}$$

Eg: $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}})$ is iterated quadratic as

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}})$$

Similarly

$\mathbb{Q}(\sqrt{\sqrt{5}+\sqrt{7}})$ is iterated quadratic extension

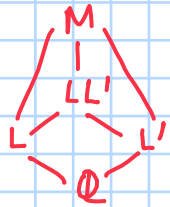
Exe: is $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}}, \sqrt{\sqrt{5}+\sqrt{7}})$ iterated quadratic, ie is the smallest field generated by two iterated quadratic a quadratic? → done down

Def: $M|_K$ field extension L, L' subfield of $M|_K$



then LL' = composite of $LL' := L(L') = L'(L)$

generating set for $LL' = \{ll' \mid l \in L, \; l' \in L'\}$

Lemma: 

If L, L': iterated quadratic then LL' is also iterated quadratic

proof:

If $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n = L$

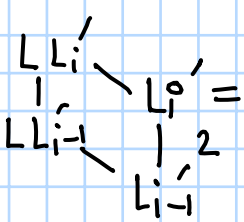
$$[L_i : L_{i-1}] = 2$$

$$\mathbb{Q} = L_0' \subset L_1' \subset \cdots \subset L_m' = L'$$

$$[L_i' : L_{i-1}'] = 2$$

then $\mathbb{Q} = L_0 \subset \cdots \subset L_n = L \subset LL_1' \subset LL_2' \subset LL_3' \subset \cdots \subset LL_m' = LL'$

$$\begin{matrix} & & 2 & & \cdots & & 2 & & \end{matrix}$$

now, 

$\{1, \alpha\}$ is basis of $L_i'|_{L_{i-1}'}$

$LL_i' = LL_{i-1}'(\alpha)$ ← composite

← monic irred polynomial deg ≤ 2

← monic irreducible polynomial deg 2

$$[LL_i' : LL_{i-1}'] \leq [L_i' : L_{i-1}'] = 2$$

$[LL_i' : LL_{i-1}']$ = 1 or 2 ← as $L_i' \subset LL_i'$

if 1 then we delete it from list or else 2

so, degree 1 → Remove them from list

$\Rightarrow LL'/\mathbb{Q}$ is iterated quadratic

Theorem: If $(x,y) \in \tilde{C}$ then x and y lie in some iterated quadratic quadratic extension of $\mathbb{Q}$

as a consequence, $\mathbb{Q} \subset \mathbb{Q}(x) \subset K$ $\quad [K:\mathbb{Q}] = 2^n$

K ↑ iterated Quadratic

then $[\mathbb{Q}(x):\mathbb{Q}] = 2^m$ for some $m \leq n$

proof: $\tilde{C} = \bigcup_{n\geq 0} C_n$, if $(x,y) \in C_0$ $(n=0)$ then

$x, y \in \{0,1\} \Rightarrow x, y \in \mathbb{Q}$

now if $(x,y) \in C_n$, $n>0$ then by induction hypothesis all points in C_{n-1} lie in iterated Quadratic Extension of $\mathbb{Q}$

(x,y) are solution of $\begin{cases} \cdot \text{ two linear Equation} \\ \cdot \text{ one linear, one quadratic with coeffs from } C_{n-1} \end{cases}$

then $C_n \subset K \rightarrow$ iterate quadratic

$(x,y) \subset$ deg 2 extension of K which is iterated Quadratic / $\mathbb{Q}$

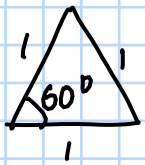
now, let's answer those statements

Trisection of an angle:

θ is constructable angle

$\Leftrightarrow \cos\theta, \sin\theta$ constructable numbers

so, $\theta = 60°$ constructable



$\cos 20°$ not constructable as $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

$\frac{1}{2} = 4x^3 - 3x$

$0 = 8x^3 - 6x - 1 \quad x = \cos 20°$

$\deg\left(\min_{\mathbb{Q}}(x)\right) = 3 \Rightarrow [\mathbb{Q}(x):\mathbb{Q}]$

$\Rightarrow x$ not constructable

Ex: show that $8x^3 - 6x - 1$ is irreducible → done down

doubling cube:

$[\mathbb{Q}((2)^{\frac{1}{3}}):\mathbb{Q}] = 3 \Rightarrow$ Not possible

Squaring circle:

$\sqrt{\pi}$ is transcendental, so not possible

Regular polygon:

if p is prime, then if $e^{2\pi i/p} \in \tilde{C}$ we are done

$[\mathbb{Q}(e^{2\pi i/p}):\mathbb{Q}] = p-1 = 2^n$

i.e $p = 2^n + 1$ for it to be constructable

$\Rightarrow n = 2^m$

as if $n = r \cdot s$ s: odd > 1

then

$p = 2^{r \cdot s} + 1$

$= (2^r)^s + 1$ ← fermat primes ← $t^3 + 1 = (t+1) f(t)$ as -1 is root, $t = 2^r$

$(2^r + 1) \mid (2^r)^s + 1$ ($\because s$ is odd)

this is not possible

If regular p-gon is constructable by RC then

constructable $\Rightarrow$ fermat prime (theorem later)

fermat prime $\Rightarrow$ constructable ←

$p = 2^{2^m} + 1$

$m = 0, 1, 2, 3, 4$ gives prime p

$m = 5$ p: not prime (no other fermat primes are known)

Theorem: (gauss) If p is fermat prime, then regular p-gon is constructible by RC

Theorem: Regular n-gon is constructable iff $n = 2^m \cdot p_1 p_2$ (p_1, p_2 are distinct fermat primes)

Note: $1^\circ, 2^\circ$ are not constructable (as 20° not constructable) as then

$1^\circ + 1^\circ \ldots + 1^\circ = 20^\circ$

$2^\circ + \ldots + 2^\circ = 20^\circ$

$60^\circ \Rightarrow 30^\circ \Rightarrow 15^\circ$ constructable

$\theta \to \theta/2$ is fine as $1 + \cos\theta = 2\cos^2\theta/2$ ← deg 2, $1 - \cos\theta = 2\sin^2\theta/2$ ← deg 2

Lemma: 72° is constructable

proof:

$e^{2\pi i/5} \in \tilde{\mathbb{C}}$ then we are done

$\zeta^4 + \zeta^3 + \zeta^2 + \zeta^1 + 1 = \left(\frac{1}{\zeta} + \zeta\right) + \left(\frac{1}{\zeta^2} + \zeta^2\right) + 1 = 0$

$\zeta^5 = 1 \quad \frac{1}{\zeta} = \zeta^4 \quad \frac{1}{\zeta^2} = \zeta^3$

let $\alpha = \frac{1}{\zeta} + \zeta$ then

$\alpha + (\alpha^2 - 2) + 1 = 0$

$\alpha^2 + \alpha - 1 = 0$

α is constructable as $\alpha = \frac{-1 \pm \sqrt{1+4}}{2} = \frac{-1 \pm \sqrt{5}}{2}$ ← constructable

$\frac{1}{\zeta} + \zeta = \alpha$

$\Rightarrow \zeta^2 - \alpha\zeta + 1 = 0$ lies in deg 2 extension of $\mathbb{Q}(\alpha)$ ($\because$ roots were also will lie in $\tilde{\mathbb{C}}$)

$\Rightarrow \zeta$ is constructable

Note: $80, 36^\circ, 18^\circ, 90^\circ$ constructable as $90, 15^\circ$ constructable $\Rightarrow 6^\circ$ constructable $\Rightarrow 3^\circ$ constructable

Exe: is $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}}, \sqrt{\sqrt{5}+\sqrt{7}})$ iterated quadratic, ie is the smallest field generated by two iterated quadratic a quadratic?

Ans:

$\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}})$ itt quadratic

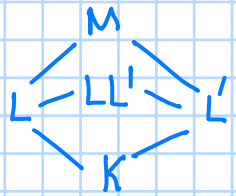
now $L = \mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}})$

$L' = \mathbb{Q}(\sqrt{\sqrt{5}+\sqrt{7}})$ ↙ itt quadratic

$M = \mathbb{R}$

$LL' = \mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{3}}, \sqrt{\sqrt{5}+\sqrt{7}})$

$K = \mathbb{Q}$ then



by theorem above LL' itt quadratic

Exe: show that $8x^3-6x-1$ is inducible

Ans:

as $8x^3-6x-1 = f(x)$ deg 3

then it is primitive as $\gcd(8,-6,-1)=1$

5/8 then $\bar{8}x^3-\bar{6}x-\bar{1}$

$= \bar{3}x^3+\bar{4}x+\bar{4}$

now $\bar{f}(\bar{0}) = \bar{4}$

$\bar{f}(\bar{1}) = \bar{1}$

$\bar{f}(\bar{2}) = \bar{1}$

$\bar{f}(\bar{3}) = \bar{2}$

$\bar{f}(\bar{4}) = \bar{2}$

i.e no roots of a 3 degree polynomial in $\mathbb{Z}/5\mathbb{Z}[x]$

$\Rightarrow$ irred in $\mathbb{Z}/5\mathbb{Z}[x]$

$\Rightarrow$ irred in $\mathbb{Z}[x]$ (∵ mod p irreducibility)

10th Feb:

we have seen $\tilde{C} = \{a+ib \in \mathbb{C} : a+ib \text{ constructed}\}$

$e = \pi_1(\tilde{C})$, i.e $\pi_1(a+ib) = a$

theorem: e is subfield of $\mathbb{R}$, if $c>0$, $c \in \tilde{C} \Rightarrow \sqrt{c} \in \tilde{C}$

cor: K subfield of e, $M|_K$ deg 2 extension then $M \subset \tilde{C}$ ($\pi_1(M) \subset e$)

proof:

$\alpha \in M|_K$ then $M = K(\alpha)$ as

$$\left.\begin{array}{c} M \\ \| \\ K(\alpha) \\ | \\ K \end{array}\right\} 2$$

$\Rightarrow [K(\alpha) : K] = 2$

so, α satisfies $\alpha^2 + a\alpha + b = 0$ $a, b \in K$

$$\alpha = \frac{-a}{2} \pm \frac{\sqrt{a^2-4b}}{2}$$

as $-\frac{a}{2} \in K$ assume $a^2 \geq 4b$ then

$\frac{a^2-4b}{4} \in K$ and $\frac{\sqrt{a^2-4b}}{2} \in \mathbb{C}$

so, $\alpha \in \mathbb{C}$ i.e $\alpha \in \tilde{C}$

$\Rightarrow M = K(\alpha) \subset \tilde{C}$

i.e $\pi_1(M) \subset \mathbb{C}$

now, if $\frac{a^2-4b}{4} < 0$

then $\beta = \sqrt{-\left(\frac{a^2-4b}{4}\right)}$ as $\beta \in \tilde{C} \Rightarrow i\beta \in \tilde{C}$

$\Rightarrow -\frac{b}{2} + i\beta \in \tilde{C}$

$\Rightarrow \alpha \in \tilde{C}$

$\Rightarrow M = K(\alpha) \subset \tilde{C}$

so, $\pi_1(M) \subset \mathbb{C}$

cor: $K \subset e$, $K = K_0 \subset K_1 \subset K_2 \cdots \subset K_n \subset \mathbb{R}$

($K_n|_K$ iterated quadratic extension of K_1, then $K_n \subset e$)

proof:

this follows trivially as $K_i \subset \mathbb{R}$ so, $\alpha \in \mathbb{C}$

now, we have seen that $f \in \mathbb{Q}[t]$ α_1, α_n: distinct roots of f in $\mathbb{C}$

$$f = a \prod_{i=1}^{n} (t-\alpha_i)^{m_i}$$

symmetry group of f over $\mathbb{Q}$: $gal(f|_{\mathbb{Q}}) = \{\sigma \in S_n | (\alpha_1, \alpha_2, \ldots \alpha_n) \text{ and } (\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(n)}) \text{ conjugate/} \mathbb{Q}\}$

evaluation map

$$\mathbb{Q}[t_1, t_2 \ldots t_n] \xrightarrow{ev(\alpha_1 \ldots \alpha_n)} \mathbb{C}$$

$$t_i \longmapsto \alpha_i$$

$\mathbb{Q}[t_1, \dots t_n] \xrightarrow{ev(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)})} \mathbb{C}$

$t_i \longmapsto \alpha_{\sigma(i)}$

then
$\ker(ev(\alpha_1, \dots \alpha_n)) = \ker(ev(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)}))$ as $(\alpha_1, \alpha_2 \dots \alpha_n)$ and $(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)})$ are conjugates

now, let $\deg f = m$

$f \in \mathbb{Q}[t] \longrightarrow Gal(f|\mathbb{Q}) \subset S_m$ (we want this but not always basic t^{s-1} $(1, w, w^2, w^3, w^4)$)

$\text{field ext}^n M|_{\mathbb{Q}}$

so, we use this to get $gal(f|\mathbb{Q})$ (intermediate step)

splitting field of $f = M$ $\quad$ $\text{field ext}^n M|_{\mathbb{Q}} = Aut(M|\mathbb{Q})$

def: $M|_K$ is a field extension i.e K is a subfield of M if $i: K \to M$ field homo, then we think of $(i: K \to M$ are field $ext^n)$

i, i' : field ext^ns
ψ: homomorphism

$$\begin{array}{ccc} M & & M' \\ i \uparrow & & i' \uparrow \\ K & \xrightarrow{\psi} & K' \end{array}$$

what we want to know is that if $\exists \varphi: M \to M'$ homo s.t

$$\begin{array}{ccc} M & \overset{\varphi}{\dashrightarrow} & M' \\ i \uparrow & \circlearrowright & i' \uparrow \\ K & \xrightarrow[\psi]{} & K' \end{array} \quad \text{diagram commutes} \quad i' \circ \psi = \varphi \circ i : K \to M'$$

If φ exist s.t diagram commutes, then we say φ extends ψ

special case:

$$\begin{array}{ccc} M & \overset{\varphi}{\dashrightarrow} & M' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\psi]{} & K' \end{array}$$

φ extends ψ if $\varphi|_K = \psi$

$$\begin{array}{ccc} a & \longrightarrow & \varphi(a) \\ \uparrow & & \| \\ a & \longrightarrow & \psi(a) \end{array}$$

we will discuss ① weather ψ has extension φ
② if so, then how many such extensions

lemma: $\psi: R \to S$ ring homomorphism

$\psi_*: R[t] \to S[t]$ unique extension of ψ s.t $\psi_*(t) = t$
and (i) ψ injective iff ψ_* injective
(ii) ψ surjective iff ψ_* surjective
(iii) ψ isomorphism iff ψ_* isomorphism

$Im(\psi_*) = (im\ \psi)[t]$ $\quad$ $\ker(\psi_*) =$ ideal generated by $\ker \psi$

$= \{\sum_1^r a_i f_i(t) \mid a_i \in \ker\psi\}$

proof:

$$\begin{array}{ccc} R[t] & \xrightarrow{\psi_*} & S[t] \\ \uparrow & & \uparrow \\ R & \xrightarrow{\psi} & S \end{array}$$

$(\psi_*)_1(\sum a_i t^i) = \sum \psi(a_i) t^i$

$(\psi_*)_2(\sum a_i t^i) = \sum \psi(a_i) t^i$

$\Rightarrow (\psi_*)_1 = (\psi_*)_2 \ \forall f \in R[t]$

$\Rightarrow \psi_*$ is unique

(i) ψ is injective, $\psi_*(f) = \psi_*(g)$

$\Rightarrow \psi_*(\sum a_i t^i) = \psi_*(\sum b_i t^i)$

$\Rightarrow \sum \psi(a_i) t^i = \sum \psi(b_i) t^i$

as all degree differ and ψ is injective

$\Rightarrow \psi(a_i) = \psi(b_i) \ \forall i$

$\Rightarrow f = g$

now if ψ_* is injective then $\psi_*|_R = \psi$ is also injective

(ii) ψ_* is surjective, then $\forall f \in S[t]$, $\exists f' \in R[t]$ s.t $\psi^*(f') = f$

then as $S \subseteq S[t] \Rightarrow \exists f' \in R[t]$ s.t $\psi^*(f') = s$

$\forall s \in S$ now this $f' \in R$ as $t \mapsto t$ so deg 0

as S has no t term

ψ is surjective then, $\forall f = \sum a_i t^i \in S[t]$

$\exists b_i \in R$ s.t $\psi(b_i) = a_i \ \forall i$

$\Rightarrow \exists f' = \sum b_i t^i$ s.t

$\psi_*(f') = \psi_*(\sum b_i t^i) = \sum \psi(b_i) t^i = \sum a_i t^i = f$

or ψ_* is surjective

(iii) from (i), (ii) this follows, also $\operatorname{img}(\psi_*) = \{\sum \psi(a_i) t^i \mid f \in R[t]\}$

$= \operatorname{img}(\psi)[t]$ ($\because$ trivial)

and $\ker(\psi_*) = \{f \in R[t] \mid \psi_*(f) \equiv 0\} = \{f \in R[t] \mid \sum \psi(a_i) t^i = 0 \Rightarrow \psi(a_i) = 0 \ \forall i\}$

$= \{\sum a_i f_i \mid a_i \in \ker(\psi), f_i \in R[t]\}$

lemma: $\alpha \in M, f(t) \in K[t]$

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\psi} & K' \\ \downarrow & & \downarrow \\ K[t] & \xrightarrow{\psi_*} & K'[t] \end{array}$$

$f(t) \mapsto \psi_*(f)$

ev_α: $t \mapsto \alpha$

$ev_{\varphi(\alpha)}$

$M \xrightarrow{\varphi} M'$

$\alpha \mapsto \varphi(\alpha)$

then $\begin{array}{ccc} K[t] & \xrightarrow{\psi_*} & K'[t] \\ {\scriptstyle ev_\alpha}\downarrow & \circlearrowright & \downarrow{\scriptstyle ev_{\varphi(\alpha)}} \\ M & \xrightarrow{\varphi} & M' \end{array}$ the diagram commutes

proof: $K[t] \to M'$

diagram commutes, let $f(t) = \sum a_i t^i \in K[t]$

then $\psi_*(f(t)) = \sum \psi(a_i) t^i$

$$\begin{array}{ccccc} f(t) & \xrightarrow{\psi_*} & \sum \psi(a_i) t^i & \xrightarrow{ev_{\varphi(\alpha)}} & \sum \psi(a_i) (\varphi(\alpha))^i \\ {\scriptstyle ev_\alpha}\downarrow & & & & \| \text{ as } \psi = \varphi \text{ on } K \\ \sum a_i \alpha^i & \xrightarrow{\varphi} & \varphi(\sum a_i \alpha^i) = \sum \varphi(a_i) (\varphi(\alpha))^i & & (\because \text{diagram commutes}) \end{array}$$

so, $ev_{\varphi(\alpha)} \circ \psi_* = \varphi \circ ev_\alpha$

Lemma: $\alpha \in M$, $f(t) \in K[t]$, $f(\alpha)=0$ then $\Psi_*(f)(\varphi(\alpha))=0$

proof:

$f(t) \in \ker(ev_\alpha)$ i.e $f(\alpha)=0$, then we want to see what happens above

$$\begin{array}{ccc} f(t) & \xrightarrow{\Psi_*} & \sum \Psi(a_i) t^i = \Psi_*(f) \\ \downarrow ev_\alpha & & \downarrow ev_{\varphi(\alpha)} \\ 0 & \xrightarrow{\varphi} & \sum \Psi(a_i)(\varphi(\alpha))^i = \sum \varphi(a_i)(\varphi(\alpha))^i = \varphi(\sum a_i \alpha^i) = \varphi(0) = 0 \end{array}$$

this means $\Psi_*(f) \in \ker(ev_{\varphi(\alpha)}) \Rightarrow \Psi_*(f)(ev_{\varphi(\alpha)})=0$

Note: from above, we got that

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\Psi} & K' \end{array}$$

$f(t) \in \ker(ev_\alpha)$ then $\Psi_*(f(t)) \in \ker(ev_{\varphi(\alpha)})$

corr: $\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \uparrow & \nearrow & \uparrow \\ K & = & K \\ & id & \end{array}$ (φ in K-homomorphism), if $f(\alpha)=0$, $\alpha \in M$, $f \in K[t]$ then $f(\varphi(\alpha))=0$

proof: as $\Psi_*(f) = \sum \Psi(a_i) t^i = \sum a_i t^i$ as $\Psi = id$

$$\Rightarrow f(\varphi(\alpha)) = 0 \quad (\because f(t)=0 \text{ as } \Psi_*(f)(\varphi(\alpha))=0 \text{ (previous lemma)})$$

so, $f(\varphi(\alpha))=0$

now, if $f(t) \in K[t]$ is annihilated by α, then it is also annihilated by $\varphi(\alpha)$

also if α: root of $f(t)$ then $\varphi(\alpha)$ is also root of $f(t)$

also if f: irreducible monic $f(\alpha)=0$ $\alpha \in M$ f: minimal polynomial of $\alpha|_K$

$$\Rightarrow f(\varphi(\alpha))=0$$

so, f is minimal polynomial of $\varphi(\alpha)|_K$

corr:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ | & \varphi & | \\ K(\alpha) & \to & K'(\alpha') \\ | & \alpha \mapsto \alpha' & | \\ K & \xrightarrow{\Psi} & K' \\ & K \cong K' & \end{array}$$

φ: restricted to $\varphi: M \to M'$ for $\varphi: K(\alpha) \to K'(\alpha')$

α: algebraic / K

Ψ: isomorphism then $\Psi_*(\min_K(\alpha)) = \min_{K'}(\varphi(\alpha))$

proof: $f(t) = \min_K \alpha \in K[t]$

$\Rightarrow f(\alpha)=0 \Rightarrow \Psi_*(t)(\varphi(t))=0$

f is monic irred in $K[t]$, as $\Psi_*: K[t] \to K'[t]$

Ψ isom $\Leftrightarrow \Psi_*$ isom ← from above

$\Rightarrow \Psi_*(f)$ monic, irred in $K'[t]$

$\Rightarrow \Psi_*(f) = \min_{K'} \varphi(\alpha)$

now,

$$\begin{array}{ccc} K[t] & \longrightarrow & \dfrac{K[t]}{\langle f \rangle} \cong K(\alpha) \\ \downarrow \tilde{\Psi}_* (\cong) & & \downarrow \Psi_* (\cong) \\ K'[t] & \longrightarrow & \dfrac{K[t]}{\Psi_*(f)} \cong K'(\alpha') \end{array}$$

13th Feb:

we have seen $M \xrightarrow{\varphi} M'$ φ: extension of ψ

$i \uparrow$, $i' \uparrow$

$K \xrightarrow{\psi} K'$

and

$$\begin{array}{ccc} M & \xrightarrow{\psi'} & M' \\ \uparrow & \circlearrowright & \uparrow \\ K & \xrightarrow{\psi} & K' \\ \downarrow & & \downarrow \\ K[t] & \xrightarrow{\psi_*} & K'[t] \\ t\downarrow & & t\downarrow \\ \alpha & \xrightarrow{\varphi} & \varphi(\alpha) \end{array}$$

diagram commutes

now, if we take $f(t) \xrightarrow{\psi_*} \psi_*(f(t))$ $\quad f(\alpha)=0 \Rightarrow \psi_*(f)(\varphi(\alpha))=0$

assume ψ: isomorphism i.e $\quad \begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ | & & | \\ K & \underset{\psi}{\cong} & K' \end{array}$ if $m(t)=\min_K \alpha$

ψ_* is isomorphism $\Rightarrow \psi_*(m(t))$ = monic irreducible

under isomorphism irreducible polynomial goes to irreducible polynomial

also, $\psi_*(m(t))$ = minimal polynomial of $\varphi(\alpha)$ over K'

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\varphi} & K'(\varphi(\alpha)) \\ | & \circlearrowright & | \\ K & \underset{\psi}{\cong} & K' \end{array} \qquad \left.\begin{array}{l} K \xrightarrow{} K' \\ \alpha \xrightarrow{} \varphi(\alpha) \end{array}\right\} \; K(\alpha) \xrightarrow{} K'(\varphi(\alpha))$$

also,

$$\begin{array}{ccccc} M & \xrightarrow{\varphi} & M' & & \\ \uparrow & \circlearrowright & \uparrow & & \\ K(\alpha) & \xrightarrow{\varphi} & K'(\varphi(\alpha)) & \cong & \dfrac{K'[t]}{\langle \psi_* m(\alpha) \rangle} \\ | & & | & & \\ K & \underset{\psi}{\cong} & K' & & \end{array} \qquad \dfrac{K[t]}{\langle m(t) \rangle} \cong$$

$$K \underset{\psi}{\cong} K' \qquad K[t] \xrightarrow[\psi_*]{\cong} K'[t]$$

$$\Rightarrow \dfrac{K[t]}{\langle m(t) \rangle} \cong \dfrac{K'[t]}{\langle \psi_* m(t) \rangle}$$

as if

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \cup & \circlearrowright & \cup \\ I & \xrightarrow{\psi} & J \\ \uparrow & & \uparrow \\ \text{ideal} & & \text{ideal} \end{array}$$

$$\begin{array}{ccc} R & \xrightarrow{\cong} & S \\ & \searrow & \downarrow \\ & & S/J \\ I \downarrow & \nearrow & \\ R/I & & \end{array}$$

R → S: surjective; I → R: inclusion; R → R/I: quotient; S → S/J: quotient; R → S/J: surjective; R/I → S/J: injective + surjective

$\Rightarrow R/I \cong S/J$

so, $K(\alpha) \cong K'(\varphi(\alpha))$, i.e for all such α extensions, we will get isomorphisms

i.e $\forall \alpha \in M$, taking basic extention

$$K(\alpha) \cong K'(\varphi(\alpha))$$

defn: M is a field, $f \in M[t]$ ($\deg f \geq 1$) then f splits in M if $f = a\prod_{i=1}^{n}(t-\alpha_i)$ where $a, \alpha_i \in M$

Eg: $f = t^2-2$ splits in $\mathbb{Q}(\sqrt{2})$ as $f(t) = (t-\sqrt{2})(t+\sqrt{2})$
does not split in $\mathbb{Q}(i)$

Eg: $f(t) = t^3-2$ in $\mathbb{Q}(\sqrt[3]{2})$ does not split as $\omega\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$
similarly $\omega^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$

$f(t)$ in $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$, $\subseteq \mathbb{C}$, splits in it

Note: If we have a degree 2 polynomial which has one root in a $F[t]$ then it has both roots

Eg: $f = t^2+t+1 \in \mathbb{F}_2[t]$

$M = \mathbb{F}_2(\alpha)$ as $\alpha^2+\alpha+1=0$ f splits in M

$f(\alpha)=0 \Rightarrow f = (t-\alpha)(t-\beta)$ in M

$\alpha+\beta = 1$

$\Rightarrow \beta = 1-\alpha$

$= -1(1+\alpha)$

$= 1+\alpha$ ($\because -1=1$ in $\mathbb{F}_2$)

defn: $f \in K[t]$, $M|_K$ M: splitting field over K if

① f splits in M

② $M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ $\alpha_1, \alpha_2, \ldots \alpha_n$: roots of f

Note: If K = algebraically closed then splitting field of $f \in K[t]$ is K

Eg: $f = t^2-2 \in \mathbb{C}[t]$
then $K = \mathbb{C}$ is splitting field

so, splitting field of f over $\mathbb{C}$ is $\mathbb{C}$
over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$
over $\mathbb{Q}(i)$ is $\mathbb{Q}(i, \sqrt{2})$

Lemma: $f \in K[t]$, then $\exists$ a splitting field $M|_K$ of f, further $[M:K] \leq n!$ ($n = \deg f$)

proof: If $n=1$: take $M = K$
($f = a(t-b)$, $a, b \in K$, $K(b) = K$) $[M:K] = 1 \leq 1!$

let $n > 1$, use induction on degree
$m \in K[t]$ be monic irreducible factor of f

$\frac{K[t]}{\langle m \rangle} = K(\alpha)$, $\alpha = \bar{t}$, $m(\alpha) = 0$

$m(t) = (t-\alpha)m_1$ in $K(\alpha)$

$f(t) = mf_1 = (t-\alpha)(f_1 m_1)$ in $K(\alpha)$

$M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ true by induction on degree
$|$ ∃ a splitting field of $f_1 m_1$ over $K(\alpha)$
$K(\alpha)$ $\quad \alpha_2, \alpha_3, \ldots \alpha_n$: roots of $f_1 m_1$
$|$
K

so, M is splitting field of K as $M = K(\alpha, \alpha_2, \ldots \alpha_n)$ → all roots of f

as m can have atmost n degree (≤ deg f)

$[M:K] = [M: K(\alpha)]\,[K(\alpha):K] \leq (n)!$
$\leq (n-1)!$ $\quad \leq n$
(∵ induction)

Lemma: M = splitting field of f over K, M' = splitting field of $\psi_* f$ over K'

$$\begin{array}{ccc} M & \overset{\exists\,\varphi}{\dashrightarrow} & M' \\ | & \circlearrowleft & | \\ K & \xrightarrow[\psi]{\cong} & K' \end{array} \qquad \begin{array}{ccc} K[t] & \xrightarrow{\cong} & K'[t] \\ & {\scriptstyle \psi_*} & \\ f & \longmapsto & \psi_*(f) \end{array}$$

then ① ∃ an isomorphism $\varphi: M \xrightarrow{\cong} M'$ and φ extends ψ

② the number of isomorphisms φ extending ψ is $\leq [M:K] \leq n!$

when $\deg f = n$

proof: $\deg f = n = 1$

$$\begin{array}{ccc} M = K & \xrightarrow{\varphi = \psi} & M' = K' \\ | & & | \\ K & \xrightarrow[\psi]{\cong} & K' \end{array}$$

then trivially ∃ an isomorphism φ extends ψ is trivial

similarly no of such isomorphisms over K is $1 \leq [M:K] = 1$

assume $n > 1$ and use induction on degree

$m(t)$: monic irreducible factor of f in $K[t]$
f splits in $M \Rightarrow m$ splits in M

choose $\alpha \in M$ s.t $m(\alpha) = 0$

$$\begin{array}{ccc} M & & M' \\ | & & \\ K(\alpha) & & \\ | & & \\ K & \cong & K' \end{array} \qquad \psi \text{ (curved arrow from } K \text{ to } K')$$

then $\psi_*(m)$: monic irreducible in $K'[t]$
(∵ ψ_* is isomorphism)

$\Rightarrow \psi_*(m)$ splits in M' as $\psi_*(m) \mid \psi_*(f)$

as, $f = m f_1 \Rightarrow \psi_*(f) = \psi_*(m)\,\psi_*(f_1)$

$\Rightarrow \psi_*(m)$ factor of $\psi_*(f_1)$

then, let $\alpha_1', \alpha_2', \ldots \alpha_s'$ be roots of $\psi_* m$ in M'

$$\frac{K[t]}{\langle m(t) \rangle} \cong K(\alpha) \xrightarrow[\theta_j]{(1 \leq s \leq \deg m)} K'(\alpha_j') = \frac{K'[t]}{\langle \psi_*(m(t)) \rangle}$$

$K \xrightarrow[\psi]{\cong} K'$

$\theta_j : K(\alpha) \longrightarrow K'(\alpha_j')$ is unique isomorphism extending ψ as

① $\theta_j|_K = \psi$

② $\theta_j(\alpha) = \alpha_j'$

So, now, $M \xrightarrow{\cong}_{\varphi} M'$ $\quad f = (t-\alpha)\tilde{f}$ in $K(\alpha)$ [tuell]

$K(\alpha) \xrightarrow{\theta_j} K'(\alpha_j')$ $\quad \psi_* f = (\theta_j)_* f$ ($\because$ diagram commutes)

$K \xrightarrow[\psi]{\cong} K'$ $\quad = (t-\alpha_j')(\theta_j)_*(\tilde{f})$

M = splitting field of f over $K(\alpha)$, similarly M' is splitting field of $(\theta_j)_*(\tilde{f})$ over $K(\alpha_j')$

① $\exists\ \varphi : M \longrightarrow M'$ s.t. $\varphi|_{K(\alpha)} = \theta_j$ ($\because$ induction)

$\Rightarrow \varphi|_K = \theta_j|_K = \psi$ so, $\exists$ φ isomorphism and extends ψ

② by induction, no. of isomorphisms φ extending θ_j is $\leq [M : K(\alpha)]$

If $\varphi : M \xrightarrow{\cong} M'$ extending ψ then $\varphi(\alpha) \in \{\alpha_1', \ldots \alpha_s'\}$ as $m(\alpha) = 0$

$\Rightarrow \varphi_*(m) = \psi_*(m)$

$\Rightarrow \varphi_*(\alpha)$ is root of $\psi_*(m)$

$\Rightarrow \varphi|_{K(\alpha)} = \theta_j$ for some $j \in \{1, 2, \ldots s\}$

[tuell], $M \xrightarrow{\varphi} M'$, $K(\alpha) \xrightarrow{\theta_j} K'(\alpha_j')$, $K \xrightarrow[\psi]{} K'$ $\Rightarrow$ # isomorphism φ extending ψ

$= \sum_j$ # extensions of θ_j

$\leq \sum_j [M : K(\alpha)] \leq \deg m \times [M : K(\alpha)]$

$= [M : K(\alpha)][K(\alpha) : K]$

$= [M : K]$

Cor: $M \xrightarrow{\varphi}_{\cong} M'$, $K \xrightarrow{=} K$, $f \longmapsto f$ — if M, M' are two splitting fields of f over K, then [tuell] are K-isomorphisms

proof: this follows trivially from above lemma

Cor: $M \xrightarrow{\varphi}_{\cong} M$, $K \xrightarrow{=} K$, $f \longmapsto f$ — if M is a splitting field of f over K, then no of automorphisms $|\mathrm{Aut}(M|_K)| \leq [M : K] \leq n!$ where $n = \deg f$

proof: this will follow trivially from above lemma

17th Feb:

we have seen, $f(t) \in K[t]$ then $\exists$ a splitting field M of f over K i.e

(i) f splits in M
(ii) $M = K(\alpha_1 \dots \alpha_n)$, $\alpha_1 \dots \alpha_n$ roots of f

If M_1, M_2 are splitting fields of f over K, then $\exists$ a K-isomorphism

$$\begin{array}{ccc} M_1 & \xrightarrow{\varphi} & M_2 \\ | & \cong & | \\ K & = & K \end{array}$$

$\varphi : M_1 \to M_2$, in fact no. of such K-isomorphisms are $\leq [M_1 : K] = [M_2 : K]$

given f, upto K-isomorphism, $\exists$ unique splitting field of f over K which we write as $\underset{K}{spl} f$ → this from corr done previously

and also, $|\underset{K}{Aut}(\underset{K}{spl} f)| \leq [\underset{K}{spl} f : K]$ → this is also a corr done previously

corr: $f \in K[t]$

$$\begin{array}{ccc} & M & \\ L & | & \underset{L}{spl} f \\ | & & | \\ K & \underset{K}{spl} f = K(\alpha_1, \alpha_2 \dots \alpha_n) & \end{array}$$

where $\alpha_1, \alpha_2, \dots \alpha_n$ are distinct roots of f
$\alpha_i \in M \ \forall i \in \{1, \dots n\}$
where $M|_K$

$\underset{L}{spl} f = L(\alpha_1, \alpha_2, \dots \alpha_n)$, then $\underset{L}{Aut}(L(\alpha_1, \alpha_2, \dots \alpha_n))$ ⊇ subgroup $\underset{K}{Aut}(K(\alpha_1, \alpha_2, \dots \alpha_n))$

proof: $\forall\ g : \underset{L}{spl} f \to \underset{L}{spl} f$

$g|_K \in \underset{K}{aut}(\underset{K}{spl} f)$ (∵ trivial)

defn: $f \in K[t]$, $gal(f|_K) = \underset{K}{Aut}(\underset{K}{spl} f)$

Note: $[\underset{L}{aut} f : L] \leq [\underset{K}{aut} f : K]$ as

$$\begin{array}{ccc} K(\alpha_1 \dots \alpha_n) & & L(\alpha_1, \dots \alpha_n) \\ | & & | \\ K(\alpha_1 \dots \alpha_{n-1}) & & L(\alpha_1 \dots \alpha_{n-1}) \\ \vdots & & \vdots \\ K(\alpha_1, \alpha_2) & & L(\alpha_1, \alpha_2) \\ | \ n_2 & & | \ m_2 \\ K(\alpha_1) & & L(\alpha_1) \\ | \ n_1 & & | \ m_1 \\ K & & L \end{array}$$

$n_1 \geq m_1$ as ⋮ $\Rightarrow n \geq m$

$\alpha_1 \in K \Rightarrow \alpha_1 \in L$
but $\alpha_1 \notin K$, $\alpha_1 \in L$ possible

defn: $M|_K$ field extension, $\mathrm{Gal}(M|K) := \mathrm{Aut}_K(M)$

then $\mathrm{Gal}(f|K)$ is a group as Aut is a group

$$\begin{array}{ccccc} M & \xrightarrow{\varphi_1} & M & \xrightarrow{\varphi_2} & M \\ | & \cong & | & \cong & | \\ K & = & K & = & K \end{array}$$

eg: $\mathrm{gal}(K|_K) = \mathrm{Aut}_K(K) = \{id\}$

$\mathrm{gal}(\mathbb{C}|_{\mathbb{R}}) = \mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{id, \kappa\}$ $\kappa(z) = \bar{z}$ ← complex conjugate

$\mathbb{C}$ = splitting field of t^2+1 over $\mathbb{R}$

$= \mathrm{spl}_{\mathbb{R}} t^2+1$

$|\mathrm{gal}(\mathrm{spl}_{\mathbb{R}} t^2+1)| \leq [\mathbb{C}:\mathbb{R}] = 2$

$\Rightarrow \mathrm{gal}(\mathbb{C}|_{\mathbb{R}}) = \{id, \kappa\}$

↑ nothing else as $|\ |=2$

eg: $\mathrm{Aut}(\mathbb{Q}(2^{1/3})|_{\mathbb{Q}})$ as $f = t^3-2$

then $\mathrm{spl}_{\mathbb{Q}} f = \mathbb{Q}((2)^{\frac{1}{3}}, \omega(2)^{\frac{1}{3}}, \omega^2(2)^{\frac{2}{3}})$

$\neq \mathbb{Q}((2)^{\frac{1}{3}})$

$$\begin{array}{ccc} \varphi: \mathbb{Q}(2^{\frac{1}{3}}) & \longrightarrow & \mathbb{Q}(2^{\frac{1}{3}}) \\ | & & | \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$

$\alpha^3-2=0 \Rightarrow \varphi(\alpha^3-2)=0 \Rightarrow (\varphi(\alpha))^3-2=0$

as φ is homomorphism

$(\varphi(\alpha))^3 = 2 \Rightarrow \varphi(\alpha) = \alpha$ as $\varphi(\alpha)$ is real, rest two roots are imaginary so, $\mathrm{Aut}(\mathbb{Q}(2^{1/3})|\mathbb{Q}) = \{id\}$

theorem: $f \in K[t]$, $\mathrm{char}(K)=0$, $M = \mathrm{spl}_K f$, then $|\mathrm{Aut}(M|K)| = [M:K]$

this theorem will be proved later

now, $\mathrm{spl}_{\mathbb{Q}}(t^3-2) = \mathbb{Q}(2^{1/3}, \omega) = M$ $\quad \mathbb{Q} = K$

$$\begin{array}{c} M = \mathbb{Q}(2^{1/3}, \omega) \\ | 2 \\ \mathbb{Q}(2^{1/3}) \\ | 3 \\ \mathbb{Q} \end{array}$$

satisfies $\omega^3-1=0$

$(\omega-1)(\underbrace{\omega^2+\omega+1}_{t^2+t+1=0 \text{ is minimal polynomial}})=0$

$\Rightarrow [M:\mathbb{Q}] = 2\times 3 = 6$

so, $|\mathrm{Aut}(M|K)| = 6$ (∵ above theorem)

now, let's compute $\mathrm{Aut}(M|K)$

$2^{1/3} \longmapsto 2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}$ as $t^3-2=0$ in all 3 cases

So, from below diagram we get $3 \times 2 = 6$ choices

$\omega \to \omega$ or ω^2 as $\omega^2 + \omega + 1 = 0$

$\mathbb{Q}(2^{1/3}, \omega) \longrightarrow \mathbb{Q}(2^{1/3}, \omega)$, $\mathbb{Q}(2^{1/3}, \omega^2) \to$ 2 choices

$\mathbb{Q}(2^{1/3}) \longrightarrow \mathbb{Q}(2^{1/3})$, $\mathbb{Q}(\omega 2^{1/3})$, $\mathbb{Q}(\omega^2 2^{1/3}) \to$ 3 choices

$\mathbb{Q} \longrightarrow \mathbb{Q}$

$f \longmapsto f$

Note: $f \in \mathbb{Q}[t]$, $M = \text{spl}_{\mathbb{Q}} f \subset \mathbb{C}$ K: complex conjugation

$K \in \text{Aut}(\mathbb{C}|\mathbb{Q})$

then $K : \mathbb{C} \to \mathbb{C}$, $\mathbb{Q} = \mathbb{Q}$

now, we want to see if $K : M \xrightarrow{\cong} M$ is isomorphism or not

as, if $\alpha \in \mathbb{C}$ is root of f then $K(\alpha) = \bar{\alpha}$ is also a root of f

$\Rightarrow \bar{\alpha} \in M \Leftrightarrow \alpha \in M$ and so, $K : M \xrightarrow[\cong]{K} M$ is an isomorphism

now, if $g \in \mathbb{Q}[p][t]$ then

$L = \text{spl}_{\mathbb{Q}[p]} g$ then $K : L \to L$ will not be an isomorphism over $\mathbb{Q}[p]$ as $\mathbb{Q}[p] \xrightarrow{K} \mathbb{Q}[p]$, $K(g) \neq g$

as $K(2^{1/3} p) = -2^{1/3} p$

roots: $p 2^{1/3}$, $p 2^{1/3} \omega$, $p 2^{1/3} \omega^2$ (minimal polynomial)

roots of minimal polynomial

as $\{p 2^{1/3}, p\omega 2^{1/3}, p\omega^2 2^{1/3}\} \neq \{-p 2^{1/3}, -p 2^{1/3}\omega, -p 2^{1/3}\omega^2\}$

$K : L \to L$ will not be an isomorphism over $\mathbb{Q}[p]$, as g not fixed $K : g \nrightarrow g$

Note: If $M \subset \mathbb{R}$, then $K = id \in \text{Aut}(M|\mathbb{Q})$, If $M \not\subset \mathbb{R}$, then K: order 2 element of group $\text{Aut}(M|\mathbb{Q})$

Ex: $H < S_p$, p is prime, H contains a p-cycle and transposition (i, j) then show that $H = S_p$ → done done

defn: $\text{Gal}(f|_K) = \underset{K}{\text{Aut}}(\underset{K}{\text{spl}} f)$, so $\text{gal}(f|_K)$ is going to act on $\underset{K}{\text{spl}} f$

$\text{gal}(f|_K) \times \text{spl}(f|_K) \longrightarrow \underset{K}{\text{spl}}(f)$

$(\sigma, x) \longrightarrow \sigma(x)$

If X = set of roots of f in $\underset{K}{\text{spl}} f$, then $\text{gal}(f|_K)$ restricts to give an action on X

$gal(f|_K) \times X \longrightarrow X$

$\Rightarrow gal(f|_K) \xrightarrow{\Phi \text{ group homomorphism}} perm(X)$

$\theta \longmapsto \sigma_\theta : X \to X$, $x \mapsto \theta(x)$

if $X = \{\alpha_1, \alpha_2, \ldots \alpha_n\}$ distinct roots of f in $spl_K f$

$perm(X) \equiv S_n$

$\{\sigma : \alpha_i \to \alpha_j\} \leftrightarrow \{\sigma : i \to j\}$

$gal(f|_K) \xrightarrow{\Phi} S_n$, $\theta \mapsto \sigma_\theta$, $\sigma_\theta(i) = j$, $\theta(\alpha_i) = \alpha_j$

Note: Φ is injective group homomorphism / group action is faithful

$ker(\Phi) = \{\theta \mid \Phi(\theta) = id\}$

$\Phi(\theta) = id \Leftrightarrow \sigma_\theta = id \Leftrightarrow \sigma_\theta(i) = i \ \forall i = 1, 2 \ldots n$

$\Leftrightarrow \theta(\alpha_i) = \alpha_i \ \forall i = 1, 2 \ldots n$

$\Leftrightarrow \theta = id$, as generators are fixed so, everything is fixed

$\in Aut_K(spl_K f)$

so, $\Phi(\theta) = id$ iff $\theta = id$

or $ker(\Phi) = id$, so Φ is injective

Note: $gal(f|_K) \cong \Phi(gal(f|_K)) \subseteq S_n$

↑ subgroup of S_n

$f(t) = a \prod_{i=1}^{n} (t - \alpha_i)^{n_i}$ in $spl_K f = M = K(\alpha_1 \ldots \alpha_n)$

$\theta \in Aut(M)$

then $\theta(f) = f$ $f = a \prod_{i=1}^{n} (t - \theta(\alpha_i))^{n_i}$ $\theta(\alpha_i) \in \{\alpha_1, \ldots \alpha_n\}$

theorem: M: alg closed field

M / K $\quad \bar{K} = \{\alpha \in M \mid \text{algebraic}/K\}$

$\bar{K}|_K$: algebraic extension

then $\bar{K}$ is algebraically closed field

proof: $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \bar{K}[t]$

then if roots of f lie in $\bar{K}$, then we are done

if we show a root of f lie in $\bar{K}$, then by induction we are done

If $a_i \in K, \forall i$, then $f \in K[t]$ will have a root in M say α then α will be algebraic over $K \Rightarrow \alpha \in \bar{K}$

$f \in M[t]$, $\exists \alpha \in M$ s.t $f(\alpha)=0$

$K(a_1, a_2 \dots a_n, \alpha)$

$\uparrow \leq \deg f$

$K(a_1, a_2, \dots a_n)$

$\uparrow < \infty$

K → as algebric to degree finite

So, α is algebric over $K \Rightarrow \alpha \in \bar{K}$ as $[K(a_1 \dots a_n, \alpha) : K] < \infty$

Ex: $H < S_p$, p is prime, H contains a p-cycle and transposition (i,j) then show that $H = S_p$

Ans:

wlog let $c = (0,1,2 \dots (p-1))$ be the p-cycle

$x = (0,a)$ be the transposition

let $a \in \mathbb{Z}/p\mathbb{Z}$

now, let H = subgroup generated by c and x

then

$c \circ x = (1, a+1)$

$\vdots$

$c^a \circ x = (a, 2a)$

then, $c^a \circ x$, $c^{2a} \circ x \dots$ i.e

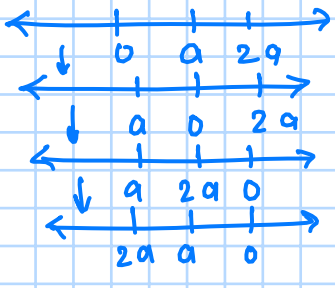
$(b-1)a, ba) \in H \quad \forall b \in \mathbb{Z}/p\mathbb{Z}$

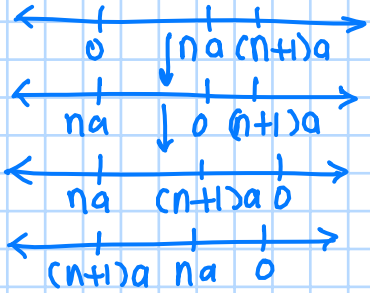
now, as $\mathbb{Z}/p\mathbb{Z}$ is a field

$\exists\, b \in \mathbb{Z}/p\mathbb{Z}$ s.t $ba = 1$

So, $\{(0,a), (a,2a), (2a,3a), \dots (ba-a, 0)\} \subseteq H$

now $(0,a) \circ (a,2a) \circ (0,a) = (0,2a) \in H$





if $(0, na) \in H$ then (true for $n=2$)

then

$(0,na) \circ (na, (n+1)a) \circ (0,na) = (0,(n+1)a) \in H$

$\Rightarrow (0, (b) \cdot a) \in H$

$\Rightarrow (0,1) \in H$

now, $(0,1) \in H \Rightarrow (1,2) \in H \quad (\because (1,2) = c \circ x)$

$\Rightarrow (2,3) \in H$

$\vdots$

So, all generators of S_p in $H \Rightarrow H = S_p$

20th Feb:

defn: M field $\supseteq K$, $(\alpha_1, \alpha_2 \ldots \alpha_n), (\beta_1, \beta_2 \ldots \beta_n) \in M^n$ are conjugate over K if $\forall\, p(t_1, t_2 \ldots t_n) \in K[t_1, t_2 \ldots t_n]$, $p(\alpha_1, \alpha_2 \ldots \alpha_n) = 0$ iff $p(\beta_1, \beta_2 \ldots \beta_n) = 0$

defn: $f(t) \in K[t]$, let $M = \underset{K}{spl}\, f = K(\alpha_1, \alpha_2 \ldots \alpha_n)$ $\alpha_1, \alpha_2 \ldots \alpha_n$: distinct roots of f

let $\Sigma = \{\sigma \in S_n : (\alpha_1, \alpha_2, \ldots \alpha_n)$ and $(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots \alpha_{\sigma(n)})$ are conjugates over $K\}$

Σ is subgroup of S_n

Σ = galois group of f over K, this was the first definition infact, this was galois definition

$\Sigma \to$ symmetry group of f over K

we have one more equivalent definition of galois group of f/K

defn: $gal(f/K) = \underset{K}{Aut}(\underset{K}{spl}\, f) = \underset{K}{aut}(M)$

now $\underset{K}{aut} M$ acts on M

$$\underset{K}{aut} M \times M \longrightarrow M = K(\alpha_1, \alpha_2 \ldots \alpha_n)$$
$$(\theta, x) \longmapsto \theta(x)$$

$X = \{\alpha_1, \alpha_2 \ldots \alpha_n\}$: set of distinct roots of f

$$\underset{K}{Aut} M \times X \longrightarrow X \qquad (\theta, \alpha_i) \longmapsto \theta(\alpha_i)$$

any $\theta \in \underset{K}{Aut} M$ permutes roots of f as over K, so rest all same

$$\underset{K}{Aut}\, M \xrightarrow{\Phi} S_n$$
$$\theta \longmapsto \sigma_\theta : i \to j \text{ where } \theta(\alpha_i) = \alpha_j$$

Φ: group homomorphism

Φ: injective as $\Phi(\theta) = \Phi(\theta') \Rightarrow \sigma_\theta = \sigma_{\theta'} \Rightarrow \theta = \theta'$

so, $\underset{K}{Aut}\, M \cong \Phi(\underset{K}{Aut} M) < S_n$

$\Rightarrow \underset{K}{Aut} M$ is isomorphic to a subgroup of S_n

theorem: symmetric group of $f/K = \Sigma$ is same as $gal(f/K)$ i.e

$$\Psi(\underset{K}{aut}(\underset{K}{spl}\, f)) = \{\sigma_\theta : \theta \in gal(f/K) = \underset{K}{Aut}(\underset{K}{spl}\, f)\}$$

proof: let $(\alpha_1, \alpha_2 \ldots \alpha_n)$ be distinct roots of f in M

$$M = K(\alpha_1, \alpha_2 \ldots \alpha_n)$$

for any $\theta \in \underset{K}{aut}(\underset{K}{spl}\, f) \Rightarrow \sigma_\theta \in \{\sigma_\theta : \theta \in gal(f/K)\}$

if we now that $(\alpha_1, \alpha_2 \ldots \alpha_n)$ and $(\alpha_{\sigma_\theta(1)}, \alpha_{\sigma_\theta(2)} \ldots \alpha_{\sigma_\theta(n)})$ are conjugates, then

$$\sigma_\theta \in \Sigma \Rightarrow \{\sigma_\theta : \theta \in gal(f/k)\} \subseteq \Sigma$$

now, let $p(t_1, t_2, \ldots t_n) \in K[t_1, t_2, \ldots t_n]$ then

$p(\alpha_{\sigma_\theta(1)}, \alpha_{\sigma_\theta(2)}, \ldots \alpha_{\sigma_\theta(n)})$ if $\sigma_\theta(i) = j$ then $\theta(\alpha_i) = \alpha_j$

$= p(\theta(\alpha_1), \theta(\alpha_2), \ldots \theta(\alpha_n))$

$$p(t_1, t_2, \ldots t_n) = \sum_{i_j \geq 0} a_{(i_1, i_2, \ldots i_n)} t_1^{i_1} t_2^{i_2} \ldots t_n^{i_n}$$

finite sum, coefficients $a_{(i_1, i_2, \ldots i_n)} \in K$

$$p(\theta(\alpha_1), \theta(\alpha_2), \ldots \theta(\alpha_n)) = \sum_{\substack{i_j \geq 0 \\ \text{finite sum}}} a_{(i_1, i_2, \ldots i_n)} \theta(\alpha_1)^{i_1} \theta(\alpha_2)^{i_2} \ldots \theta(\alpha_n)^{i_n}$$

$$= \theta\left(\sum_{\substack{i_j \geq 0 \\ \text{finite sum}}} a_{(i_1, i_2, \ldots i_n)} \alpha_1^{i_1} \alpha_2^{i_2} \ldots \alpha_n^{i_n} \right)$$

$$= \theta(0)$$

$$= 0$$

and, $|\mathbb{Q}[t]|$ is countable but $\mathbb{Q}[[t]]$ is uncountable

here as each coeff can be non-zero

$$\underbrace{|\mathbb{Q} \times \mathbb{Q} \times \ldots\ldots|}_{\text{uncountable}} = |\{0,1\} \times \{0,1\} \times \ldots\ldots| = |\mathbb{R}|$$

$K[[t_1, t_2 \ldots t_n]]$ is local (unique maximal ideal)

as $p(\theta(\alpha_1), \theta(\alpha_2), \ldots \theta(\alpha_n)) = 0$

if $p(\alpha_1, \alpha_2, \ldots \alpha_n) = 0 \Leftrightarrow \theta(p(\alpha_1 \ldots \alpha_n)) = 0$ ($\because \theta$ is automorphism)

$\Leftrightarrow p(\theta(\alpha_1), \ldots \theta(\alpha_n)) = 0$

$\Leftrightarrow p(\alpha_{\sigma_\theta(1)}, \ldots \alpha_{\sigma_\theta(n)}) = 0$

$\forall\, \sigma_\theta \in \Sigma$

$\Rightarrow gal(f/K) \subset \Sigma$

Let $\sigma \in \Sigma$ we want $\sigma = \sigma_\theta$ for some $\theta \in gal(f/k)$

$\theta : K(\alpha_1, \alpha_2, \ldots \alpha_n) \longrightarrow K(\alpha_1, \ldots \alpha_n)$

$\| \quad$ as α_i root of f, $\exists$ monic irreducible s.t
$K[\alpha_1, \alpha_2, \ldots \alpha_n]$ $\forall\, \alpha_i$ root of $m \Rightarrow \frac{K[t]}{\langle m(t) \rangle} \cong K[\alpha_i] = K(\alpha_i)$ or $K[\alpha]$ is a field

let θ by $\theta|_K = id$, $\theta(\alpha_i) = \alpha_{\sigma(i)}$ now we need to show

① θ is well defined

② $\theta : K$ automorphism of $K[\alpha_1, \alpha_2, \ldots \alpha_n]$

$$\theta: K[\alpha_1, \dots \alpha_n] \longrightarrow K[\alpha_1, \dots \alpha_n]$$
$$p(\alpha_1 \dots \alpha_n) \longmapsto p(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)})$$

well defined:

If $p(\alpha_1 \dots \alpha_n) = q(\alpha_1 \dots \alpha_n)$
$\Rightarrow (p-q)(\alpha_1 \dots \alpha_n) = 0$

as $\sigma \in \Sigma \Rightarrow (p-q)(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)}) = 0$

$\Rightarrow p(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)}) = q(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(n)})$

$\Rightarrow \theta$ is well defined

1-1: $\theta(p) = \theta(q)$
$\Leftrightarrow (p-q)(\alpha_{\sigma(1)} \dots \alpha_{\sigma(n)}) = 0$

$\Leftrightarrow (p-q)(\alpha_1, \dots \alpha_n) = 0$

$\Rightarrow p(\alpha_1 \dots \alpha_n) = q(\alpha_1 \dots \alpha_n)$

onto:
as $\forall\ p(\alpha_1 \dots \alpha_n) \in K[\alpha_1 \dots \alpha_n]$
$\exists\ \sigma^{-1}$ s.t

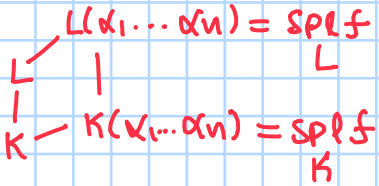
$p(\alpha_{\sigma^{-1}(1)}, \dots \alpha_{\sigma^{-1}(n)}) \in K[\alpha_1 \dots \alpha_n]$

s.t $\theta(p(\alpha_{\sigma^{-1}(1)}, \dots \alpha_{\sigma^{-1}(n)})) = p(\alpha_{(1)}, \alpha_{(2)}, \dots \alpha_{(n)})$

so, $\theta \in \mathrm{Aut}_K(M) \Rightarrow \sigma_\theta = \sigma \Rightarrow \mathrm{gal}(f/K) \subset \Sigma$

so, $\mathrm{gal}(f/K) = \Sigma$

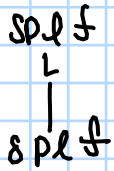
cor: $f \in K[t]$
$\alpha_1, \alpha_2 \dots \alpha_n$ distinct roots of f



$\mathrm{gal}(f/K)$ (= symmetric group of f over K), $\mathrm{gal}(f/L)$ = symmetric group of f/L

then $\mathrm{gal}(f/K) \supseteq \mathrm{gal}(f/L)$

proof:



then any $\theta \in \mathrm{Aut}_L(\mathrm{spl}_L f)$

$\Rightarrow \theta \in \mathrm{Aut}_K(\mathrm{spl}_K f)$

$\Rightarrow \mathrm{Aut}_L(\mathrm{spl}_L f) \subseteq \mathrm{Aut}_K(\mathrm{spl}_K f)$

$\Rightarrow \mathrm{gal}(f/L) \subseteq \mathrm{gal}(f/K)$

also, $f(t_1, t_2 \dots t_n) \in L[t_1, t_2, \dots t_n] \cup K[t_1, t_2, \dots t_n]$

so, $\sigma \in \sum_L \Rightarrow \sigma \in \sum_K$

Eg: $f=(t^2+1)(t^2-2)\in\mathbb{Q}[t]$

$$gal(f/\mathbb{Q})=\underset{\mathbb{Q}}{Aut}(\mathbb{Q}(i,\sqrt{2}))$$

$$\begin{array}{c} \mathbb{Q}(i,\sqrt{2}) \\ | \\ \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{array}$$ 2 aut, 2 aut

$$\begin{array}{ccc} \mathbb{Q}(i,\sqrt{2}) & \longrightarrow & \mathbb{Q}(i,\sqrt{2}),\ \mathbb{Q}(i,-\sqrt{2}) \\ | & & | \\ \mathbb{Q}(i) & \longrightarrow & \mathbb{Q}(i),\ \mathbb{Q}(-i) \\ | & & | \\ \mathbb{Q} & \xrightarrow{id} & \mathbb{Q} \end{array}$$

$\Rightarrow \underset{\mathbb{Q}}{Aut}(\mathbb{Q}(i,\sqrt{2}))\cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ($\because$ group of order 4)

$\Rightarrow gal(f/\mathbb{Q})\cong \mathbb{Z}/2\times\mathbb{Z}/2\mathbb{Z}$

also, $gal(f/\mathbb{Q}(i))\cong\mathbb{Z}/2\mathbb{Z}$

$gal(f/\mathbb{R})\cong\mathbb{Z}/2$

$gal(f/\mathbb{C})=(id)$

Note: $\begin{array}{c} M \\ | \\ K \end{array}$, M: algebraically closed

$$\begin{array}{c} M \\ | \\ K \end{array}\supset \bar{K}=\{\alpha\in M \mid \text{algebraic/}K\}$$

(i) $\bar{K}/K$: algebraic extension

(ii) $\bar{K}$: algebraically closed field

Defn: $\bar{K}$ is algebraic closure of K

Eg: $\bar{\mathbb{Q}}$ = algebraic closure of $\mathbb{Q}$

$$\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{Q} \end{array}\supset \bar{\mathbb{Q}}\ (\bar{\mathbb{Q}}\cap\mathbb{R}: \text{Real algebraic closure of } \mathbb{Q})$$

Theorem: K field, then an algebraic closure will exist and if M_1, M_2 are algebraic closures of K, then $\exists$ K isomorphism from $M_1\to M_2$
(i.e algebraic closure of K is unique upto K-isomorphism)

proof: Assume K is countable, then $K[t]$ is countable
let $f_1, f_2, \ldots$ be monic irreducible polynomials in $K[t]$

$$K\subset \underset{\text{spl}_K f_1}{M_1}\subset \underset{\text{spl}_{M_1} f_2}{M_2}\subset\cdots$$

∞

now $M=\bigcup_{i=1}^{\infty} M_i$ is a field as

① $1,0\in M$ (trivial)

② $\alpha \in M$ then $\alpha^{-1}, -\alpha \in M$ (trivial)
as $\alpha \in M$
$\Rightarrow \alpha \in M_i$ for some i
$\Rightarrow \alpha^{-1} \in M_i, -\alpha \in M_i$

③ $\alpha, \beta \in M$ then $\exists\, i, j$ s.t
$\alpha \in M_i$, $\beta \in M_j$
wlog $i<j$
then as
$M_i \subset M_{i+1} \dots \subset M_j$
$\Rightarrow \alpha \in M_j$

so, $\alpha+\beta \in M_j$, $\alpha\beta \in M_j$
$\Rightarrow \alpha+\beta \in M$, $\alpha\beta \in M$

so, now above $M = \bigcup_{i=1}^{\infty} M_i$ is a field

now M is algebric closure of K if ① M/K: algebric extension
② M is algebrically closed

$\forall \alpha \in M$, $\exists\, i$ s.t $\alpha \in M_i$, now

M_i — $[M_i : M_{i-1}] \le \deg f_i$
M_{i-1} — $[M_1 : K] \le \deg f_1$
M_{i-2} — $\Rightarrow [M_i : K] \le \deg f_i \deg f_{i-1} \dots \deg f_1$
M_1 — (∵ tower lemma)
K — $\Rightarrow [M_i : K] < \infty$

then, M_i — $[M_i : K] = [M_i : K(\alpha)][K(\alpha) : K] < \infty$
$K(\alpha)$ — $\Rightarrow [K(\alpha) : K] < \infty$
K

as $[K(\alpha) : K] < \infty$, α is algebric over K

so, $\forall \alpha \in M$, α is algebric over K i.e M is algebric extension of K

now, M is algebrically closed if $\forall f(t) \in M[t]$, roots of $f(t) \in M[t]$
↑ data of algebrically closed

now, if $f(t) = \sum_{i=1}^{n} a_i t^i$ $a_i \in M$ $\forall i$
then $f(t) \in K(a_1, a_2, \dots a_n)[t]$
if α is a root of $f(t)$
then
$\alpha \in K(a_1, a_2, \dots a_n, \alpha)$ — $\le \deg(f)$
$K(a_1, a_2, \dots a_n)$ — $< \infty$ (∵ $a_1, a_2, \dots a_n$ are algebric over K)
K

$\Rightarrow [K(a_1, a_2, \dots a_n, \alpha) : K] < \infty$

$K(a_1, a_2 \ldots a_n, \alpha)$
|
$K(\alpha)$
|
K

$\Rightarrow [K(a_1 \ldots a_n, \alpha) : K(\alpha)][K(\alpha) : K] < \infty$

$\Rightarrow [K(\alpha) : K] < \infty$

$\Rightarrow \alpha$ is algebraic over K

$\Rightarrow \alpha \in M$

so roots of $f(t) \in M[t]$ are in $M \Rightarrow M$ is algebraically closed — ②

from ①, ② we have M to be algebraic closure of K

now if K is uncountable, then $\forall$ irreducible monic $f \in K[t]$ introduce a variable X_f

$R = K[X_f : f \text{ is monic irreducible}]$

$I = \langle f(X_f) : f \text{ is monic irreducible} \rangle$

I = ideal of R generated by $\{f(X_f) : f \text{ monic irreducible}\}$

I is a proper ideal (assume this) then $\exists$ maximal ideal $M \supset I$

$$M_1 = \frac{R}{M} = \frac{K[X_f : f \text{ is monic irred}]}{M}$$

$K \subset R$

$K/M = K$ as constants $\notin M$ ($\because M$ is maximal)

$\Rightarrow K \subset R/M$

$K \subset M_1$ is algebraic extension as for $f(X_f) \in I \subset M$

$\Rightarrow \overline{f(X_f)} = 0$ in $M \Rightarrow f(\overline{X}_f) = 0$ in M as $K \subset M$

$\Rightarrow \overline{X}_f$ is root of f

as $X_f \in R \Rightarrow \overline{X}_f \in R/M = M_1$

so, $\frac{K[X_f]}{M}$ is s.t $\overline{X}_f$ is a root of f ($K[X_f]$ is generated by X_f)

$\Rightarrow \overline{X}_f$ is algebraic in $\frac{K[X_f]}{M}$

$\forall \alpha \in \frac{K[X_f]}{M}$, $\alpha = \underbrace{\sum}_{\text{finite sum}} a (\overline{X}_{f_1})^{n_1} \ldots (\overline{X}_{f_r})^{n_r}$ any finite combination

as all algebraic $\Rightarrow \alpha$ is algebraic over K

as sum, product inverse operations of algebraic are closed

$\Rightarrow M_1$ is algebraic extension of K

now, repeate this process $M_2 = \frac{R}{M_1}$

$K \subset M_1 \subset M_2 \subset \cdots$

similar to above $M_1 \subset M_2$, and M_2 is algebraic extension over M_1

Now, $M = \bigcup_{i \geq 1} M_i$ becomes algebraic extension over K — (3)

and M is algebraically closed as

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in M[t]$$

Now, $a_i \in M$

$\Rightarrow a_i \in M_r$ for some r

$\Rightarrow f \in M_r[t]$

So, one of the irreducible factors of f will have a root in M_{r+1}

$\Rightarrow$ roots of $f \in M_{r+1}$

$\Rightarrow$ roots of $f \in M$

So, $\forall f \in M[t]$, roots of $f \in M \Rightarrow M$ is algebraically closed — (4)

from (3), (4) we get $\exists$ algebraic closure given field K

6th March:

Note: K field, $f(t) \in K[t]$, splitting field of f over K is an extension $M|K$ s.t

(a) f splits in M, i.e f = product of linear polynomials in $M[t]$

(b) $M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ $\alpha_1, \alpha_2, \ldots \alpha_n$: roots of f

Theorem: splitting field of f over K exist

the above theorem was by $K[t]/\langle p \rangle = K(\alpha_1)$ (induction arguments)

P: irreducible factor of f

s.t $f = (t-\alpha_1) f_1$ in $K(\alpha_1)[t]$

Theorem: $f \in K[t]$, $M = \underset{K}{spl}\, f$

$$\begin{array}{ccc} M & \overset{\varphi}{\cong} & M' \\ | & & | \\ K & \xrightarrow[\psi]{\cong} & K' \\ | & & | \\ f & & \psi_* f \end{array}$$

$\psi_* f$ = image of f in $K'[t]$

$M' = \underset{K'}{spl}\, \psi_* f$

then ① $\exists$ an isomorphism $\varphi: M \to M'$ s.t $\varphi|_K = \psi$ (φ is extension of ψ)

② there exist almost $[M:K]$ no of such extensions φ of ψ

we have seen, this theorem also by induction

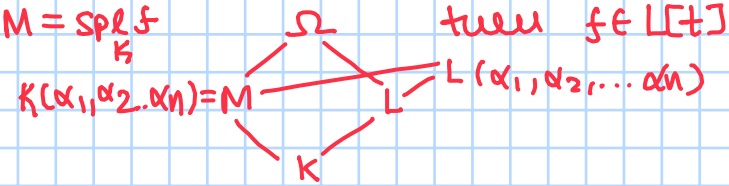
Cor: $\psi = id : K \to K$, any two splitting fields of $f \in K[t]$ over K are K-isomorphic

Cor:

$$\begin{array}{ccc} M & \overset{\varphi}{\cdots\to} & M \\ | & \cong & | \\ K & \xrightarrow[id]{} & K \end{array}$$

then $|\underset{K}{Aut}(M)| \leq [M:K] \leq (\deg f)!$

Lemma: $f \in K[t]$, $M = \underset{K}{spl}\, f$



then $f \in L[t]$

$\underset{L}{spl}\, f = L(\alpha_1, \alpha_2 \ldots \alpha_n)$
$= K(\alpha_1, \alpha_2, \ldots \alpha_n)L$
$= ML$ (composit)

then $[M:K] \geq [ML:L]$

proof: as



we have seen

$[LM:L] \leq [M:k]$ (∵ before theorem)

Cor:

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

then $\underset{K}{spl}\, f = M \Rightarrow M = \underset{L}{spl}\, f$

proof: It is straightforward from $\underset{L}{spl}\, f = ML = M$

Defn: $M|_K$ extension, $Gal(M|_K) = Aut_K(M)$ $f \in K[t]$

$$Gal_K(f) = Gal(spl_K f|_K) \text{ or } Gal_K(spl_K f)$$

Exe: Show that $Aut_{\mathbb{Q}}(\mathbb{R}) = \{id\}$ → done down

So, from above theorem, $|Gal_K(f)| = |Aut_K(spl_K f)| \leq [spl_K f : K]$

now, $Gal_K(f)$ acts on $spl_K f$

$$(\sigma, \alpha) \mapsto \sigma(\alpha)$$

$\sigma \in Gal_K(f)$, $\alpha \in spl_K(f)$

as $\sigma \in Aut_K(spl_K f)$

$= Aut_K(K(\alpha_1, \alpha_2, \ldots \alpha_n))$

as $\sigma|_K = id$, so if we just know their action on

$S = \{\alpha_1, \alpha_2, \ldots \alpha_n\}$ (set of distinct roots of f)

then $gal_K(f)$ acts on S

i.e $\sigma(\alpha_i) \in S$ $\forall i \in \{1, 2, \ldots n\}$

$Gal_K(f) \xrightarrow{\rho} Perm(S) = S_n$ is group homomorphism

ρ is injective/one-one

$\rho(\sigma): i \mapsto j$ if $\sigma(\alpha_i) = \alpha_j$

if $\rho(\sigma) = id \Rightarrow i \mapsto i \Rightarrow \sigma(\alpha_i) = \alpha_i$ $\forall i$

$\Rightarrow \sigma|_K = id$ & $\sigma|_S = id$

$\Rightarrow \sigma|_{spl_K f} = id$

$\Rightarrow \sigma = id$

So, $Gal_K(f) \cong img(\rho)$ subgroup of S_n

Corr: $|Gal(f)|$ divides $n!$, n = no of distinct root of f

proof: It follows trivially from

$$gal_K(f) = img(\rho) < S_n$$

$$\Rightarrow |gal_K(f)| \,||S_n| = n!$$

Exe: Show that

① $Aut_{\mathbb{Q}}(\bar{\mathbb{Q}} \cap \mathbb{R}) = \{id\}$ → done down

② $|Aut_{\mathbb{Q}}(\bar{\mathbb{Q}})| =$ infinite

$\bar{\mathbb{Q}} \cap \mathbb{R}$ = Real algebraic numbers

Fundamental theorem of galois theory:

FTGT gives "nice" field ext^n. $Gal(M|K)$ gives information about $M|_K$
In particular, FTGT

$$|Gal_K(f)| = [spl_K f : K]$$

Eg: $M = K(\alpha) = spl_K f \quad f = \min_K \alpha$

let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots \alpha_n$ are distinct roots of f in M

then $gal_K(f) = Aut_K(K(\alpha))$

$$\begin{array}{ccc} & & \varphi \\ K(\alpha) & \dashrightarrow & K(\alpha_i) = spl_K f \\ | & & | \\ K & = & K \\ f & \longmapsto & f \end{array}$$

$[K(\alpha) : K] = \deg f \quad (\because f = \min_K \alpha)$

$$\begin{array}{c} K(\alpha) \\ | \\ K(\alpha_i) \\ | \\ K \end{array} \qquad [K(\alpha) : K(\alpha_i)][K(\alpha_i) : K] = [K(\alpha) : K]$$

$[K(\alpha_i) : K]$: $\deg 1$; $[K(\alpha) : K(\alpha_i)]$: $\deg f$; $[K(\alpha) : K]$: $\deg f$ ($K(\alpha_i) = spl_K f$)

$$\Rightarrow [K(\alpha) : K(\alpha_i)] = 1$$

$$\Rightarrow K(\alpha) = K(\alpha_i)$$

$$K[\alpha] \cong \frac{K[t]}{\langle f \rangle} \cong K[\alpha_i]$$

$$\Rightarrow K[\alpha] \cong K[\alpha_i], \text{ s.t. } \varphi(\alpha) = \alpha_i$$

So, in this case, $Aut_K(K(\alpha)) = \{\sigma_i : \sigma_i(\alpha) = \alpha_i\}$

$M = K(\alpha) = spl_K f$

$$|Aut_K(K(\alpha))| = |Gal_K(f)| = \text{no of distinct roots of } f \text{ in } spl_K f$$

FTGT will tell us $[spl_K f : K] = |Gal_K(f)| = \text{no of distinct root of } f$

Note: If f does not split in $M = K(\alpha)$ then

$$|Gal(K(\alpha)|K)| < [K(\alpha) : K]$$

Note: If f splits in $K(\alpha)$ but roots maybe repeating

$$|Gal_K(K(\alpha)|K)| < [K(\alpha) : K]$$

Eg: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

$t^3 - 2$ $|Gal_K(f)| = 1$, $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$

one root but does not split in $\mathbb{Q}(\sqrt[3]{2})$

$gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$ as $\sqrt[3]{2} \to \sqrt[3]{2}$

but $[\mathbb{Q}(2^{1/3}):\mathbb{Q}]=3$ → as f does not split here

Eg: $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$ $\quad f(t) = t^p - x^p \in \mathbb{F}_p(x^p)[t]$

$= (t-x)^p$

($\because$ characteristic is prime p)

$f(t) = (t-x)^p$ splits in $\mathbb{F}_p(x)$

$= \min_{\mathbb{F}_p(x^p)} x$ as of form $(t-x)^p$

So, $x \to x \Rightarrow Gal(\mathbb{F}_p(x)/\mathbb{F}_p(x^p)) = \{id\}$

$\Rightarrow |Gal(\mathbb{F}_p(x)/\mathbb{F}_p(x^p))| = 1 < p = [\mathbb{F}_p(x) : \mathbb{F}_p(x^p)]$

Note: $f \in K[t]$ and f monic f, f' have common root $\alpha \in \bar{K}$

$f = \min_K \alpha$ $\quad f' =$ derivative of f

$\deg f' < \deg f$

$f'(\alpha) = 0 \Rightarrow f' \equiv 0$

Char 0 not possible, so second case cannot happen if char is 0

if $\text{char } K = p > 0$, $f(t) = \sum_{i=0}^{n} a_i x^i$

$f'(t) = \sum i a_i x^{i-1}$

$= 0$

$\Rightarrow i a_i = 0$ in K

$\Leftrightarrow a_i = 0$ or $i = 0$ in K

$\Rightarrow f \in K[t^p]$ (only when $f \in K[t^p]$, second case can happen)

Exe: $f \in K[t]$ has a multiple root α in $\bar{K}$ iff $f(\alpha)=0, f'(\alpha)=0$ → done down

Defn: M/K algebraic ext^n, M/K is normal ext^n if $\forall \alpha \in M$, $\min_K \alpha$ splits in M

Exe: ① K/K is normal

② $\bar{K}/K$ is normal → done down

③ $[M:K]=2$ then M/K is normal

Lemma: M/K algebraic, M/K is normal iff $\forall$ irreducible $f \in K[t]$ either f has no root in M or if f has one root in M then it splits in M

proof: ($\Leftarrow$) $\alpha \in M$, $f = \min_K \alpha \in K[t]$ irreducible

then f splits in f, so extension is normal

($\Rightarrow$) $\forall \alpha \in M$, $\min_K \alpha \in K[t]$ splits in M ($\because M/K$ is normal)

let $f \in K[t]$ be irreducible (wlog it is monic)

if it was no root in M
or it was one root in M

if it has one root in M say α, then as it is ① irreducible ② monic

$$f = \min_K \alpha$$

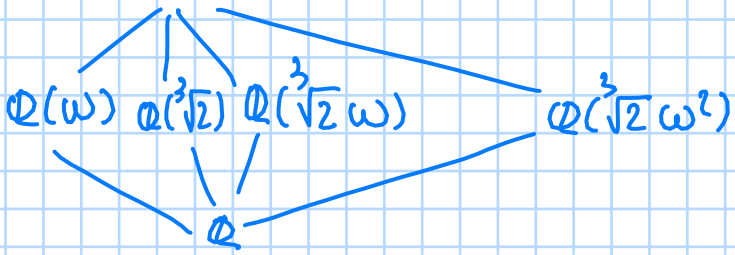
$\Rightarrow f$ splits in M ($\because M/_K$ is normal)

Theorem: $M/_K$ algebraic, then $M/_K$ is finite and normal

$\Leftrightarrow M = \mathrm{spl}_K f$

Eg: from above theorem

$$\mathrm{spl}_{\mathbb{Q}}(t^3-2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$



$$\mathrm{Gal}_{\mathbb{Q}}(t^3-2) = S_3$$

Note: there is a correspondence between subgroups and subfields of S_n and $\mathrm{spl}_K f$ respectively

Exe: Show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{id\}$

Ans:

Let $\phi : \mathbb{R} \to \mathbb{R}$ s.t $\phi_{\mathbb{Q}} = id$

if ϕ is isomorphism, then let $x > 0, x \in \mathbb{R}$

$\exists y \in \mathbb{R}$ s.t $x = y^2 > 0$

$\Rightarrow \phi(x) = \phi(y^2)$

$\Rightarrow \phi(y)^2 > 0$

$\Rightarrow \phi(x) > 0$

So, $x > 0 \Rightarrow \phi(x) > 0$ i.e $a < b$, $b - a > 0$

$\Rightarrow \phi(b-a) > 0$

$\Rightarrow \phi(a) < \phi(b)$

So, ϕ is strictly increasing

also $\phi(r) = r \ \forall r \in \mathbb{Q}$

now, $\forall x \in \mathbb{R}, \exists r, s \in \mathbb{Q}$ s.t

$r < x < s$

$\Rightarrow r < \phi(x) < s$

if $r \to s$ (by continuity we can make them arbitrarily close)

$\Rightarrow \phi(x) = x \quad \forall x \in \mathbb{R}$

so, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{id\}$

Exe: show that

① $\mathrm{Aut}_{\mathbb{Q}}(\bar{\mathbb{Q}} \cap \mathbb{R}) = \{id\}$

② $|\mathrm{Aut}_{\mathbb{Q}}(\bar{\mathbb{Q}})| =$ infinite

Ans: as $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{id\}$

$\Rightarrow \mathrm{Aut}_{\mathbb{Q}}(\bar{\mathbb{Q}} \cap \mathbb{R}) = \{id\}$

as $\bar{\mathbb{Q}} \cap \mathbb{R} \subseteq \mathbb{R}$

let $u_n = \sqrt[2^n]{2}$

also let $F = \mathbb{Q}(u_1, u_2, \ldots) \subset \bar{\mathbb{Q}}$

then $[\mathbb{Q}(u_n) : \mathbb{Q}(u_{n-1})]$

$= [\mathbb{Q}(\sqrt[2^n]{2}) : \mathbb{Q}(\sqrt[2^{n-1}]{2})] = 2$

as $x^2 - u_{n-1}$ is minimal polynomial as not deg $1 \to$ deg 2 smallest

now, $\mathrm{Aut}_{\mathbb{Q}(u_{n-1})}\mathbb{Q}(u_n) = \mathrm{Gal}_{u_{n-1}}(x^2 - u_{n-1}) = \{(1\,2), id\}$

as $\pm u_n$ are conjugates

so, $|\mathrm{Aut}_{\mathbb{Q}(u_{n-1})}\mathbb{Q}(u_n)| = 2 \quad \forall n$

$\mathbb{Q}(u_n)$

$|$ 2

$\mathbb{Q}(u_{n-1})$

$\vdots$

$|$

$\mathbb{Q}(u_1)$

$|$ 2

$\mathbb{Q}$

$\Rightarrow [\mathbb{Q}(u_n) : \mathbb{Q}] = 2^n$

now $|\mathrm{Aut}_{\mathbb{Q}(u_n)}\mathbb{Q}(u_{n+1})| = 2$

any one automorphism from this extends to $\mathbb{Q}(u_{n+2}) \mid \mathbb{Q}(u_n)$ in 2 ways as

$\mathbb{Q}(u_{n+2})$ —( )→ some K isomorphism
|2
$\mathbb{Q}(u_{n+1})$ —φ—( )→ some K isomorphism
|2
$\mathbb{Q}(u_n) = \mathbb{Q}(u_n)$

so, $|\mathrm{Aut}_{\mathbb{Q}(u_n)} \mathbb{Q}(u_{n+2})| = 4$

$\Rightarrow |\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u_n)| = 2^n$

$\Rightarrow \lim_{n\to\infty} 2^n = |\mathrm{Aut}_{\mathbb{Q}} F| \leq |\mathrm{Aut}_{\mathbb{Q}} \bar{\mathbb{Q}}|$

$\Rightarrow |\mathrm{Aut}_{\mathbb{Q}} \bar{\mathbb{Q}}|$ is infinite

Exe: $f \in K[t]$ has a multiple root α in $\bar{K}$ iff $f(\alpha)=0$, $f'(\alpha)=0$

Ans:

($\Rightarrow$) $f \in K[t]$ has multiple root α in $\bar{K}$

then $f(t) = (t-\alpha)^2 g(t)$ in $\bar{K}[t]$ ($\because$ multiple root ≥ 2)

$\Rightarrow f(\alpha)=0$ trivial as it's the root

also $f'(t) = 2(t-\alpha) g(t) + g'(t)(t-\alpha)^2$

$\Rightarrow f'(\alpha) = 0$

($\Leftarrow$) if $f(\alpha)=0$, $f'(\alpha)=0$ then

$f'(t) = (t-\alpha) g(t)$ → some polynomial

$f(t) = \int (t-\alpha) g(t)\, dt$

$= g(t)\frac{(t-\alpha)^2}{2} - \int \frac{g'(t)}{2}(t-\alpha)^2 dt + c$

$g'(t)$ can be some polynomial or constant

if $g'(t)$ is some polynomial we repeate then it is some constant

$\Rightarrow f(t) = (t-\alpha)^2 h(t) + c$

now as $f(\alpha)=0 \Rightarrow c=0$

so, $f(t) = (t-\alpha)^2 h(t)$

or f has multiple root α in $\bar{K}$

Exe: ① $K|_K$ is normal

② $\bar{K}|_K$ is normal

③ $[M:K]=2$ then $M|_K$ is normal

Ans:

$K|_K$ is normal as $\forall \alpha \in K$, $\min_K \alpha = t-\alpha \in K[t]$

splits in K is trivial

$\bar{K}|_K$ is normal as $\forall \alpha \in \bar{K}$, $\min_K \alpha \in K[t]$ as $\alpha \in \bar{K}$

$\Rightarrow$ all roots of $\min_K \alpha \in \bar{K}$

$\Rightarrow \bar{K}$ splits $\min_K \alpha$

if $[M:K]=2$ then M is algebric extension of K

let $\{1, \alpha\}$ be basis of $M:K$

then let $f = \min_K \alpha$ is a deg 2 polynomial

s.t $f=(t-\alpha)(t-\beta) \in K[t]$

$\Rightarrow \alpha+\beta \in K$, $\alpha\beta \in K$ $\beta \notin K$

$\Rightarrow \beta = -\alpha$

so $f = t^2 - \alpha^2$

now, all $\varphi \in M$, if $\varphi \in K$ then trivial

$\min_K \varphi$ just splits in M

if $\varphi \notin K$ then

$\varphi = a + b\alpha$ where $a, b \in K$ $b \neq 0$

then $\deg(\min_K \varphi) \geq 1$

also, $\exists\ g(t) = \left(\left(\frac{t-a}{b}\right)^2 - \alpha^2\right) b^2$ s.t

① it is monic

② $g(\varphi) = 0$

so, g is minimal as deg 2 (smallest possible)

as $g(t) \in K[t]$, $\min_K \varphi$ splits in M

as roots are $a \pm b\alpha \in M$

so, $[M:K]=2 \Rightarrow M$ is normal

10th March :

$L|_K$ is normal if $\forall \alpha \in L$ $\min_K \alpha \in K[t]$ splits in L

Theorem: $L|_K$ is finite and normal iff $L = \text{spl}_K f$ $(f \in K[t])$

proof:

($\Rightarrow$) $L = K(\alpha_1, \alpha_2 \ldots \alpha_n)$ $(\because L|_K$ is finite)

and $L|_K$ is normal

let $f = \prod_{i=1}^{n} \min_K \alpha_i$ then as $\min_K \alpha_i$ splits in L $(\because L|_K$ is normal)

$\Rightarrow f$ splits in L — ①

and $L = K$ (roots of f) — ②

$\Rightarrow L = \text{spl}_K f$ $(\because$ ①, ②)

($\Leftarrow$) $L = \text{spl}_K f$ $f \in K[t]$

$= K(\alpha_1, \alpha_2, \ldots \alpha_n)$ $\alpha_1, \alpha_2, \ldots \alpha_n$ distinct roots of f in L

$[L : K] \leq \deg f|_0 < \infty$

if $\delta \in L$ then $g = \min_K \delta$ splits in L as

$$\begin{array}{c} M = \text{spl}_L\, g \\ | \\ L = K(\alpha_1, \alpha_2, \ldots \alpha_n) \\ | \\ K \end{array}$$

$\xi \in M$ be any root of g if $\xi \in L$ then we are done

$$\begin{array}{ccc} L(\delta) = K(\alpha_1, \ldots \alpha_n, \delta) & & K(\alpha_1, \alpha_2, \ldots \xi) = L(\xi) \\ \| & & | \\ L & K(\delta) \xrightarrow[\cong]{\psi} & K(\xi) \\ & | & | \\ & K = & K \end{array}$$

$$\begin{array}{c} L = \text{spl}_K f \\ \| \\ L(\delta) = \text{spl}_{K(\delta)} f \end{array} \Rightarrow \text{spl}_{K(\delta)} f = L$$

then $\psi_*(f) = f$ $(\because \psi$ is K-isomorphism)

as $f \in K[t]$

$$\begin{array}{ccc} \text{spl}_{K(\delta)} f = L & \xrightarrow{\varphi} & M^* \\ | & & | \\ K(\delta) & \xrightarrow[\cong]{\psi} & K(\xi) \end{array}$$

$\exists$ isomorphism $\varphi : L \to M^*$ extending ψ s.t $\varphi|_{K(\delta)} = \psi$

$\Rightarrow \varphi(L) = M^*$

$\varphi(K(\underbrace{\alpha_1, \alpha_2, \ldots \alpha_n}_{L})) = K(\varphi(\alpha_1), \varphi(\alpha_2), \ldots \varphi(\alpha_n))$

$= L(\varepsilon)$ as $\{\varphi(\alpha_1), \ldots \varphi(\alpha_n)\} = \{\alpha_1, \ldots \alpha_n\}$

as $\alpha_1 \ldots \alpha_n$: roots of f

$\varphi(\alpha_1), \ldots \varphi(\alpha_n)$: roots of $\varphi(f) = f$

so, $M^* = L(\varepsilon)$

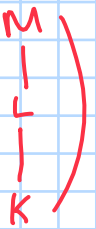
and $\varphi(\delta) = \psi(\delta) = \varepsilon$

$\Rightarrow \varepsilon \in K(\varphi(\alpha_1), \ldots \varphi(\alpha_n))$

$\Rightarrow \varepsilon \in M^* = L(\varepsilon)$

$\Rightarrow \varepsilon \in L$ so we are done

conv: $M|_K$ normal $\Rightarrow M|_L$ normal



proof: $[M:K] < \infty$ and $M|_K$ is normal

$\Rightarrow \exists f \in K[t]$ s.t $M = spl_K f$

$\Rightarrow M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ (roots of f)

$= L(\alpha_1, \alpha_2, \ldots \alpha_n)$

$= spl_L f$

$\Rightarrow M|_L$ is normal

Note: $M|_K$ normal $\not\Rightarrow L|_K$ normal

Eg: $M = \mathbb{Q}(2^{1/3}, e^{2\pi i/3})$

$L = \mathbb{Q}(2^{1/3})$ → Not normal

$K = \mathbb{Q}$

} normal

as $M = spl_{\mathbb{Q}}(t^3 - 2)$

Theorem: $M|_K$ finite normal, $\alpha, \alpha' \in M$ conjugate $/K$ (i.e $\forall g(t) \in K[t]$, $g(\alpha) = 0$ iff $g(\alpha') = 0$)

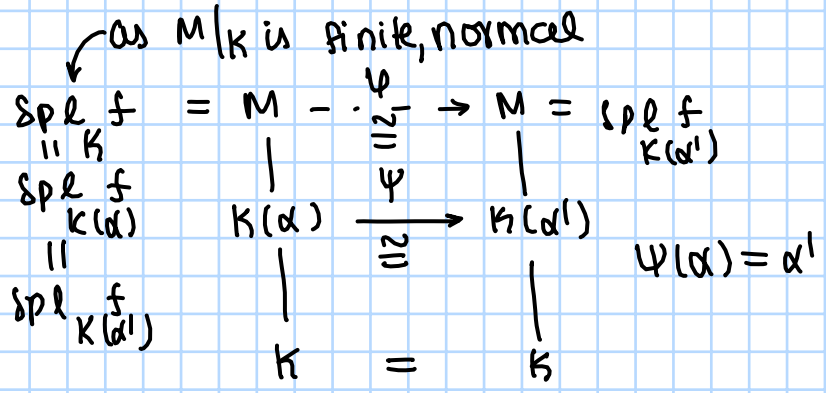
iff $\exists \varphi \in Gal(M|_K)$ s.t $\varphi(\alpha) = \alpha'$

(i.e under action of $Gal(M|_K)$ acts on M α, α' are conjugate $/K$ iff α, α' are in the same orbit)

proof: ($\Rightarrow$)

α, α' are conjugate $/K$

$\Rightarrow \min_K \alpha = \min_K \alpha' = g(t)$



∃ isomorphism $\varphi: M \to M$ extending ψ

$\Rightarrow \varphi \in Aut(M|_K) = Gal(M|_K)$

$\varphi(\alpha) = \psi(\alpha) = \alpha'$

($\Leftarrow$) Assume $\varphi(\alpha) = \alpha'$, $\varphi \in Gal(M|_K)$

if we show $\min_K \alpha = \min_K \alpha'$ then we are done

Let $g(t) = \min_K \alpha \in K[t]$

$$\varphi: \begin{array}{ccc} M & \xrightarrow{\cong} & M \\ | & & | \\ K & = & K \end{array}$$

now, $\varphi_* g = g$, now $(\varphi_* g)(\alpha) = g(\varphi(\alpha)) = g(\alpha') = 0$ as $g(\alpha) = 0$

$\Rightarrow g = \min_K \alpha'$

so, $\min_K \alpha = \min_K \alpha'$

eg: $\mathbb{C}|_{\mathbb{R}}$ finite normal

α, α' conjugate $/\mathbb{R} \Leftrightarrow \exists \varphi \in \{id, \kappa\}$ s.t $\varphi(\alpha) = \alpha'$

i.e $\alpha' \in \{\alpha, \bar{\alpha}\}$

this become same as

α, α' conj $/\mathbb{R} \Leftrightarrow \alpha = \alpha'$ or $\alpha = \bar{\alpha}$

cor: $M|_K$ is finite normal, $M = Spl_K f$ $G = Gal(M|_K) := Gal_K(f)$

G acts on $M = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$ = roots of f

$\Leftrightarrow G$ acts on $\{\alpha_1, \alpha_2, \ldots \alpha_n\}$

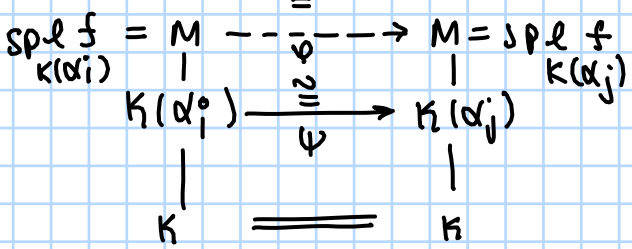
so, $G \to S_n = perm(\{\alpha_1, \alpha_2, \ldots \alpha_n\})$ is an injective group homomorphism

action is transitive

proof: injective is from above calculations

transitive then given α_i, α_j $\exists \varphi \in G$ s.t

$$\varphi(\alpha_i^\circ) = \alpha_j^\circ$$



$$\exists \varphi \in Gal(M|_K) = Gal(spl_K f|_K) = Gal_K(f) = G$$

$$s.t \quad \varphi|_{K(\alpha_i)} = \psi$$

$$\Rightarrow \varphi(\alpha_i) = \alpha_j$$

Note: If f is not irreducible then $\psi : K(\alpha_i) \to K(\alpha_j)$ may not exist

Eg: $f = t^2 - 1 = (t-1)(t+1)$

$gal_{\mathbb{R}}(f) = \{id\}$ as 1 and -1 not conjugate over $\mathbb{R}$

Eg: $M = spl_{\mathbb{Q}} t^3 - 2 = \mathbb{Q}(2^{1/3}, z_3)$ $\quad z_n = e^{2\pi i/n}$

$[M : \mathbb{Q}] = 6$

$f \in \mathbb{Q}[t]$ irreducible, f has 3 distinct roots

$\Rightarrow Gal_{\mathbb{Q}}(f) < S_3 \qquad |S_3| = 3! = 6 \Rightarrow |Gal_{\mathbb{Q}} f| = 3$ or 6

as, $Gal_{\mathbb{Q}}(f)$ is transitive (so, atleast 3 elements needed)

$\Rightarrow Gal_{\mathbb{Q}}(f) \in \{A_3, S_3\}$

roots $\alpha_1 = 2^{1/3} \quad \alpha_2 = 2^{1/3} z_3 \quad \alpha_3 = 2^{1/3} z_3^2 = 2^{1/3} \bar{z}_3 = \overline{2^{1/3} z_3}$

$K : \mathbb{C} \to \mathbb{C}$

$z \mapsto \bar{z}$ $\qquad K : M \to M$ as $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_2$

$\Rightarrow K|_M \in Gal(M|_{\mathbb{Q}})$

and $K^2 = id \Rightarrow$ order of $K = 2$

$\Rightarrow 2 \mid |Gal_{\mathbb{Q}}(f)|$

$\Rightarrow 6 \mid |Gal_{\mathbb{Q}}(f)|$

$\Rightarrow Gal_{\mathbb{Q}}(f) = S_3$

all 6 permutations of $(\alpha_1, \alpha_2, \alpha_3)$ will gives an automorphism of $spl_{\mathbb{Q}} f$

eg: $f(t)=\frac{t^p-1}{t-1}$; p is prime

$= t^{p-1}+t^{p-2}+\dots+1$ irreducible / $\mathbb{Q}$

roots are $\{z, z^2, z^3, \dots z^{p-1}\}$ roots of f $z=z_p$

$\mathbb{Q}(z)=$ spl$_{\mathbb{Q}}$ f $\quad [\mathbb{Q}(z):\mathbb{Q}]=p-1$

$|Gal(\mathbb{Q}(z)|_{\mathbb{Q}})| \leq [\mathbb{Q}(z):\mathbb{Q}] = p-1$

$\Rightarrow |Gal(\mathbb{Q}(z)|\mathbb{Q})| \leq p-1$

let $Gal(\mathbb{Q}(z)|\mathbb{Q}) = G$, $\forall i,j$, $\exists \varphi_{ij} \in G$ s.t

$$\varphi_{ij}(z^i) = z^j$$

$z \xrightarrow{\varphi_p} z^p \quad p=1,2,\dots p-1$

requires $p-1$ automorphisms

$\Rightarrow |G| \geq p-1$

so, $|G|=p-1$ and $G=\{\varphi_1, \varphi_2, \dots \varphi_{p-1}\}$

also $G \cong C_{p-1}$ ← cyclic group as

$\langle z \rangle$ = cyclic of order p

all z^i, $i \in \{1,2,\dots p-1\}$ are generators of $\langle z \rangle$

$G = \langle \varphi_2 \rangle = \langle \varphi_1 \rangle = \langle \varphi_3 \rangle \dots$

now, $\left.\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}\right\}$ finite $\quad M|_K$ normal $\not\Rightarrow L|_K$ is normal

then we want to find some extra condition which will ensure $L|_K$ is normal

$M|_K$ normal $\Rightarrow M|_L$ is normal

$Gal(M|_L) \xrightarrow{\Psi} Gal(M|_K)$; Ψ is injective group homomorphism

$$\left\{ \begin{array}{ccc} \sigma: M & \to & M \\ | & & | \\ L & = & L \\ | & & | \\ K & = & K \end{array} \right\}$$

THEOREM: $L|_K$ is normal iff $\forall \varphi \in Gal(M|_K)$, $\varphi(L) := \{\varphi x \mid x \in L\} = L$

i.e $Gal(M|K) \to Gal(L|K)$ is a surjective group homomorphism

$\sigma \mapsto \sigma|_L$

with normal Gal(M|L)

Theorem: $\begin{matrix} M \\ | \\ L \\ | \\ K \end{matrix}$ finite, $M|_K$ normal, then $L|_K$ is normal iff Gal(M|L) is a normal subgroup of Gal(M|K)

$\frac{Gal(M|K)}{Gal(M|L)} \cong Gal(L|K)$ from above theorem

also, $\begin{matrix} M \\ | \\ L \\ | \\ K \end{matrix}$ normal $\quad H = Gal(M|_L) \leq G = Gal(M|_K)$ ($\because \Psi$ above)

now $L|_K$ is normal iff $H \trianglelefteq G$

in this case $G/H \cong Gal(L|_K)$

eg:

$\begin{matrix} \mathbb{Q}(2^{1/3}, z_3) \\ | \\ \mathbb{Q}(2^{1/3}) \\ | \\ \mathbb{Q} \end{matrix}$ $H \cong S_2 \not\trianglelefteq S_3$

so, $\mathbb{Q}(2^{1/3})|_{\mathbb{Q}}$ not normal

eg: $\begin{matrix} \mathbb{Q}(2^{1/3}, z_3) \\ | \\ \mathbb{Q}(z_3) \\ | \\ \mathbb{Q} \end{matrix}$ $H \cong A_3$ as $H \cong \langle (1,2,3) \rangle$

$2^{1/3} \xrightarrow{\sigma} 2^{1/3} z_3$

then $\sigma^2(2^{1/3}) = \sigma(2^{1/3} z_3)$

$= \sigma(2^{1/3})\,\sigma(z_3)$

$= 2^{1/3}(z_3)^2$

$\alpha_1 \to \alpha_2$

$\alpha_2 \to \alpha_3$

$\alpha_3 \to \alpha_1$

so, $H \cong A_3$ and

$A_3 \trianglelefteq S_3 \Rightarrow S_3/A_3 \cong S_2 \cong Gal(\mathbb{Q}(z_3)|\mathbb{Q})$

13th march:

Theorem: M/K normal $\Rightarrow M/L$ normal

M / L / K : finite

Note: M/K normal $\not\Rightarrow L/K$ normal, we have seen a counterexample

Theorem: M/K is finite normal then

① L/K is normal iff $\sigma L = L$ $\forall \sigma \in Gal(M/K)$

i.e $\forall x \in L$, $\sigma(x) \in L$ $\forall \sigma \in Gal(M/K)$

② Assume L/K is normal, then

ⓐ $Gal(M/L)$ is a normal subgroup of $Gal(M/K)$

ⓑ $Gal(L/K)$ is naturally isomorphic to $\frac{Gal(M/K)}{Gal(M/L)}$

proof: ① ($\Rightarrow$) L/K is normal, $\forall \sigma \in Gal(M/K)$, $\alpha \in L$

then $\sigma\alpha = \alpha'$, α, α' are conjugates in M over K
($\because$ theorm done previously)

$\Rightarrow \min_K \alpha = \min_K \alpha' = g(t) \in K[t]$

L/K is normal, g is irreducible

$g(\alpha) = 0$ $\alpha \in L \Rightarrow$ g splits in L as L/K is normal

$\Rightarrow \alpha' \in L$

so, $\sigma(\alpha) = \alpha' \in L$

$\Rightarrow \sigma(L) \subseteq L$ ——①

as $\sigma \in Gal(M/K)$, $\sigma^{-1} \in Gal(M/K)$

$\Rightarrow \sigma^{-1}(L) \subseteq L$

$\Rightarrow L \subseteq \sigma(L)$ ——②

then from ① ② $L = \sigma(L)$

($\Leftarrow$) Assume $\sigma L = L$ $\forall \sigma \in Gal(M/K)$

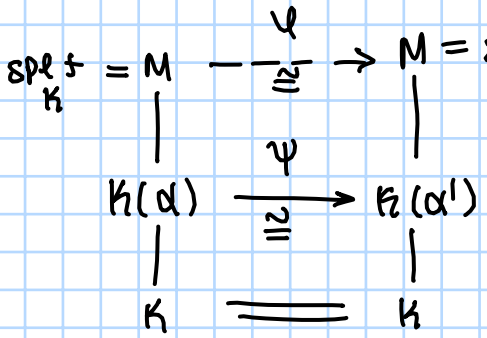
let $\alpha \in L$ $g = \min_K \alpha \in K[t]$ irreducible polynomial

if g splits in L then we are done

as it already splits in M ($\because M/K$ is normal, $\alpha \in L \subseteq M$)

let α' be a root of $g \Rightarrow \alpha' \in M$

$\min_K \alpha = \min_K \alpha' = g$



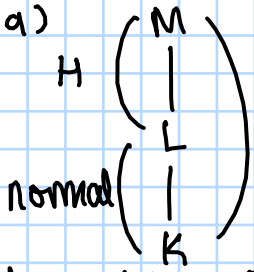
$\Rightarrow \varphi \in \mathrm{Gal}(M|_K)$ as it extends ψ

$\Rightarrow \varphi(\alpha) = \psi(\alpha) = \alpha'$

as $\varphi \in \mathrm{Gal}(M|_K)$ $\varphi(\alpha) \in L \Rightarrow \alpha' \in L$

$\Rightarrow L|_K$ is normal as $\forall \alpha \in L$, $\min_K \alpha$ splits in L

② (a)



$H \trianglelefteq G$ is trivial

$H = \mathrm{Gal}(M|_L)$ $\quad G = \mathrm{Gal}(M|_K)$

let $\sigma \in G$, $\theta \in H$, now if $\underbrace{\sigma\theta\sigma^{-1}}_{\in G} \in H$ then we are done

if $\sigma\theta\sigma^{-1}(x) = x$ $\forall x \in L$, then we are done

as $\sigma \in G$, $\theta \in H \trianglelefteq G$, $\sigma^{-1} \in G$

$\Rightarrow \sigma\theta\sigma^{-1} \in G$

i.e $\sigma\theta\sigma^{-1} : M \to M$

s.t $\sigma\theta\sigma^{-1}|_K = \mathrm{id}$

if $\sigma\theta\sigma^{-1}|_L = \mathrm{id} \Rightarrow \sigma\theta\sigma^{-1} \in H = \mathrm{Gal}(M|_L)$

now, $x \in L$, as $L|_K$ is normal from part 1 of theorem

$\sigma^{-1}(x) \in L$ → $L|k$ normal iff $\sigma(L) = L$

$\theta\sigma^{-1}(x) = \sigma^{-1}(x) \in L$ $(\because \theta \in H, \theta|_L = \mathrm{id})$

$\Rightarrow \sigma\theta\sigma^{-1}(x) = \sigma\sigma^{-1}(x)$

$= x \in L$

so, $\sigma\theta\sigma^{-1}(x) = x$ $\forall x \in L \Rightarrow \sigma\theta\sigma^{-1} \in H = \mathrm{Gal}(M|_K)$

$\Rightarrow H \trianglelefteq G$

(b) now $L|_K$ is normal and $\mathrm{Gal}(M|_L) \trianglelefteq \mathrm{Gal}(M|_K)$

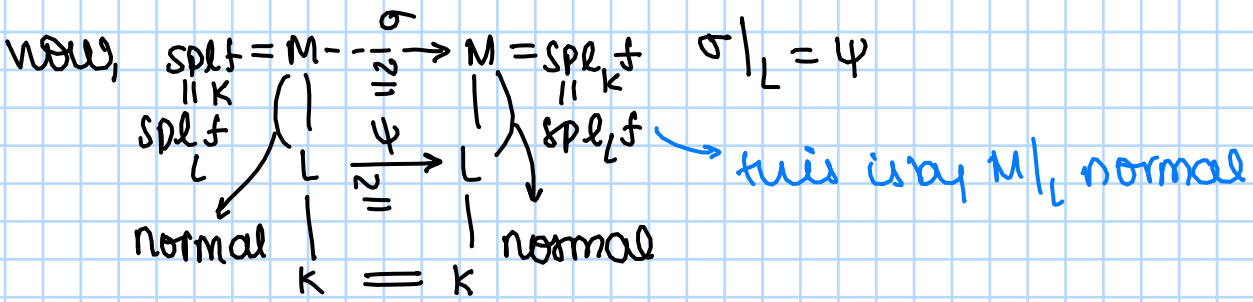
$\mathrm{Gal}(M|_K) \xrightarrow{\Phi} \mathrm{Gal}(L|_K)$

$\sigma \longmapsto \sigma|_L$ $\quad (\because \sigma(L) = L$ by first part$)$

now, if Φ is surjective and $\ker(\Phi) = \mathrm{Gal}(M|_L)$

then, $\dfrac{\mathrm{Gal}(M|_K)}{\mathrm{Gal}(M|_L)} \cong \mathrm{Gal}(L|_K)$

$$\ker(\Phi) = \{\sigma \in \mathrm{Gal}(M|_K) \mid \sigma|_L = id\}$$
$$= \{\sigma \in \mathrm{Gal}(M|_L)\}$$
$$= \mathrm{Gal}(M|_L)$$

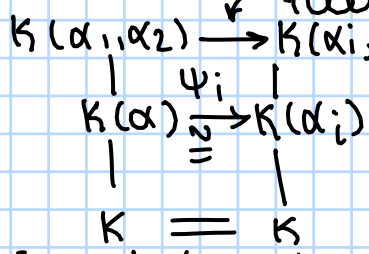
now, 

so, $\forall \psi \in \mathrm{Gal}(L|_K), \exists \sigma$ s.t $\sigma|_L = \psi$ and $\sigma \in \mathrm{Gal}(M|_K)$

$\Rightarrow \Phi$ is surjetic

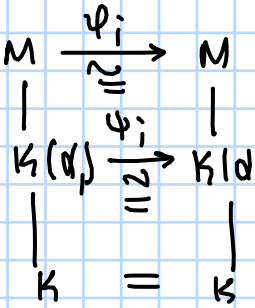
Note: $f \in K[t]$ inducible, $M = \underset{K}{spl} f = K(\alpha_1 \dots \alpha_n)$ $\alpha_1, \alpha_2, \dots \alpha_n$: distinct root of f

they may not be conjugate over $K(\alpha)$



so, it is not true that we can extend ψ_i s.t

$K(\alpha_1, \alpha_2) \xrightarrow{\sim} K(\alpha_i, \alpha_j)$ but if we keep doing it



$\psi_i^0 \to$ we have $|\mathrm{Gal}(M|_L)|$ roots

$\psi_i^1 \to$ we get n diffent entries

aim of galois theory is $|\mathrm{Gal}(M|_K)| = [M:K]$

Note: we already have $|\mathrm{Gal}(M|_K)| \leq [M:K] \leq (\deg f)!$

Def: $f \in K[t]$ inducible is separable if f has no repeated roots in $\underset{K}{spl} f$

if $\deg f = n$, then f has n roots in $\underset{K}{spl} f$ counting multiplicity

f: inducible
f: separable

then f has n distinct roots in spl_K^f

Frobenius map:

① p: prime, $0<i<p$ then p divides $\binom{p}{i}$

② F: ring of char $p>0$ $a,b \in F$

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

$$(ab)^p = a^p b^p$$

$$\theta: \begin{array}{ccc} F & \longrightarrow & F \\ x & \longmapsto & x^p \end{array} \quad \text{char } F = p$$

θ is ring homophism, it is called the frobenius map

now, if F is field then θ is injective

if F is finite field then θ is automorphism

↑ frobenius automorphism

Cor: If char $F = p$, then every $x \in F$ has atmost one p^{th} root in F

F is a field

i.e $\alpha^p = \beta^p = x \in F \Rightarrow \alpha = \beta$

proof:

let $\alpha^p = \beta^p = x$

then $\theta(\alpha) = \theta(\beta)$

θ is one-one

$\Rightarrow \alpha = \beta$

Eg: $F = \mathbb{F}_p$ $\quad \mathbb{F}_p \xrightarrow{\theta} \mathbb{F}_p$

$x \longmapsto x^p$

$(\mathbb{F}_p^{\times})$ group of order $p-1$ $\Rightarrow x^{p-1} = 1 \quad \forall x \in \mathbb{F}_p^{\times}$

$\Rightarrow x^p = x \quad \forall x \in \mathbb{F}_p$

$\Rightarrow \theta|_{\mathbb{F}_p} = id$

so, $\theta: x \longmapsto x$

each elemt of $\mathbb{F}_p$ was a p^{th} root

Eg: $F = \mathbb{F}_p(t)$

$$F \xrightarrow{\theta} F$$

$$\text{img}(\theta) = \theta\left(\frac{f(t)}{g(t)} : f, g \in \mathbb{F}_p[t]\right) = \left(\frac{\theta(f)}{\theta(g)}\right)$$

$$f = a_0 + a_1 t + \cdots + a_n t^n \qquad a_i \in \mathbb{F}_p$$

$$\Rightarrow \theta(f) = \theta(a_0) + \cdots \theta(a_n) t^{pn}$$
$$= a_0 + a_1 t^p + \cdots a_n t^{pn}$$
$$= f(t^p)$$

so, $\text{im}(\theta) = \left\{ \frac{f(t^p)}{g(t^p)} \right\}$, so θ is not an automorphism

as $t \notin \text{img}(\theta)$ so θ is not surjective ($\because$ below exercise)

Exe: show that $t \notin \text{img}(\theta) = \left\{ \frac{f(t^p)}{g(t^p)} \right\}$ → done down

Eg: $F = \mathbb{F}_p(t)$

$X^p - t \in F[X]$, let $u \in$ root

$$u^p - t = 0$$

$$f = x^p - u^p \in spl_F f[X]$$
$$= (X-u)^p$$

f has only one distinct root

as $R = \mathbb{F}_p[t] =$ PID $\Rightarrow t$ is prime ($\because t$ is irreducible)

$f \in R[X]$ $f = X^p - t$

so, $t \nmid 1$ but $t \mid -t$, $t^2 \nmid t$ by division $\Rightarrow f$ is irreducible

also, $f = g.h$ $\deg g < p \Rightarrow g$ splits over $spl_F f[X]$

$\Rightarrow g = (X-u)^i$ $0 < i < p$

coeff of x^{i-1} is $-iu \in F \Rightarrow (-i)^{-1}(i)\, u \in F$

$\Rightarrow u \in F$

but $u = t^{1/p} \notin \mathbb{F}_p(t)$

↓

$t \in \mathbb{F}_p(t^p)$ this is not true as shown in above exercise

so, $f(X) = X^p - t$ is not seperable

Theorm: $f \in K[t]$ irreducible, ① K finite field $\Rightarrow$ f is seperable

② $\text{char } K = 0 \Rightarrow f$ is seperable

Exe: $\theta \in \text{Gal}(M|_K)$ then $\theta|_L \in \text{Gal}(L|_K)$

any extension $\begin{pmatrix} M \\ | \\ L \\ | \\ K \end{pmatrix}$ normal → done down

Exe: Are the rings $\frac{\mathbb{Z}[x]}{\langle x^2+7\rangle}$, $\frac{\mathbb{Z}[x]}{\langle 2x^2+7\rangle}$ isomorphic → done down

and are the rings $\frac{\mathbb{Q}[x]}{\langle x^2+7\rangle}$, $\frac{\mathbb{Q}[x]}{\langle 2x^2+7\rangle}$ isomorphic

Exe: Show that $t \notin \text{img}(\Theta) = \left\{ \frac{f(t^p)}{g(t^p)} \right\}$

Ans: $\left\{ \frac{f(t^p)}{g(t^p)} \right\}$ if $\exists f, g \in \mathbb{F}_p[t]$

s.t $\frac{f(t^p)}{g(t^p)} = t$

then $f(t^p) = t \cdot g(t^p)$

$p(\deg f) = p(\deg g) + 1$

$\Rightarrow p(\deg f - \deg g) = 1$

$\Rightarrow$ as $p \geq 2$ this is not possible

So, $t \notin \left\{ \frac{f(t^p)}{g(t^p)} \right\}$

Exe: any extension $\left(\begin{smallmatrix} M \\ | \\ L \\ | \\ K \end{smallmatrix}\right)$ normal $\varphi \in \text{Gal}(M|_K)$ then $\varphi|_L \in \text{Gal}(L|_K)$

Ans: $\left(\begin{smallmatrix} M \\ | \\ L \\ | \\ K \end{smallmatrix}\right)$ normal

$\varphi \in \text{Aut}_K(M)$

then $\alpha \in L$, as $L|_K$ is normal $\min_K \alpha$ splits in K

any extension

and let $\alpha' = \varphi(\alpha)$ then for $f = \min_K \alpha \in K[t]$

$\varphi_*(f(\alpha)) = f(\varphi_*(\alpha)) = f(\alpha') = 0$

$\Rightarrow \min_K \alpha' = \min_K \alpha$

$\Rightarrow \alpha' \in L$ ($\because L$ splits $\min_K \alpha'$)

$\Rightarrow \varphi(\alpha) \in L$

$\varphi : K(\alpha) \xrightarrow{\cong} K(\alpha')$

$| \quad = \quad |$

$K \quad = \quad K$

So, $\varphi(L) \subseteq L \ \forall \varphi \in \text{Aut}_K(M)$

$\Rightarrow \varphi^{-1}(L) \subseteq L$

$\Rightarrow \varphi(\varphi^{-1}(L)) \subseteq \varphi(L)$

$\Rightarrow L \subseteq \varphi(L)$

So, $L = \varphi(L)$ and $\varphi|_L : L \to L$ is an automorphism s.t $\varphi|_K = id \Rightarrow \varphi|_L \in \text{Gal}(L|_K)$

ex: Are the rings $\frac{\mathbb{Z}[x]}{\langle x^2+7\rangle}$, $\frac{\mathbb{Z}[x]}{\langle 2x^2+7\rangle}$ isomorphic

and are the rings $\frac{\mathbb{Q}[x]}{\langle x^2+7\rangle}$, $\frac{\mathbb{Q}[x]}{\langle 2x^2+7\rangle}$ isomorphic

Ans: $\frac{\mathbb{Z}[x]}{\langle x^2+7\rangle}$ $\frac{\mathbb{Z}[x]}{\langle 2x^2+7\rangle}$

$R = \frac{\mathbb{Z}[x]}{\langle x^2+7\rangle}$

then if 2 is a unit in R, i.e

$2f + (x^2+7)g = 1$ in $\mathbb{Z}[x]$

$(x^2+7)g = 1$ in $\mathbb{Z}/2\mathbb{Z}[x]$

$\Rightarrow 8\, g(1) = 1$ in $\mathbb{Z}/2\mathbb{Z}[x]$

this is a contradiction

so, 2 is not a unit in R

$R' = \frac{\mathbb{Z}[x]}{\langle 2x^2+7\rangle}$ then as $2(x^2+3) = 2x^2+6 = 2x^2+6-2x^2-7$

$\equiv -1$

$\Rightarrow 2$ is a unit in R'

as $2^{-1} \equiv -x^2-3$

as

$2\,2^{-1} = -2x^2-6 \equiv 2x^2+7-2x^2-6$

$\equiv 1$

so, R is not isomorphic to R'

now as $7\nmid 1, 7\mid 7, 7^2\nmid 7 \Rightarrow x^2+7$ is irreducible in $\mathbb{Q}[x]$

also $2x^2+7$ is irreducible (∵ same as above)

so, now $\left[\frac{\mathbb{Q}[x]}{\langle x^2+7\rangle} : \mathbb{Q}\right] = 2$

$\left[\frac{\mathbb{Q}[x]}{\langle 2x^2+7\rangle} : \mathbb{Q}\right] = 2$

so, both are finite fields (∵ $\langle f(x)\rangle$ is maximal)

and same degree over vector space, trivially we can form a trivial isomorphism of basis

$\Rightarrow \frac{\mathbb{Q}[x]}{\langle 2x^2+7\rangle} \cong \frac{\mathbb{Q}[x]}{\langle x^2+7\rangle}$

17th March:

Exe: R, S: Ring with 1, find all ideals, prime ideals, maximal ideals → done down
given for $R, S = \mathbb{Z}, \mathbb{Z}$

we have seen that $f \in K[t]$ irreducible, f is seprable if f has no roots in $spl_K f$, K is any field

this is equivalent as if $\deg f = n$, then f has n distinct roots in $spl_K f$

Defn: $f \in K[t] \setminus 0$ is seprable if all irreducible factors of f are seprable

Eg: $f(t) = t^3 \to$ irreducible factors $= t, t, t$ all seperable

$\Rightarrow f(t)$ is seprable

Eg: $K = \mathbb{F}_p(t)$ $f(x) = x^p - t$ irreducible (∵ done before)
↳ all roots are same
$f(x)$ is not seprable (∵ done before)

Theorem: If $\operatorname{char} K = 0$ or K is a finite field, then all irreducible polynomials in $K[t]$ are seprable

Defn: $f = \sum_0^n a_i t^i \in K[t]$ (K-field)

then $Df := \sum_0^n i a_i t^{i-1} \in K[t]$

Df is called formal derivation of f

Lemma: $D: K[t] \longrightarrow K[t]$
① $D(f+g) = D(f) + D(g)$
② $D(fg) = (Df)g + f \cdot (Dg)$
③ $D(k) = 0$, $k \in K$ constant polynomial

Exe: show above lemma → done down

now, $D: K(t) \longrightarrow K(t)$

$$D\left(\frac{f}{g}\right) = D\left(f \cdot \frac{1}{g}\right)$$

$$D\left(g \cdot \frac{1}{g}\right) = D(1) = 0$$

$$D(g)\frac{1}{g} + g\,D\left(\frac{1}{g}\right) = 0$$

$$\Rightarrow D\left(\frac{1}{g}\right) = -\frac{D(g)}{g^2}$$

so, $D\left(\frac{f}{g}\right) = D\left(f \cdot \frac{1}{g}\right) = D(f)\frac{1}{g} + D\left(\frac{1}{g}\right) f$

$$= \frac{D(f)g}{g^2} - \frac{D(g)f}{g^2}$$

$$= \frac{D(f)g - D(g)f}{g^2}$$

Lemma: $f \in K[t] \setminus 0$ then the following are equivalent

(i) f has repeated roots in $spl_K f$

(ii) f and Df have a common root in $spl_K f$

(iii) f and Df have a common non-constat factor in $K[t]$

proof: (i) $\Rightarrow$ (ii)

$f = (t-\alpha)^2 g$ in $M[t]$ $\quad M = spl_K f$

$Df = 2(t-\alpha)g + (t-\alpha)^2 Dg$

$Df(\alpha) = 0$

(ii) $\Rightarrow$ (iii) $\exists \alpha \in M$ s.t $f(\alpha)=0$, $Df(\alpha)=0$
then $t-\alpha \in M[t]$
$t-\alpha$ is a common factor of f and Df

but $t-\alpha \notin K[t]$ (not always)

but as $K[t]$ is PID $\Rightarrow f \in \langle \min_K \alpha \rangle$

$Df \in \langle \min_K \alpha \rangle$

$\Rightarrow \min_K \alpha \mid f, \min_K \alpha \mid Df$

$\Rightarrow f, Df$ has a common factor in $K[t]$

(iii) $\Rightarrow$ (ii) $f = gf_1$ in $K[t]$
$Df = gf_2$

g is not constant, then as root of g is a root of f

$\exists \alpha \in spl_K f$ s.t $f(\alpha)=0$ & $g(\alpha)=0$

so, $f(\alpha)=0$, $Df(\alpha)=0$ s.t $\alpha \in spl_K f$

(ii) $\Rightarrow$ (i) $f(\alpha)=0$, $(Df)(\alpha)=0$ $\quad f=(t-\alpha)g$ in $M[t]$

$Df = g + (t-\alpha)Dg$ in $M[t]$

$Df(\alpha) = g(\alpha) = 0 \Rightarrow g$ will factor $(t-\alpha)h$

$\Rightarrow f = (t-\alpha)^2 h$

so, α is a repeated root in $spl_K f$

lemma: $f \in K[t]$ is irreducible polynomial, then f is inseparable iff $Df \equiv 0$

proof:

($\Rightarrow$) f is inseparable $\Rightarrow f$ has repeated roots
$\Rightarrow f, Df$ has a common factor in $K[t]$
non-constant

f irreducible $\Rightarrow$ common factor is f itself

$\Rightarrow f \mid Df$ but $\deg f > \deg Df \Rightarrow Df = fh$

$\deg Df = \deg f + \deg h$

$\Rightarrow \deg h = -\infty \Leftrightarrow h = 0$
$\Leftrightarrow Df = 0$

as only polynomial with negative degree is 0 ($\deg = -\infty$)

($\Leftarrow$) f is irreducible and $Df \equiv 0$ then we want to show f is inseparable or f has repeated roots

$\Updownarrow$

f and Df have a common factor in $K[t]$

as $f \mid 0$, $f \mid f \Rightarrow f, Df$ have a common factor in $K[t]$

$\Leftrightarrow f$ has repeated roots

cor: char $K = 0$ then all irreducible $f \in K[t]$ is separable

proof:

$f \notin K$, $f \in K[t]$, f is irreducible and non constant then $Df \neq 0$ ($\because \deg Df = \deg f - 1$)

$\Rightarrow f$ is separable

as $f = a_0 + a_1 t + \cdots a_n t^n$ $n \geq 1$ $a_n \neq 0$

$Df = a_1 + 2a_2 t + \cdots \underbrace{n a_n t^{n-1}}_{\neq 0} \neq 0$

$\neq 0$ as $n \neq 0$ (unit), $a_n \neq 0$ (unit) and char $= 0$

cor: If char $K = p > 0$, $f \in K[t]$ irreducible

f is inseparable $\Leftrightarrow f = a_0 + a_1 t^p + \cdots a_n t^{np} \in K[t^p]$

proof:

($\Leftarrow$) as $Df = p a_1 t^{p-1} + \cdots n a_n p t^{np-1}$
$\equiv 0$ ($\because$ char $= p$)

$\Rightarrow Df \equiv 0$

$\Leftrightarrow f$ is inseparable

($\Rightarrow$) if f is inseparable then $Df \equiv 0$

$f = \sum_{i=0}^{n} a_i t^i$ then $Df = \sum a_i i t^{i-1} = 0$

$\Leftrightarrow i a_i = 0$ in K $\forall i$

$\Leftrightarrow i \mid p$ or $a_i \mid p$ or $i = 0$ or $a_i = 0$

if $i \neq 0$ then $a_i = 0$ (↓ 0) or $a_i \mid p$ (↓ 0) or $i \mid p$ ($\because$ char $= p$)

$\Rightarrow i \mid p$ if $i \neq 0$ else all 0

so, $f = \sum a_i t^{ip}$

def: M/K field extension, $\alpha \in M$ is separable/K if $\min_K \alpha \in K[t]$ is separable polynomial

def: M/K is a separable extension if $\forall \alpha \in M$, α is separable/K

so, if $\alpha \in M$ is separable $/K$, then $\min_K \alpha \in K[t]$ is separable and so

α' conjugate of α

$\min_K \alpha' = \min_K \alpha$ ($\because \alpha', \alpha$ are conjugate)

as $\min_K \alpha$ has no rep roots, no. of conjugates of $\alpha = \deg(\min_K \alpha)$

$f = \min_K \alpha$, then $\{\underset{\parallel}{\alpha_1}, \alpha_2, \dots \alpha_{\deg f}\}$ are conjugates of α in $\operatorname{spe}_K f$
$\quad\ \alpha$

Lemma: char $K = 0$, M/K algebraic extension then M/K is separable extension

proof:
$\forall \alpha \in M$, $\min_K \alpha$ is irreducible ($\because M/K$ is algebraic, so $\min_K \alpha$ exist)

$\Rightarrow \min_K \alpha$ is separable ($\because$ char $K = 0$)

Lemma: $\left.\begin{matrix} M \\ | \\ L \\ | \\ K \end{matrix}\right\}$ algebraic, M/K separable $\Rightarrow M/L$, L/K separable

proof: $\forall \alpha \in M$, $\min_K \alpha$ is separable

now, $\forall \alpha \in L$, $\min_K \alpha$ is inducible ($\because \alpha \in M$)

& separable ($\because$ trivial)

so, L/K is separable

now, $f = \min_K \alpha \in K[t]$ separable for $\alpha \in M$

$g = \min_L \alpha \in L[t]$

then $\langle g \rangle = \ker\left(L[t] \xrightarrow{\Psi} M,\ t \mapsto \alpha,\ \Psi|_L = id \right)$

then $g \mid f \Rightarrow gh = f$ in $L[t]$

f was no repeated roots

$\Rightarrow g$ was no repeated roots

so, g is separable

Lemma: If F is a finite field then $|F| = p^n$ p: prime, $n \geq 1$

Lemma: $\forall$ prime p & $n \geq 1$, $\exists$ a field with p^n elements

proof:

let $M = \operatorname{spe}_{\mathbb{F}_p} f$ $\quad f = t^{p^n} - t$

$Df = p^n t^{p^n - 1} - 1 = -1$ ($\because$ char $\mathbb{F}_p = p$)

$\quad\ = -1 \neq 0$

$\Rightarrow f, Df$ was no, non-constant factors

$\Rightarrow f$ is separable ($\because f, Df$ has no common roots) $\Leftrightarrow f$ has no rep roots

$\Rightarrow f$ has p^n distinct roots

$\Rightarrow |M| \geq p^n$

now, $|M| = p^n$ only when M consist of roots of f, then $|M| = p^n$

roots of polynomial: $f(\alpha) = 0 \Rightarrow \alpha^{p^n} = \alpha$

M is a finite field as it is a $spl_{\mathbb{F}_p} f$

$$[M : \mathbb{F}_p] \leq \deg(f)$$

$$\Rightarrow |M| \leq p^{\deg(f)}$$

$$\Rightarrow |M| < \infty$$

$\theta : M \to M$, $x \mapsto x^p$ Frobenius map

ring homomorphism θ : 1-1

as $|M| < \infty \Rightarrow \theta$ is surjective also

so, θ is an isomorphism

in particular $M = \text{img}(\theta)$

$$= \{ x^p \mid x \in M \}$$

$\theta \circ \dots \circ \theta = \theta^n \in Aut(M)$

$$\text{Find points}(\theta^n) = \{ \beta \in M \mid \theta^n(\beta) = \beta \}$$

$$= \{ \beta \in M \mid \beta^{p^n} = \beta \}$$

$$= \{ \text{zeros of } f \text{ in } M \}$$

$Fix(\theta^n)$ is subfield of M

but by definition of $spl_{\mathbb{F}_p} f$, M has to be smallest possible extension

$$\Rightarrow spl_{\mathbb{F}_p} f = Fix(\theta^n) = M$$

$$\Rightarrow |M| = p^n$$

Note: $M = spl_{\mathbb{F}_p} f$, $f = t^{p^n} - t$, $|M| = p^n$, so if we have two finite fields with

$$|M_1| = p^n, \quad |M_2| = p^n$$

then $M_1 = spl_{\mathbb{F}_p} t^{p^n} - t = M_2$

$\Rightarrow M_1$ and M_2 are isomorphic

upto $\mathbb{F}_p$-isomorphism, $\exists$ unique finite field with p^n elements

Exe: R, S : Ring with 1, find all ideals, prime ideals, maximal ideals
give for $R, S = \mathbb{Z}, \mathbb{Z}$

Ans: R, S Ring with 1

ideals: $\mathbb{Z}/n\mathbb{Z}$ $n \in \{0,1,2,\dots\}$

also $\{0\}$

prime ideals: $\mathbb{Z}/p\mathbb{Z}$ p is prime and $\{0\}$ trivial

$\Updownarrow$

maximal

Exe: show above lemma

Ans:

$D : K[t] \longrightarrow K[t]$

now $f+g = \sum a_i t^i + \sum b_i t^i$

$D(f+g) = \sum i a_i t^{i-1} + \sum i b_i t^{i-1} = D(f) + D(g)$

also $fg = (\sum a_i t^i)(\sum b_j t^j)$

$= \sum\sum a_i b_j t^{i+j}$

$D(fg) = \sum\sum (i+j) a_i b_j t^{i+j-1}$

$= \sum\sum i a_i b_j t^{i+j-1} + \sum\sum j a_i b_j t^{i+j-1}$

$= D(f)g + D(g)f$

K is constant $\Rightarrow$ trivially $D(K) = 0$

20th march :

we have already seen that given prime p, $n \geq 1$, $\exists$ a finite field M with p^n elements

$M = spl_{\mathbb{F}_p} f \qquad f = t^{p^n} - t$

$Df = -1 \Rightarrow f$ has no repeated roots
$\Rightarrow |M| \geq p^n$

also $\theta : M \to M \quad \alpha \to \alpha^p$
θ : frobenius automorphism of M

θ^n : $Fix(\theta^n)$ = fixed field

$\theta^n = \theta$ or roots of f

$\Rightarrow \{\text{roots of } f \text{ in } M\} = Fix(\theta^n) \subseteq M$
(subfield of M)

by construction, M is smallest such, so $M = Fix(\theta^n)$
or $|M| = p^n$

corollary: If M_1, M_2 are fields with p^n elements then M_1, M_2 are isomorphic

proof:
M_1^* : cyclic group of order $p^n - 1$ (∵ done in tutorial)
$\Rightarrow$ every element is root of $t^{p^n - 1} - 1$

$\forall a \in M, \quad a^{p^n - 1} = 1$

$\Rightarrow$ every elemt of M_1 is root of $t^{p^n} - t = f$

now f has p^n distict roots $(Df = -1)$

$\Rightarrow M_1 = \{\text{roots of } t^{p^n} - t\} = spl_{\mathbb{F}_p}(t^{p^n} - t)$

similarly $M_2 = spl_{\mathbb{F}_p}(t^{p^n} - t)$

as any two spl of f over $\mathbb{F}_p$ are isomorphic

$M_1 \cong M_2$

Note: $\mathbb{F}_{p^n}$ = finite field with p^n elements

$\mathbb{F}_p = \mathbb{Z}/p$ but $\mathbb{F}_{p^2} \neq \mathbb{Z}/p^2\mathbb{Z}$

as char $\mathbb{F}_{p^2} = p$ but char $\mathbb{Z}/p^2\mathbb{Z} = p^2$

let $\mathbb{F}_{p^n}^\times = \langle \alpha \rangle$ then from our above construction $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$

$\mathbb{F}_p[X] \xrightarrow{\Phi} \mathbb{F}_p[\alpha]$
$x \longmapsto \alpha$

$\ker \Phi = \{f \in \mathbb{F}_p[X] \mid f(\alpha) = 0\}$
$= \langle f(x) \rangle$ some irreducible polynomial

$\exists!$ f is irreducible polynomial of degree n (monic) on $\mathbb{F}_p[\alpha] = \mathbb{F}_{p^n}$

Theorem: $\mathbb{F}_{p^n}$ is separable over $\mathbb{F}_p$

proof:

$\forall \alpha \in \mathbb{F}_{p^n}$, $\min_{\mathbb{F}_p} \alpha \in \mathbb{F}_p[t]$ by our construction

Theorem: $f \in \mathbb{F}_{p^n}[t]$ irreducible $\Rightarrow$ f is separable

proof:

If not separable then $Df = 0$

$$\Rightarrow f(t) = a_0 + a_p t^p + \cdots a_{mp} t^{mp}$$

$\theta \in Aut(\mathbb{F}_{p^n}) \Rightarrow \mathbb{F}_{p^n} = \{a^p : a \in \mathbb{F}_{p^n}\}$

$$\text{if } a^p = b_0^p$$

$$f = b_0^p + b_1^p t^p + \cdots b_{mp}^p t^{mp}$$

$$= (\underbrace{b_0 + \cdots + b_m t^m}_{\in \mathbb{F}_{p^n}[t]})^p$$

$\Rightarrow f$ is irreducible $\Rightarrow$ contradiction

Lemma: $M|L|K$: algebraic

$M|K$ separable $\Rightarrow$ $M|_L$, $L|_K$ separable

proof: trivial formalization

Lemma: $M|_K$ = finite normal, separable

then $|Gal(M|_K)| = [M:K]$

proof:

$M = Spl_K f = K(\alpha_1, \ldots \alpha_n)$

$\alpha_1 \ldots \alpha_n$: roots of f

$$K(\alpha_1, \alpha_2) \xrightarrow{\varphi_{j,K}} K(\alpha_j, \alpha_{2,K}) \quad K = 1, 2 \ldots n_2$$

$$K(\alpha_1) \xrightarrow{\varphi_j} K(\alpha_j) \quad j = 1, 2 \ldots n_1$$

$$K = K$$

$f_1 = \min_K \alpha_1$ ($\because \alpha_1$ is sep) has roots $\alpha_1 \ldots \alpha_{n_1}$, $n_1 = \deg f_1$

$$|Gal(M|_K)| = |Aut_K(\ell)| = n_1 n_2 \ldots n_h = [M:K]$$

Eg: $M|_K$ separable, not normal

$$Gal\left(\mathbb{Q}(2^{1/3})\big|_{\mathbb{Q}}\right) = \{id\}$$

Eg: $M|_K$ normal, not separable

$F_p(t^{1/p}) \mid F_p(t)$

$\min_{F_p(t)} t^{1/p} = x^p - t = (x - t^{1/p})^p$

$\mathrm{Gal}(F_p(t^{1/p}) \mid F_p(t)) = \{id\}$

Eg:

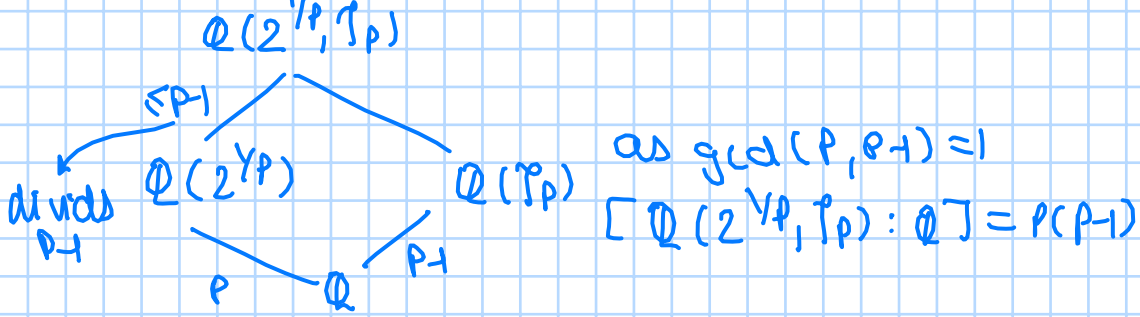
$|\mathrm{Gal}_{\mathbb{Q}}(t^p - 2)| = |\mathrm{Gal}(\mathrm{spl}_{\mathbb{Q}}(t^p - 2) \mid \mathbb{Q})|$

$\mathrm{spl}_{\mathbb{Q}}(t^p - 2) = \mathbb{Q}[2^{1/p}, \gamma_p]$ → seperable as distinct roots

also finite normal is trivial

so, $|\mathrm{Gal}(\mathrm{spl}_{\mathbb{Q}}(t^p - 2 \mid \mathbb{Q})| = [\mathrm{spl}_{\mathbb{Q}}(t^p - 2) : \mathbb{Q}]$

$= [\mathbb{Q}(2^{1/p}, \gamma_p) : \mathbb{Q}]$



Fixed field:

M = field, $\sigma \in \mathrm{Aut}(M)$

Eg: K: prime subfield of $M = \begin{cases} \mathbb{Q}\cdot 1, & \mathrm{char}\, K = 0 \\ \mathbb{Z}/p\mathbb{Z}\cdot 1, & \mathrm{char}\, K = p \end{cases}$

$\sigma|_K = id \Rightarrow \sigma \in \mathrm{Aut}(M|_K)$

now, $\mathrm{Fix}(\sigma) = \{a \in M \mid \sigma(a) = a\} \subseteq M$

subfield of M $S \subseteq \mathrm{Aut}(M)$

$\mathrm{Fix}(S) = \bigcap_{\sigma \in S} \mathrm{Fix}(\sigma)$

↓ subfield of M

THEOREM: H: finite subgroup of $\mathrm{Aut}(M)$

$[M : \mathrm{Fix}(H)] \leq |H|$

proof: let $|H| = n$

M / $\mathrm{Fix}(H)$) if $\alpha_1, \alpha_2 \ldots \alpha_{n+1} \in M$ linearly dependent over $\mathrm{Fix}(H)$

then $[M : \mathrm{Fix}(H)] \leq |H|$

now consider $x_1\sigma(\alpha_1) + x_2\sigma(\alpha_2) \cdots + x_{n+1}\sigma(\alpha_{n+1}) = 0$ $\forall \sigma \in H$, $x_i \in \mathrm{Fix}(H)$

then n-equations, $n+1$ variables

$\Rightarrow$ {solution set is in M^{n+1}} has $\dim_M \geq 1$

non-trivial solution, then we are done

$\in Fix(H^{n+1})$

we want, $(x_1, \ldots x_{n+1}) \in Fix(H^{n+1}) \setminus \{0\}$

if $(x_1 \ldots x_{n+1}) \in M^{n+1}$ is a solution of system

then $(\varphi(x_1), \ldots \varphi(x_{n+1})) \in M^{n+1}$ also solution for all $\varphi \in H$

as, $x_1(\varphi+\sigma)(\alpha_1) + \cdots x_{n+1}(\varphi+\sigma)(\alpha_{n+1}) = 0$

$\Rightarrow \varphi(x_1)\sigma(\alpha_1) + \cdots \varphi(x_{n+1})\sigma(\alpha_{n+1}) = 0$

wlog a non-zero solution with smallest no. of non-zero

$(x_1, x_2, \ldots x_\ell, 0, \ldots 0)$ is a solution

$1 \leq \ell \leq n+1$

$x_1 \ldots x_\ell \neq 0$

$\Rightarrow x_\ell^{-1}(x_1 \ldots x_\ell, 0, \ldots 0)$ is also a solution

so we may assume $(x_1, \ldots x_{\ell-1}, 1, 0, 0 \ldots 0)$ is a solution

$\Rightarrow (\varphi(x_1), \ldots \varphi(x_{\ell-1}), 1, 0, \ldots 0)$ is a solution $\forall \varphi \in H$

$\Rightarrow (\varphi(x_1) - x_1, \ldots \varphi(x_{\ell-1}) - x_{\ell-1}, 0, \ldots 0)$

$\downarrow$

eigenvector solution

by minimality of $\ell \Rightarrow \varphi(x_i) = x_i \ \forall i \ \forall \varphi \in H$

$\Rightarrow (x_1, \ldots x_\ell, 0, \ldots 0) \in Fix(H^{n+1})$

$\Rightarrow x_1\alpha_1 + \cdots x_\ell\alpha_\ell = 0$ LD over $Fix(H^{n+1})$

Eg: $K: \mathbb{C} \longrightarrow \mathbb{C}$

$\| \quad \|$

$\alpha \longmapsto \bar{\alpha}$

$H = \langle K \rangle$ of order 2 $= \{id, K\}$

$[\mathbb{C} : Fix(H)] \leq 2$

$\|$

$\mathbb{R}$

Eg: $Gal\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}\right) = Aut_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right)$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = spl_{\mathbb{Q}}(x^2-2)(x^2-3)$

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 \quad \sigma = \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad \tau = \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases}$

$\infty_1 \ G = \{1, \sigma, \tau, \sigma\tau\} = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) / \langle\sigma\rangle\langle\tau\rangle$

as $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{0,1\} \times \{0,1\}$

$= \{(0,0), (0,1), (1,0), (1,1)\}$

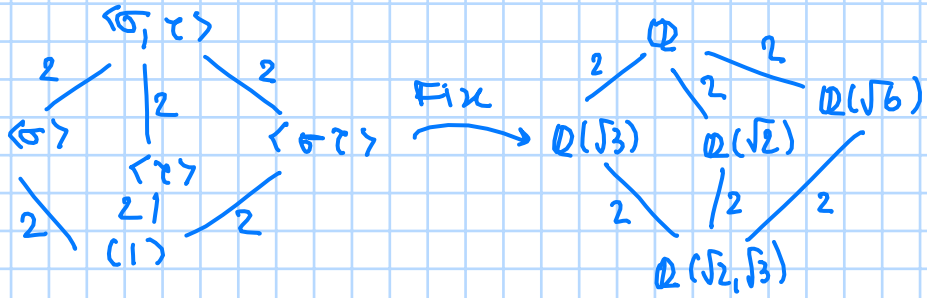
this does not work, so we consider $\langle\sigma\rangle \times \langle\tau\rangle$

now, $\text{Fix}(\langle\sigma\rangle) = \mathbb{Q}(\sqrt{2})$

$O(\sigma) = 2$

$\text{Fix}(\langle\tau\rangle) = \mathbb{Q}(\sqrt{3})$

now, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \text{Fix}(\sigma)] \leq 2$



$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \text{Fix}(\sigma)] = 2$

24th March :

M/K field extension, $\mathcal{H} = \{\text{subfields of } M/K\}$

$= \{L : K \subset L \subset M\}$

↖ subfield of M

$\mathcal{G} = \{\text{subgroups of } Gal(M/K)\}$

$$\begin{array}{ccccc} L & \xrightarrow{Gal(M/-)} & \mathcal{G} & \xrightarrow{Fix(-)} & \mathcal{H} \\ \cap & & & & \\ \mathcal{H} & & H & \longmapsto & Fix(H) \\ & & \cap & & \\ & & \mathcal{G} & (\because \text{it fixes } L) & \end{array}$$

$H < Gal(M/K)$ $\quad M > Fix(H) > K$

Lemma : ① $L_1 \subset L_2 \in \mathcal{H}$

$Gal(M/L_1) \supseteq Gal(M/L_2)$

② $H_1 \leq H_2 \in \mathcal{G}$ then $Fix(H_1) \supseteq Fix(H_2)$

proof : From below diagram, both follow

$$\begin{array}{ccc} M & & Gal(M/M) \\ \cup & & \cap \\ L_2 & Gal(M/-) & Gal(M/L_2) \\ \cup & \longrightarrow & \cap \\ L_1 & & Gal(M/L_1) \\ \cup & & \cap \\ K & & Gal(M/K) \end{array}$$

$$\begin{array}{ccc} M & & (1) \\ \cup & & \cap \\ Fix(H_1) & Fix(-) & H_1 \\ \cup & \longleftarrow & \cap \\ Fix(H_2) & & H_2 \\ \cup & & \cap \\ Fix(Gal(M/K)) & & Gal(M/K) \end{array}$$

Note: From above, $Gal(M/-) : \mathcal{H} \to \mathcal{G}$ is inclusion reversing

and $Fix(-) : \mathcal{G} \to \mathcal{H}$ is also inclusion reversing

Lemma: $L \in \mathcal{H}$, $H \in \mathcal{G}$ $\quad L \subset Fix(H) \Leftrightarrow H \subset Gal(M/L)$

proof :

$L \subset Fix(H) \Leftrightarrow \sigma$ fixes L elementwise $\forall \sigma \in H$

$\sigma a = a \quad \forall a \in L$, σ is an automorphism ($\because$ def^n)

$H \subset Gal(M/L) \Leftrightarrow \sigma \in H$ s.t $\sigma(a) = a \quad \forall a \in L$ and σ is automorphism

Lemma: $L \subset Fix(Gal(M/L))$ and $H \subset Gal(M/Fix(H))$

proof:

$H = Gal(M|L) \Rightarrow L \subset Fix(H) \Rightarrow L \subset Fix(Gal(M|L))$

(∵ previous lemma)

similarly let $L = Fix(H) \subseteq Fix(H)$

$\Rightarrow H \subset Gal(M|L)$

$\Rightarrow H \subset Gal(M|Fix(H))$

(∵ previous lemma)

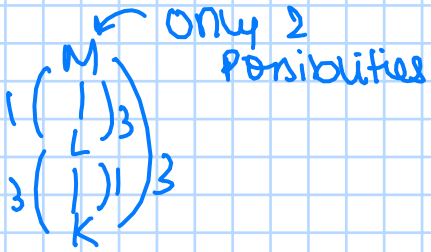
$$\begin{array}{ccc} L \in \mathcal{H} & \xrightarrow{Gal(M|_)} & Gal(M|L) \\ \cap & & \downarrow Fix(_) \\ & & Fix(Gal(M|L)) \end{array}$$

$$\begin{array}{ccc} H \in \mathcal{G} & \xrightarrow{Fix(_)} & Fix(H) \\ \cap & & \downarrow Gal(M|_) \\ & & Gal(M|Fix(H)) \end{array}$$

eg: $\mathbb{Q}(2^{1/3}) \,|\, \mathbb{Q} = M|_k$, $Gal(M|_k) = \{id\}$

$\mathcal{H} = \{\mathbb{Q}, \mathbb{Q}(2^{\frac{1}{3}})\}$

$\mathcal{G} = \{(1)\}$



$$\begin{array}{ccc} (1) \in \mathcal{G} & \xrightarrow{Fix(_)} & \mathbb{Q}(2^{\frac{1}{3}}) \\ \cap & & \downarrow Gal(\mathbb{Q}(2^{\frac{1}{3}})|_) \\ & & (1) \end{array}$$

$$\begin{array}{ccc} \mathbb{Q}(2^{\frac{1}{3}}) & \xrightarrow{Gal(\mathbb{Q}(2^{\frac{1}{3}})|_)} & (1) \\ \cap & & \downarrow Fix(_) \\ & & \mathbb{Q}(2^{\frac{1}{3}}) \end{array}$$

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{Gal(\mathbb{Q}(2^{\frac{1}{3}})|_)} & (1) \\ \cap & & \downarrow Fix(_) \\ & & \mathbb{Q}(2^{\frac{1}{3}}) \end{array}$$

Fundamental theorem of Galois theory:

Theorem: $M|_k$ finite, normal, separable then

① $\mathcal{H} \underset{\text{Fix}(-)}{\overset{\text{Gal}(M|-)}{\rightleftarrows}} \mathcal{G}$ are inverse to each other

② $|\text{Gal}(M|_L)| = [M:L] \ \forall L \in \mathcal{G}$
$|H| = [M:\text{Fix}(H)] \ \forall H \in \mathcal{G}$

③ $L|_k$ is normal extension $\Leftrightarrow \text{Gal}(M|_L) \trianglelefteq \text{Gal}(M|_k)$
normal subgroup

④ If $L|_k$ is normal then
$$\frac{\text{Gal}(M|k)}{\text{Gal}(M|_L)} \cong \text{Gal}(L|_k)$$

proof: $H \in \mathcal{G}$, $H \leq \text{Gal}(M|_{\text{Fix}(H)})$ ($\because$ previous lemma)

$\Rightarrow |H| \leq |\text{Gal}(M|\text{Fix}(H))|$

$= [M:\text{Fix}(H)]$ ($\because$ $M|_L$ finite normal separable then $[M:L] = |\text{Gal}(M|L)|$ done before)

as M / $\text{Fix}(H)$ / K — normal separable

$\Rightarrow$ M / $\text{Fix}(H)$ is normal separable

now, $|H| \leq [M:\text{Fix}(H)]$

in last case we have shown that

$[M:\text{Fix}(H)] \leq |H|$ ($\because$ $H < \text{Aut}(M)$, finite then $[M:\text{Fix}(H)] \leq |H|$)

$\Rightarrow |H| = [M:\text{Fix}(H)]$ —— ①

now $|\underbrace{\text{Gal}(M|L)}_{H}| = [M:\text{Fix}(H)]$ ($\because$ ①)

$= [M:\text{Fix}(\text{Gal}(M|_L))]$

M / $\text{Fix}(\text{Gal}(M|L))$ / L

but as $M|_L$ is Normal, seperable ($\because$ M / L / K)

$\Rightarrow |Gal(M|L)| = [M:L] = [M:Fix(Gal(M|L))]$ — ②

$[M:L]\left(\begin{array}{c} [M:L]\left(\begin{array}{c} M \\ | \\ Fix(Gal(M|L)) \end{array} \right. \\ , \left(\begin{array}{c} | \\ L \end{array} \right. \end{array} \right.$

$\Rightarrow L = Fix(Gal(M|L))$

$\Rightarrow Fix \circ Gal(M|_) = id_{\mathcal{H}}$ — ③

①, ② shows part (2)

③ shows one way of part (1)

$$\begin{array}{ccc} H & \xrightarrow{Fix(_)} & Fix(H) \\ \subset & & \downarrow Gal(M|_) \\ & & Gal(M|Fix(H)) \end{array}$$

$\Rightarrow H \subset Gal(M|Fix(H))$
and their orders are same ($\because$ ①)

$\Rightarrow H = Gal(M|Fix(H))$ ($\because$ finite and same order) — ④

so, ③, ④ shows (1)

in (3) ($\Rightarrow$) is done before

($\Leftarrow$) given $Gal(M|_L) \triangleleft Gal(M|_K)$ we want to show that $L|_K$ is normal ext^n

equivalently, we have to show $\sigma L = L \quad \forall \sigma \in Gal(M|K)$
($\because$ theorem done before)

$\sigma L = \{\sigma a : a \in L\}$ → this is from previous part

now, first show that $\leq$: group acting on a set X

$H \leq G, \ g \in G$

then, $Fix(gHg^{-1}) = g\,Fix(H)$

where $Fix(H) = \{x \in X \mid \sigma x = x, \ \forall \sigma \in H\}$

$$\begin{aligned} Fix(gHg^{-1}) &= \{x \in X \mid ghg^{-1}(x) = x, \ \forall h \in H\} \\ &= \{x \in X \mid hg^{-1}(x) = g^{-1}(x), \ \forall h \in H\} \\ &= \{x \in X \mid g^{-1}(x) \in Fix(H)\} \\ &= g\,Fix(H) \end{aligned}$$

now, $G = Gal(M|_K)$ acts on M

$H = Gal(M|_L) \trianglelefteq Gal(M|_K)$

then $Fix(gHg^{-1}) = Fix(H)$ $(\because g \in G)$

$= gFix(H)$ $(gHg^{-1} = H, \forall g \in G)$

$\Rightarrow Fix(H) = Fix(Gal(M|_L))$

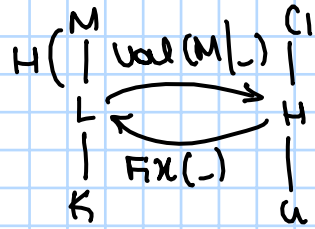
$= L$ $(\because$ part (1)$)$

$\Rightarrow Fix(H) = L = gFix(H)$

$\Rightarrow L$ is normal as $gL = L \ \forall g \in Gal(M|_K)$

part (4) is already done before

Note:



$M|_K$ is finite, normal, separable

$\Rightarrow M|_L$: finite, normal, separable

$\Rightarrow Gal(M|_L) = H$, $Fix(H) = L$

Note: $M|_K$ finite $\&x^n \Rightarrow G = Gal(M|_K)$ is finite

$\Rightarrow \mathcal{G} =$ subgroup of G is finite

Note: FTGT shows that if $M|_K$ is normal and seperable, then we will have

$|\mathcal{G}| = |\mathcal{H}|$

$\Rightarrow \exists$ only finite many subfields of $M|_K$

In general, $M|_K$ finite $\not\Rightarrow \mathcal{H}$ is finite

also, $M|_K$ finite normal, then $M = spl_K f$

$Gal(M|_K)$ acts on M

$Gal(M|_K)$ acts on $\Sigma = \{$roots of f in $M\}$

then action is faithful as

$Gal(M|_K) \subset Perm(\Sigma)$ is injective

if $|\Sigma| = n$ then, $|Gal(M|_K)| \mid n!$

Note: If $\alpha, \beta \in \Sigma$, then $\exists \varphi \in Gal(M|_K)$, $\varphi\alpha = \beta$ iff α, β are conjugates $/K$

iff $\min_K \alpha = \min_K \beta$

So, if f is irreducible $\Rightarrow Gal(M|_K)$ acts transitively on Σ

Eg: $M|_K$ finite, seperable, normal $[M:K] = p$ (prime) then

$\mathcal{F} = \{M, K\}$ ($\because$ prime degree)

$\mathcal{G} = \{(1), \mathrm{Gal}(M|K)\}$ by FTGT

$|\mathrm{Gal}(M|K)| = p$

$[M:K]$ $\quad \mathrm{Gal}(M|K) \cong C_p$ ← cyclic group of order p

Eg: $f = (t^2+1)(t^2-2)$

$M = \mathrm{spl}_{\mathbb{Q}} f = \mathbb{Q}(i, \sqrt{2})$ $\quad [M:\mathbb{Q}] = 4$

$\Rightarrow |\mathrm{Gal}(M|\mathbb{Q})| = 4$

$\mathbb{Q}(i)$

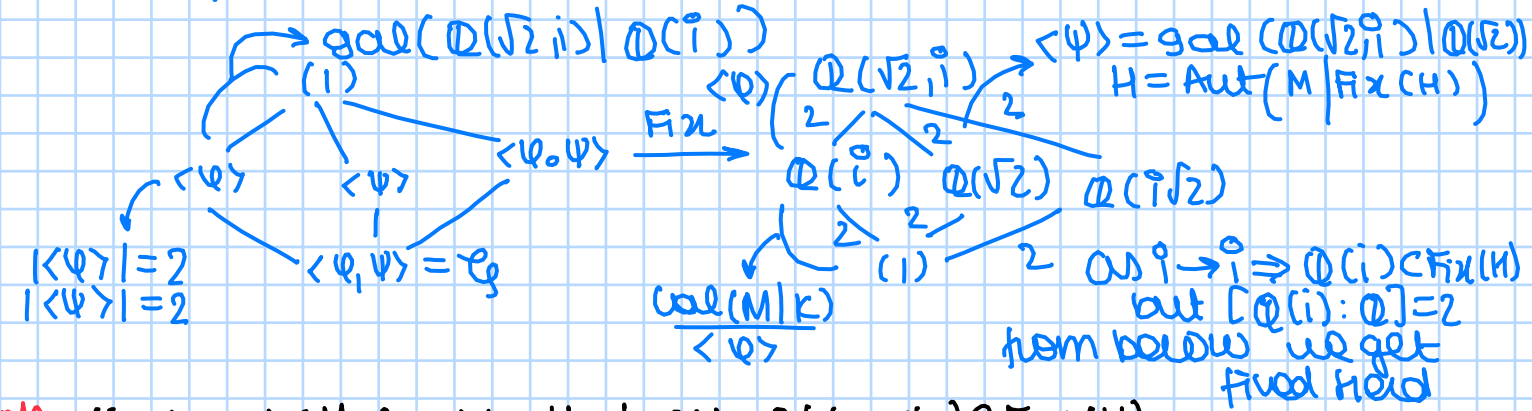
$\Sigma = \{\text{roots of } f\}$

$\mathbb{Q}$ $\quad = \{\pm i, \pm\sqrt{2}\}$

Conjugates $(i, -i)$, $(\sqrt{2}, -\sqrt{2})$

$\Rightarrow \mathrm{Gal}(M|\mathbb{Q}) = \{ \underset{}{\mathrm{id}},\ \underset{\sqrt{2}\to-\sqrt{2},\ i\to i}{\varphi},\ \underset{\sqrt{2}\to\sqrt{2},\ i\to -i}{\psi},\ \underset{\sqrt{2}\to-\sqrt{2},\ i\to -i}{\varphi\circ\psi} \}$

$\because \mathrm{Gal}(M|\mathbb{Q}) \cong C_2 \times C_2$



Note: if $\alpha_1 \dots \alpha_r \in M$ fixed by H then $\mathbb{Q}(\alpha_1 \dots \alpha_r) \subseteq \mathrm{Fix}(H)$

$\mathbb{Q}(\alpha_1 \dots \alpha_r) = \mathrm{Fix}(H)$

iff $[M : \mathbb{Q}(\alpha_1 \dots \alpha_r)] = [M : \mathrm{Fix}(H)] = |H|$

27th March :

Defn: M/K is galois extension if M/K is finite, normal, separable

Theorm: M/K is galois extension then

$$\mathcal{H} = \{\text{subfields of } M/K\} \longleftrightarrow \mathcal{G} = \{\text{subgroups of } \mathrm{Gal}(M/L)\}$$

Cor:

$$\begin{array}{ccc} M & & (1) \\ | & \mathrm{Gal}(M/-) \rightarrow & | \\ L & \leftarrow \mathrm{Fix}(-) & \mathrm{Gal}(M/L) \\ | & & | \\ K & & \mathrm{Gal}(M/K) = G \end{array}$$

$\mathrm{Fix}(\mathrm{Gal}(M/K)) = K$
$\forall\ \alpha \in M \setminus K,\ \exists\ \varphi \in G$ s.t. $\varphi\alpha \neq \alpha$

proof: It follows from previous theorm

eg: $f = t^4 - 2 \in \mathbb{Q}[t]$

↑ induce $\mathrm{Spl}_{\mathbb{Q}} f = \mathbb{Q}(2^{\frac{1}{4}}, i)$

$$\Sigma = \{\pm 2^{\frac{1}{4}}, \pm i 2^{\frac{1}{4}}\}$$

$$\begin{array}{ccc} \mathbb{Q}(2^{\frac{1}{4}}, i) & & \\ | \ 2 & & \\ \mathbb{Q}(2^{\frac{1}{4}}) & \Big) 8 & \Big) \mathrm{Gal}(f) \ |G| = [M:\mathbb{Q}] \\ | \ 4 & & \\ \mathbb{Q} & & \end{array}$$

any $\varphi \in G$ is uniquely determined by $\varphi 2^{\frac{1}{4}}$, φi

conjugates of $2^{\frac{1}{4}}/\mathbb{Q}$ are $\{\pm 2^{\frac{1}{4}}, \pm i 2^{\frac{1}{4}}\}$

conjugates of $i/\mathbb{Q}$ are $\{\pm i\}$

maximum no of φ is $4 \times 2 = 8$

we know that $|G| = 8 \Rightarrow$ all choices of $\varphi 2^{\frac{1}{4}}, \varphi i$ gives all elements of G

$$\rho : \begin{array}{l} 2^{\frac{1}{4}} \rightarrow i 2^{\frac{1}{4}} \\ i \rightarrow i \end{array}$$

$$2^{\frac{1}{4}} \xrightarrow{\rho} i 2^{\frac{1}{4}} \xrightarrow{\rho} -2^{\frac{1}{4}} \xrightarrow{\rho} -i 2^{\frac{1}{4}} \xrightarrow{\rho} 2^{\frac{1}{4}}$$

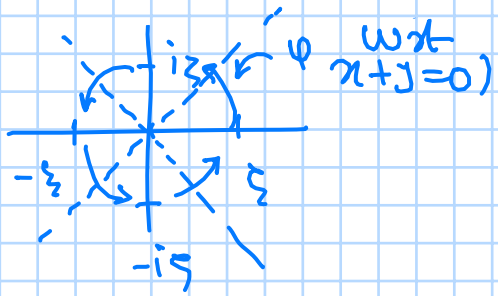
$o(\rho) = 4$ $\quad \kappa : \begin{array}{l} 2^{\frac{1}{4}} \rightarrow 2^{\frac{1}{4}} \\ i \rightarrow -i \end{array}$ $\quad o(\kappa) = 2$

$\kappa \notin \langle \rho \rangle$

$G = \langle \rho, \kappa \mid \rho^4 = 1,\ \kappa^2 = 1,\ \kappa\rho\kappa = \rho^{-1} \rangle$ ← dihedral / symmetries of square

$\varphi \in G$	$\varphi 2^{\frac{1}{4}}$	φi	$\varphi(i 2^{\frac{1}{4}})$	order of φ
id	$2^{\frac{1}{4}}$	i	$i 2^{\frac{1}{4}}$	1
ρ	$i 2^{\frac{1}{4}}$	i	$-2^{\frac{1}{4}}$	4
ρ^2	$-2^{\frac{1}{4}}$	i	$-i 2^{\frac{1}{4}}$	2
ρ^3	$-i 2^{\frac{1}{4}}$	i	$2^{\frac{1}{4}}$	4

Reflection in x-axis	K	$2^{1/4}$	$-i$	$-i2^{1/4}$	2
$x+y=0$	Kp	$-i2^{1/4}$	$-i$	$-2^{1/4}$	2
y axis	Kp^2	$-2^{1/4}$	$-i$	$i2^{1/4}$	2
$x-y=0$	Kp^3	$i2^{1/4}$	$-i$	$2^{1/4}$	2



now, $|G|=8$, H is a proper subgroup then $|H|=2$ or 4

order 2 - subgroups:

$\langle p^2\rangle, \langle K\rangle, \langle Kp\rangle, \langle Kp^2\rangle, \langle Kp^3\rangle$

normal subgroups:

$Kp^2 = p^{-2}K$
$= p^2K$
$(\because o(p)=4)$

$KpK^{-1} = p^{-1}$
$\Rightarrow (KpK^{-1})^r = p^{-r}$
$\Rightarrow Kp^{-1}K^{-1} = p^{-r}$
$\Rightarrow Kp^r = p^{-r}K$

$\Rightarrow p^2 \in Z(G)$ ↑ cover as it commutes with generators

$\Rightarrow \langle p^2\rangle$ is normal

now, $p(Kp^i)^{-1}p = Kp^{-1}p^ip^{-1} = Kp^{i-2}$

$o(Kp^i)=2$, $Kp^i = Kp^{i-2} \Rightarrow p^2 = id$ which is a contradiction $(\because o(Kp^i)=2)$

as $g: G \to G$, $x \to gxg^{-1}$ is an automorphism and non-trivial element goes non trivial element (if $\langle Kp^i\rangle$ is normal)

$\Rightarrow \langle Kp^i\rangle$ not normal $\forall i$

$\Rightarrow \langle p^2\rangle$ is only normal order 2

now if $H \leq G$, $|H| = \frac{|G|}{2}$ then $H \trianglelefteq G$ is always true,

order 4 are: $\langle p\rangle$

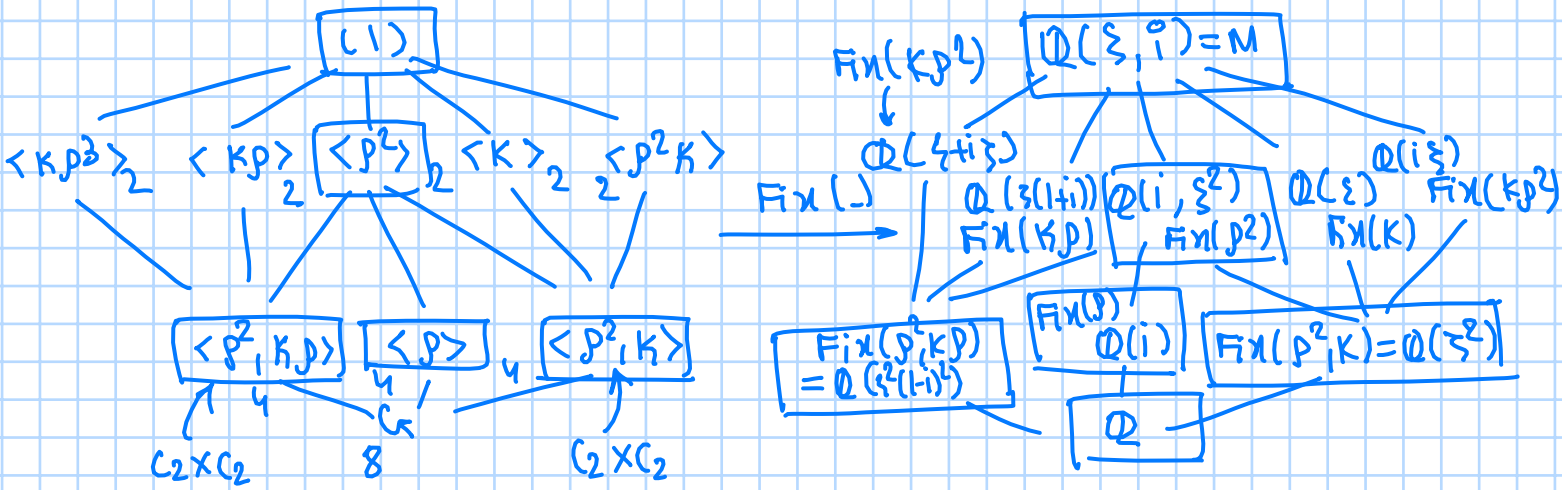
if $|H|=4$ $Kp^i, Kp^j \in H$ $i>j$

$\Rightarrow Kp^i(Kp^j)H = Kp^{i-j}K^{-1} \in H$
$= (KpK^{-1})^{i-j} \in H$
$= (p^{-1})^{i-j} \in H$

but $p \notin H$ as if $p \in H \Rightarrow K \in H$ $(\because Kp^i \in H)$
$\Rightarrow H = G$ (contradiction)

so, $(p^{-1})^{i-j} = p^2 \in H$, then $K \in H$ (of any order 2)

$\langle p\rangle$, $\langle p^2, K\rangle$, $\langle p^2, Kp\rangle$
$\langle p^2, Kp^2\rangle$, $\langle p^2, Kp^3\rangle$



$|H|$ | M ← Galois ext with Galois group H

$L = Fix(H)$

M | 4

$Fix(\rho) = \mathbb{Q}(i)$

| 2

$\mathbb{Q}$

M

$Fix(\rho^2) = \mathbb{Q}(i, \xi^2)$

$\mathbb{Q}$

$k\rho$: $\xi \to -i\xi$ } $\xi - i\xi \Rightarrow -i\xi + \xi$ $\quad Fix(\rho^2, k) = Fix(\rho^2) \cap Fix(k)$

$-i\xi \to ?$ }

were the bond ones are normal ⇒ galois

Ex: show that $k\rho k = \rho^{-1}$ i.e $k\rho = \rho^{-1}k$ or $k\rho(\xi) = \rho^{-1}k(\xi)$ → done done

$k\rho(i) = \rho^{-1}k(i)$

Solvable groups:

Defn: G is a group, G is solvable if $\exists$ a sequence $G_0 = (1) \trianglelefteq G_1 \trianglelefteq G_2 \cdots \trianglelefteq G_n = G$ s.t G_{i+1}/G_i is abelian

Theorem: $f \in \mathbb{Q}[t]$ is solvable by radicals, $\bigcup K_n$ = radical extension of $\mathbb{Q}$

$\mathbb{Q} \subset K_1 = \mathbb{Q}(\sqrt[n]{a} \mid a \in \mathbb{Q}, n \geq 1) \subset K_1(\sqrt{a}, a \in K_1, n \geq 1) \cdots$

$\bigcup_{n \geq 1} K_n$ is a radical expression of radical coming from $\mathbb{Q}$

(i.e roots of f lie in radical extension of $\mathbb{Q}$)

iff $Gal_{\mathbb{Q}}(f)$ is a solvable group

we will see that S_5 is not solvable, i.e if $\deg f = 5$ and $Gal_{\mathbb{Q}}(f) = S_5$ then f is not solvable by radicals

similarly S_n $n \geq 5$ this holds true

Note: S_4 is solvable, so upto deg 4 we can solve polynomials by radicals

Defn: G, group $G^{(0)} = G \supseteq G^{(1)} = [G, G] \supseteq G^{(2)} = [G^{(1)}, G^{(1)}] \supseteq \cdots$

$= $ subgroup of G generated by $\{xyx^{-1}y^{-1} \mid x, y \in G\}$

is called the derived series of G

Eg: $G^{(0)} = G$ $\quad G^{(1)} = [G, G] = G$ then

$G^{(n)} = G$ and it keeps on going

Defn: $[G, G]$ is called commutator of G

Defn: if $[G, G] = G$ then G is called perfect

Theorem: G is solvable iff $G^{(n)} = (1)$ for some n

Conv: $G \xrightarrow{\varphi} \tilde{G}$ surjective group homomorphism

① $\varphi(G^{(i)}) \subset \tilde{G}^{(i)}$

② if G is solvable $\Rightarrow \tilde{G} = \varphi(G)$ is solvable

③ if G is solvable and $H \leq G$ then H is solvable

④ if G is solvable and $N \trianglelefteq G$ then $G|_N$ is solvable

⑤ If $N \trianglelefteq G$, N and $G|_N$ both solvable then G is solvable

⑥ G_1, G_2 solvable $\Rightarrow G_1 \times G_2$ solvable

proof:

① $G \xrightarrow{\varphi} \tilde{G}$ $\forall\, \tilde{g} \in \tilde{G}, \exists\, g \in G$ s.t $\varphi(g) = \tilde{g}$

now, let $G^{(0)} = G$

$$G^{(n)} = [G^{(n-1)} : G^{(n-1)}] = \left\{ xyx^{-1}y^{-1} \,\middle|\, x, y \in G^{(n-1)} \right\}$$

then $\varphi(G^{(0)}) \leq \tilde{G}^{(0)}$ is trivial

also if $\varphi(G^{(i)}) \leq \tilde{G}^{(i)}$

then $G^{(i+1)} = [G^{(i)} : G^{(i)}]$

$$= \left\{ xyx^{-1}y^{-1} \,\middle|\, x, y \in G^{(i)} \right\}$$

is s.t $\varphi(G^{(i+1)}) = \left\{ \varphi(x)\varphi(y)\varphi(x^{-1})\varphi(y^{-1}) \,\middle|\, x, y \in G^{(i)} \right\}$

$$\leq \left\{ \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} \,\middle|\, \tilde{x}, \tilde{y} \in \tilde{G}^{(i)} \right\}$$

$$= \tilde{G}^{(i+1)}$$

so, by induction, $\forall n$, $\varphi(G^{(n)}) \leq \tilde{G}^{(n)}$

② now G is solvable $\Rightarrow \exists\, n$ s.t $G^{(n)} = (1)$

$$G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)}$$

then, $\varphi(G) = \tilde{G}$ is s.t

let $\varphi(G^{(i)}) = \tilde{G}^{(i)}$

then

$$G^{(n)} \trianglelefteq G^{(n-1)} \cdots \trianglelefteq G^{(0)}$$

$$\Rightarrow \varphi(G^{(n)}) \trianglelefteq \varphi(G^{(n-1)}) \cdots \trianglelefteq \tilde{G}^{(0)}$$

$$\Rightarrow \tilde{G}^{(n)} \trianglelefteq \cdots \trianglelefteq \tilde{G}^{(0)} \quad \text{so, } \tilde{G} \text{ is solvable}$$

$$\tilde{G}^{(n)} = (1)$$

③ given G is solvable and $H \leq G$

then $\exists\, n$ s.t $G^{(n)} = (1)$

$$G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(0)}$$

now $H \cap G^{(n)} \trianglelefteq H \cap G^{(n-1)} \trianglelefteq \cdots \trianglelefteq H \cap G^{(0)} = H$

$$\Rightarrow (1) \trianglelefteq H \cap G^{(n-1)} \trianglelefteq \cdots \trianglelefteq H$$

s.t $G^{(i+1)}/G^{(i)}$ is abelian

$\Rightarrow H \cap G^{(i+1)}/H \cap G^{(i)}$ is abelian

and so, $H_i = H \cap G^{(i)}$ s.t

$(1) \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_0 = H$

H_{i+1}/H_i abelian $\Rightarrow H$ is solvable

④ G is solvable and $N \trianglelefteq G$, then

$\varphi: G \to G/N$

then as $N \trianglelefteq G \Rightarrow \varphi$ is surjective homomorphism

$\Rightarrow \varphi(G) = G/N$ is solvable by ②

⑤ as $N, G/N$ is solvable

then $\exists\, n_1$ s.t $N^{(n_1)} \trianglelefteq N^{(n_1-1)} \cdots \trianglelefteq N^{(0)}$

$\exists\, n_2$ s.t $G/_N{}^{(n_2)} \trianglelefteq G/_N{}^{(n_2-1)} \cdots \trianglelefteq G/_N{}^{(0)}$

let $n = \max(n_1, n_2)$ then

$N^{(n)} \times G/_N{}^{(n)} \trianglelefteq N^{(n-1)} \times G/_N{}^{(n-1)} \cdots \trianglelefteq N^{(0)} \times G/_N{}^{(0)}$

$\Rightarrow N \times G/_N$ is solvable

then $\varphi: N \times G/_N \to G$

$(a, \bar{b}) \to a + \bar{b}$

is s.t $\varphi(N \times G/_N) = G$ and so by ②

G is solvable

⑥ generalising the result for $N, G/_N$ will imply $G_1 \times G_2$ solvable

Ex: show that $KpK = p^{-1}$ i.e $Kp = p^{-1}K$ or $Kp(\xi) = p^{-1}K(\xi)$

$Kp(i) = p^{-1}K(i)$

Ans: $K: \begin{matrix} \xi \to \xi \\ i \to -i \end{matrix}$ $p: \begin{matrix} \xi \to i\xi \\ i \to 1 \end{matrix}$

then $Kp: \begin{matrix} \xi \to -i\xi \\ i \to -i \end{matrix}$

$p^{-1}: \begin{matrix} \xi \to -i\xi \\ i \to i \end{matrix}$ $K: \begin{matrix} \xi \to \xi \\ i \to -i \end{matrix}$

$p^{-1}K: \begin{matrix} \xi \to -i\xi \\ i \to -i \end{matrix}$

so, $Kp = p^{-1}K$

7th April:

Defn: G is a group, G is solvable if $\exists$ finite series $(1) = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = G$ s.t H_{i+1}/H_i is abelian

Defn: derived/commutator series of G $G = G^{(0)} \trianglerighteq G^{(1)} = [G,G] \trianglerighteq G^{(2)} = [G^{(1)}, G^{(1)}]$

G is a group, then $[G,G] = G^{(1)}$ is normal subgroup of G

$\varphi_g : G \to G$, $x \mapsto gx^{-1}g$ conjugate automorphism

$[G,G] = \langle xyx^{-1}y^{-1} ;\ x,y \in G \rangle$ subgroup generated by all commutators

$\varphi_g(\langle [x,y] \rangle)$

$= \langle \varphi_g [x,y] \rangle$

$= \langle [\varphi_g(x), \varphi_g(y)] \rangle$

$\Rightarrow \varphi_g([G,G]) \subseteq [G,G]$
$\supseteq$ by $\varphi_{g^{-1}}$

so, $\varphi_g([G,G]) = [G,G] \Rightarrow [G,G]$ is normal

now, $G/_{[G,G]}$: abelian group

only when commutator is trivial

i.e $[\bar{g}, \bar{h}] = \bar{1}$

$\Rightarrow \overline{[g,h]} = \bar{1}$

but $[g,h] \in [G,G]$ so trivial

Theorem: G is solvable iff $G^{(m)} = (1)$ for some m

proof: ($\Leftarrow$) $G^{(0)} = G \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(m)} = (1)$

$G^{(0)} = H_m$, $G^{(1)} = H_{m-1}$, $G^{(m)} = H_0$

H_{i+1}/H_i = abelian $\Rightarrow$ G is solvable

($\Rightarrow$) given G is solvable, $H_0 = (1) \trianglelefteq H_1 \trianglelefteq H_2 \cdots \trianglelefteq H_m = G$
H_{i+1}/H_i abelian

if $G^{(i)} \le H_{m-i}$, then $G^{(m)} \le H_{m-m} = H_0 = (1)$

$\Rightarrow G^{(m)} = (1)$

now if $i=0$ then $G^{(0)} \le H_m = G$ but $G^{(0)} = G$

so true for $i=0$

assume, true for $i-1 > 0$, use induction on i

then $G^{(i-1)} \le H_{m-(i-1)} = H_{m+1-i}$ is true ($\because$ induction)

then $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \le [H_{m-i+1}, H_{m-i+1}]$

now, given H_{m-i+1}/H_{m-i} is abelian

$H \trianglelefteq G$, G/H abelian $\Rightarrow \left[\frac{G}{H}, \frac{G}{H}\right] = (\bar{1})$

$\left[\overline{G, G}\right] = (\bar{1})$ $\quad \left(\begin{array}{l} G \to G/H \text{ gp homomorphism} \\ g \mapsto \bar{g} \end{array}\right)$

$(\bar{1}) = \left[\overline{G, G}\right] \leq \frac{G}{H}$

$\Rightarrow [\bar{a}, \bar{a}] \leq H \quad (\because H \text{ is ker of } -)$

so, $[gH, \tilde{g}H] = [g, \tilde{g}]H$

so, $H \trianglelefteq G$, G/H abelian $\Rightarrow [G, G] \leq H$

now, $[H_{m-i+1}, H_{m-i+1}] \leq H_{m-i}$

$\Rightarrow G^{(i)} \leq H_{m-i}$ true for i

Eg: solvable groups

① abelian groups as $G^{(1)} = (1)$

② p-group G (i.e $|G| = p^n$)

G need not be abelian like

$Q_8 = \langle i, j \mid i^2 = -1, j^2 = 1, ij = -ji \rangle$

$|Q_8| = 2^3$ 2-group, not abelian

$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$

then $|G| = p^n$ G: solvable then centre of G

$Z(G) \neq (1) \Rightarrow (1) \trianglelefteq Z(G)$

$G \xrightarrow{\pi} G/Z(G)$

$\uparrow$ p group so it's centre non-trivial

$G \xrightarrow{\varphi} H$ surjective $\quad K \trianglelefteq H \Rightarrow \varphi^{-1}(K) \trianglelefteq G$

so, $Z\left(G/Z(G)\right) = \pi^{-1}\left(Z\left(G/Z(G)\right)\right) = H_2$

$H_2 \trianglelefteq G$ s.t $H_2 \not\trianglelefteq H_1$

so, $(1) \trianglelefteq Z(G) \not\trianglelefteq H_2 \cdots$ by induction done

$Z(G) = H_1$

and $Z(G)$ and $G/Z(G)$ p group of order $<|G|$ solvable by induction on $|G|$

↑ abelian

$\Rightarrow G$ is solvable ($\because$ prev corr)

Exe: If $|G|<60$, then G is solvable → done down

Eg: Non-solvable A_5 : Basic

$(1) \trianglelefteq A_5$

↑ No other normal subgroup

$A_5/(1)$ not abelian

$\Rightarrow A_5$ is not abelian

Theorem: (Wedderburn) If $|G| = p^a q^b$, p,q primes $a,b \in \mathbb{N}$ then G is solvable

Note: G is basic, non-abelian then not solvable

Theorem: (Feit-Thompson) $|G|$ = odd then G is solvable

So, $|G|<\infty$, G is basic, non-abelian then $|G|$ = even

Theorem: $G \overset{\varphi}{\twoheadrightarrow} \tilde{G}$ surjective group homorphism

(i) G is solvable $\Rightarrow$ any subgroup $H \leq G$ is solvable

(ii) G is solvable $\Rightarrow \tilde{G}$ solvable

(iii) $H \trianglelefteq G$, H and G/H are solvable $\Leftrightarrow G$ is solvable

proof: (i) $H^{(1)} \leq G^{(1)}$

$\vdots$

$H^{(m)} \leq G^{(m)} = (1)$

(ii) $\varphi(G^{(0)}) = \tilde{G}^{(0)}$

$\varphi(G^{(1)}) = \varphi([G,G]) = [\varphi(G), \varphi(G)] = [\tilde{G}, \tilde{G}] = \tilde{G}^{(1)}$

(iii) ($\Leftarrow$) is from (i), (ii)

($\Rightarrow$) $H^{(m)} = (1)$ ($\because H$ is solvable)

$\left(\frac{G}{H}\right)^{(n)} = (\bar{1})$ ($\because \frac{G}{H}$ is solvable)

$G \twoheadrightarrow G/H = \bar{G}$

$[G,G] \twoheadrightarrow \left[\frac{G}{H}, \frac{G}{H}\right] = [\overline{G,G}]$

So, $\left(\frac{G}{H}\right)^{(n)} = \overline{[G,G]^{(n)}} = (\bar{1})$

$\Rightarrow [G,G]^{(n)} + H = H \Rightarrow [G,G]^{(n)} \subseteq H$

$\Rightarrow ([G,G]^{(n)})^{(1)} \subseteq H^{(1)}$

$\vdots$

$\Rightarrow [G,G]^{(n+m)} \subseteq H^{(m)} = (\bar{1})$

$\Rightarrow [G,G]^{(n+m)} = (\bar{1})$

Defn: $f \in \mathbb{Q}[t]$ is solvable by radicals, if all the roots of f in $\mathbb{C}$ are radicals

Radicals are $\mathbb{Q} \subset \mathbb{Q}^{(1)} \subset \mathbb{Q}^{(2)} \dots$

$\mathbb{Q}^{(1)} = \mathbb{Q}(\sqrt[n]{r} ; r \in \mathbb{Q}, n \geq 1)$

$\mathbb{Q}^{(1)}$ gives $\mathbb{Q}^{(2)}$

$$R = \bigcup_{n=1}^{\infty} \mathbb{Q}^{(n)}$$

Note: Any group with basic subgroup, then not solvable

Eg: $\sqrt[5]{\sqrt[3]{\sqrt{2}+\sqrt{2}+3}} \in \mathbb{Q}^{(2)}$

$\sqrt{2} \in \mathbb{Q}^{(1)}$

$\sqrt[3]{\sqrt{2}+\sqrt{2}+3} \in \mathbb{Q}^{(3)}$

Any element of $\mathbb{Q}^{rad}$ is called radical

Theorem: $f \in K[t]$ is separable then f is solvable by radicals iff $Gal_K(f)$ is solvable

$\exists f \in \mathbb{Q}[t]$ s.t $Gal_{\mathbb{Q}}(f) = S_n$ $n \geq 5$, f is not solvable by radicals

but $|S_4| = 24 \Rightarrow S_4$ is solvable

suppose, $\deg f = p \leftarrow$ prime

↑ irreducible in $\mathbb{Q}[t]$

assume p has $p-2$ real roots (distinct)

f has precisely two non-real roots

$\Rightarrow \alpha_1, \alpha_2, \dots \alpha_p$: roots of f

$Gal_{\mathbb{Q}}(f)$ contains a p-cycle

$K : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$

$K \in Gal_{\mathbb{Q}}(f)$

$Gal_{\mathbb{Q}}(f) \ni (12)$ and $S_p = \langle (p\text{cycle}), \text{transposition} \rangle$

Exe: If $|G| < 60$, then G is solvable

Ans:

now $|G| < 60 \Rightarrow$ all groups are not basic

so, $\exists\, Z(G) \trianglelefteq G$ and $Z(G) \neq (1)$ or G

then by induction $Z(G)$, $G/Z(G)$ are solvable

$\Rightarrow G$ is solvable

10th April:

All fields are subfields of $\mathbb{C}/\mathbb{Q}$

Defn: $L|_K$ field extn, $L|_K$ is radical extension if

$L = K(\alpha_1, \alpha_2 \dots \alpha_n)$ $\quad \alpha_i^{n_i} \in K(\alpha_1 \dots \alpha_{i-1})$ $\quad n_i \in \mathbb{N}$

$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \dots \subset K(\alpha_1 \dots \alpha_n)$

$a_1 = \alpha_1^{n_1}$ $\quad a_2 = \alpha_2^{n_2}$ $\quad \dots$

$\alpha_1 = \sqrt[n_1]{a_1}$ $\quad \alpha_2 = \sqrt[n_2]{a_2}$ $\quad \dots$

$\alpha \in \mathbb{C}$ is a radical over K if $\exists$ a finite radical extn $M|_K$ and $\alpha \in M$

Eg: $e^{3/4}$ is a radical over $\mathbb{Q}(e)$

$\alpha = \sqrt[3]{\sqrt{2}+1} + \sqrt[2]{3}$ is a radical over $\mathbb{Q}$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[2]{3}) \subset \mathbb{Q}(\sqrt[3]{3}, \sqrt{2}) \subset \mathbb{Q}(\sqrt[2]{3}, \sqrt{2}, \sqrt[3]{\sqrt{2}+1})$

Defn: $f(t) \in K[t]$ is solvable by radicals if all roots of f in $\mathbb{C}$ are radicals
this is equivalent to

$Spl_K(f)$ is contained in a finite radical extn

as $Spl_K(f) = K(\alpha_1, \alpha_2 \dots \alpha_n)$ $\alpha_i \subset L_i$ radical extn of K then
$\alpha_1, \alpha_2 \dots \alpha_n \in L_1 L_2 \dots L_n \Rightarrow K(\alpha_1, \alpha_2, \dots \alpha_n) \subset L_1 L_2 \dots L_n$

composite of radical extn is radical as

$L_1 = K(\alpha_1, \alpha_2 \dots \alpha_n)$ $\quad \alpha_i^{n_i} \in K(\alpha_1, \dots \alpha_{i-1})$

$L_2 = K(\beta_1 \dots \beta_m)$ $\quad \beta_j^{m_j} \in K(\beta_1 \dots \beta_{j-1})$

$L_1 L_2 = K(\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_m)$

Theorem: $f \in K[t]$ is solvable by radicals over K, then $Gal_K(f)$ is solvable gp

Lemma: ① $Gal_K(t^n - 1)$ is abelian

② if $\zeta_n \in K$, then $Gal_K(t^n - a)$ is abelian

③ $Gal_K(t^n - a)$ is solvable

④ $L|_K$ is finite, Galois, radical extn then $Gal(L|_K)$ is solvable

⑤ $M|_K$ is radical extension, then normal closure of $M|_K$ is also radical

⑥ $L|_K$ is radical then $Gal(M|_K)$ is solvable $\quad L \subset M \subset K$

⑦ $f \in K[t]$ is solvable by radical $\Rightarrow Gal_K(f)$ is solvable

proof: ① $Spl_K(t^n - 1) = K(\zeta_n)$

now, $\sigma \in Gal_K(t^n - 1) = G$

$\sigma(\zeta) = \zeta^i$ ζ^i $i = 1, \dots n-1$ are roots of $t^n - 1$

$\tau \in G$, $\tau(\zeta) = \zeta^j$

$\sigma\tau(\zeta) = \tau\sigma(\zeta) = \zeta^{ij} \Rightarrow \sigma\tau = \tau\sigma$

$\Rightarrow G$: abelian

② roots of $t^n - a$ are $\alpha\zeta^i$ $i = 0, 1 \dots n$ α is one root of $t^n - a$

then $\sigma, \tau \in \mathrm{Gal}_K(t^n - a)$ $\mathrm{spl}_K(t^n - a) = K(\alpha)$

↑ automorphism of α

$\sigma(\alpha) = \alpha\zeta^i$ $i \in \{0, \dots n-1\}$

$\tau(\alpha) = \alpha\zeta^j$ $j \in \{0, \dots n-1\}$

$\Rightarrow \sigma\tau(\alpha) = \alpha\zeta^{ij} = \tau\sigma(\alpha)$

$\Rightarrow G$: abelian

③ $\mathrm{spl}_K(t^n - a) = K(\alpha, \zeta)$ α is a root of $t^n - a$

$K(\alpha, \zeta)$ — H abelian by ②

$K(\zeta)$

K — G abelian by ①

$H \trianglelefteq G$ as $K(\zeta)/K$ is galois $\left(\because \begin{matrix} M \\ | \\ L \\ | \\ K \end{matrix}\right)$ Gal_G L/K is gal iff $\mathrm{Gal}(M/L) \trianglelefteq G$

and $G/H \cong \mathrm{Gal}\left(\frac{K(\zeta)}{K}\right)$ abelian

$\Rightarrow G/H$ abelian, H is also abelian

$\Rightarrow G/H$ solvable, H is solvable

$\Rightarrow G$ is solvable

⑤ M/K radical, $M = K(\alpha_1 \dots \alpha_n)$ $\alpha_i^{n_i} \in K(\alpha_1 \dots \alpha_{i-1})$

normal closure of M/K is N/K $f_i = \min_K \alpha_i$ $N = \mathrm{spl}_K(\Pi f_i)$

$= L_1 L_2 \dots L_n$

$L_i = \mathrm{spl}_K f_i$

N/K is finite galois extension

β is root of f_1, β is conjugate to α_1

$\exists \sigma \in \mathrm{Gal}_K(f_1)$ s.t. $\sigma(\alpha_1) = \beta$

$\mathrm{spl}(\Pi f_i)$ ↺ — this extension is always possible

$\mathrm{spl}(f_1)$ ↺ σ

K — normal

normal

$N \circlearrowright \sigma(\alpha_1) = \beta$

$|$

$M = K(\alpha_1 \dots \alpha_n)$ β, α_1 are conjugates over K

$M = K(\alpha_1, \dots \alpha_n)$

$\sigma M = K(\sigma\alpha_1, \dots \sigma\alpha_n)$

$\sigma(\alpha_i^{n_i}) = \sigma(\alpha_i)^{n_i} \in K(\sigma\alpha_1 \dots \sigma\alpha_n)$

so, σM is a radical extension

$N = \prod_{\sigma \in Gal(M|K)} \sigma M$ and, σM is radical ext^n $/K \Rightarrow N/K$ is radical extension

④ $\left.\begin{array}{l} L \\ | \\ K \end{array}\right)$ finite, galois, radical

then $L = K(\alpha_1, \alpha_2 \dots \alpha_n)$

$\alpha_i^{n_i} \in K(\alpha_1 \dots \alpha_{i-1})$

$M \subset M(\alpha)$, $\alpha^n \in M$

$n = p_1 \cdots p_\gamma$ p_i: prime

$M \subset M(\alpha_1) \subset M(\alpha_1, \alpha_2)$

$\alpha^{p_2 \cdots p_n}$ $\quad$ $\alpha^{p_3 \cdots p_n}$

$\alpha_1^{p_1} = \alpha^n \in M$, $\alpha_2^{p_2} \in M(\alpha_1)$

so, we may assume n prime then induction on n:

$n = 0$: trivial $G = (1)$ so, solvable

$n \neq 1$: (1) $\quad$ $K(\alpha_1 \dots \alpha_n) = L$

solvable H $\longleftarrow$ $Gal(L|_)$ $\quad$ $K(\alpha_1)$ $\quad$ $\alpha_1^p \in K$ $\quad$ $n_1 = p$ (wlog $n_1 = p$)

by induction G $\quad$ K $\quad$ $\min_K \alpha_1 \mid t^p - \alpha_1^p \in K[t]$

$\Rightarrow \xi \in L$

$(1) \subset H \subset G$

solvable

Replace K by $K(\xi)$ ie $K(\alpha_1 \dots \alpha_n)(\xi)$

(1) $\quad$ $Gal(L|_)$ $\quad$ $|$ $\quad$ H

H $\longleftarrow$ $K(\alpha_1)(\xi)$ $\quad$ H_1

$|$

abelian $K(\xi)$ $\quad$ G

abelian K

solvable by induction Hypothesis

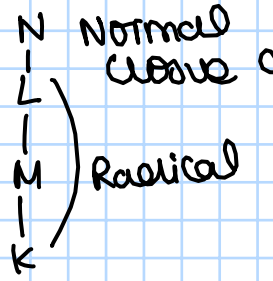
by induction $H \trianglerighteq K_2 \trianglerighteq \cdots$ (1)

$H_1 \trianglerighteq H$ ($\because H_1/H$ is abelian, ②)

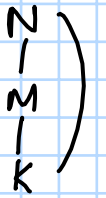
$G \trianglerighteq H_1$ ($\because G/H_1$ is abelian, ①)

$\Rightarrow G$ is solvable

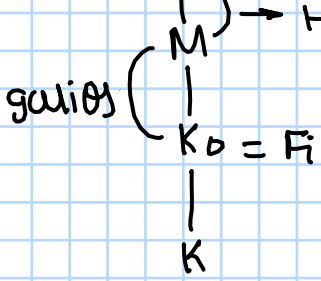
⑥



$\Rightarrow$



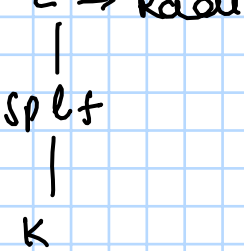
$\Rightarrow Gal(N|K)$ is solvable ($\because$ ④)



and $Gal(M|_{K_0}) = Gal(M|_K)$

$\dfrac{Gal(N|M)}{H} = Gal(M|_{K_0}) = Gal(M|_K)$

① $f \in K[t]$ is solvable by radicals



$\Rightarrow Gal_K(splf)$ solvable ($\because$ ⑥)

THEOREM: $f \in \mathbb{Q}[t]$, deg p: prime, f: irred $\exists$ only two non-real roots of f then $Gal_{\mathbb{Q}}(f) \cong S_p$

proof: $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$ α root of f

$\Rightarrow p \mid [splf_{\mathbb{Q}} : \mathbb{Q}] = |G|$

also $G \leq S_p$ ($\because G$ acts on roots of f) and $p \mid |G| \Rightarrow \exists$ p-cycle $\sigma \in G$

$K: \mathbb{C} \to \mathbb{C}$ $\quad z \to \bar{z}$ $\quad o(K)=2$, $K \in G$ $\quad (1\,2)$ as $\alpha_1, \bar{\alpha}_1, \alpha_3, \ldots \alpha_{p-1}$

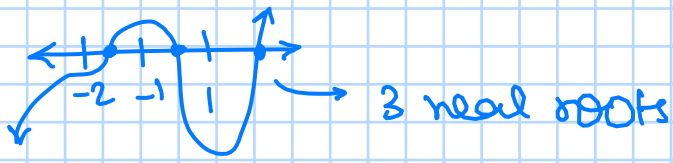
$\tau = (1\,2)$ $\qquad\qquad \bar{\alpha}_1 = \alpha_2$

Exe: Show that $\langle p\text{-cycle}, (12) \rangle = S_p$ → done above

Eg: $f(t) = t^5 - 6t + 3$, f: irred (Eisenstein)

$f' = 5t^4 - 6$ → separable

f' has 2 real roots



Exe: Show that $\langle p\text{-cycle}, (12) \rangle = S_p$

Ans:

$c = (0, 1, 2 \ldots (p-1))$

$t = (0, a)$

$(0, a)$, $(a, 2a)$, ... in G

$\exists b$ s.t $ab = 1 \Rightarrow (0, a), \ldots ((b-1)a, 1)$

$\Rightarrow (0, a), (0, 2a), \ldots (0, 1)$ can be generated as $(0, a)(a, 2a)(0, a) = (0, 2a)$

now, c, $(0, 1)$ are standard generators, so we are done

17th April:

Theorem: $M|_K$ finite extension, then $M = K(\alpha)$ is a basic extension iff $\exists$ only finitely many subfields of $M|_K$

Corr: $M|_K$ separable extension (finite degree) then $M = K(\alpha)$

proof: $M|_K$ separable $\Rightarrow$ N = Normal closure of M over K

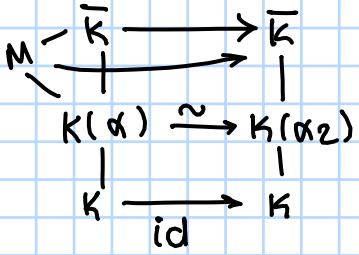
N = composite of M

$= \prod_\sigma M$

σ: isomorphisms $M \to \bar{K}$

$L|_K$ Galois $\Rightarrow$ {subgroups of $Gal(L|K)$} $\leftrightarrow$ {subfields of $L|K$}

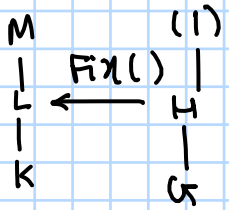
$\alpha \in M$, K $\quad \min_K \alpha = f(x)$, $\alpha_1, \dots \alpha_n$: roots of f



Idea is that if K finite $\Rightarrow$ M finite $\Rightarrow M^\times = \langle \alpha \rangle$
$\Rightarrow M = K(\alpha)$

K infinite, M finite over K $\Rightarrow M = K(\alpha_1 \dots \alpha_n)$
$= K(\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n)$ for some $c_i \in K$
(Not fixed by any element)

Corr: $M|_K$ Galois, K infinite then $M = K(\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n)$ $\beta = \alpha_1 + \dots c_n\alpha_n$
iff ($\sigma(\beta) = \beta$ for $\sigma \in Gal(M|K)$ iff $\sigma = id$)



Eg: $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$

$\sigma: \sqrt{2} \to \pm\sqrt{2}$
$\sqrt{3} \to \pm\sqrt{3}$
$\vdots$

$\sqrt{2} + \sqrt{3} + \sqrt{5}$ is fixed by id only so, $\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})/\mathbb{Q}$
$= \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$

$M = \mathbb{Q}(x_1, x_2, \dots x_n)$ $\quad S_n \subset Aut(M/\mathbb{Q})$ $\quad \sigma(x_i) = x_{\sigma(i)}$
σ

$$Fix(S_n) = \mathbb{Q}(s_1, \ldots s_n)$$
$$s_1 = \sum x_i$$
$$s_2 = \sum_{i<j} x_i x_j$$
$$\vdots$$
$$s_n = x_1 \ldots x_n$$

S_n acts on $\mathbb{Q}[x_1 \ldots x_n]$

$$Fix(S_n) = \mathbb{Q}[s_1 \ldots s_n]$$

Eg: $x_1^2 + x_2^2 + x_3^2 = f \in Fix(S_3)$ ↑ as invariant under $\sigma \in S_3$

Also, $f \in \mathbb{Q}(s_1, s_2, s_3)$

lexicographic ordering on $\mathbb{N}_{\neq 0}$ $(a_1, a_2, a_3) > (b_1, b_2, b_3)$

if $a_i = b_i$ $i = 1, \ldots j$ Also, $(1,2) > (0,100)$

$a_{j+1} > b_{j+1}$

given f: symmetric polynomial, if $x_1^{a_1} \ldots x_n^{a_n}$ occurs in f

$x_1^{\sigma(a_1)}, \ldots x_n^{\sigma(a_n)}$ occurs in f $\forall \sigma \in S_n$

we may assume $(a_1 \ldots a_n) > (\sigma(a_1), \ldots \sigma(a_n))$ $\forall \sigma \in S_n \setminus (id)$

$x_1^2 + x_2^2 + x_3^2$ — $(0,2,0)$, $(2,0,0)$, $(0,0,2)$

f - coeff of $(x_1^{a_1} \ldots x_n^{a_n})\, s_1^{a_1 - a_2} s_2^{a_2 - a_3} \ldots s_n^{a_n}$

this was lexicographic order smaller than f

$$x_1^2 + x_2^2 + x_3^2 - 1 \cdot s_1^{2-0} s_2^{0-0} s_3^0$$
$$= x_1^2 + x_2^2 + x_3^2 - (x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3)$$
$$f = s_1^2 - 2s_2$$

Eg: $f = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_3 + x_2^2 x_1 + x_3^2 x_1 + x_3^2 x_2$

largest degree: $(2,1,0)$

$f - s_1 s_2 \rightarrow$ Reduce the degree and then repeat algorithm

$$f - s_1 s_2 = -3x_1x_2x_3$$
$$f = s_1 s_2 - 3s_3$$

Eg: $\mathbb{Q}(\zeta_p) / \mathbb{Q}$ $\{1, \zeta, \ldots \zeta^{p-1}\}$ basis

$Hom(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$

$Fix(H) = \mathbb{Q}\left(\sum_{\sigma \in H} \sigma\xi\right)$

$K(\alpha)$ / K galois extension $\Rightarrow$ normal basis $= \{\sigma\alpha ;\ \sigma \in Hom(K(\alpha)/K)\}$

now, $\mathbb{F}_3[X]$ deg 1 - 3
deg 2 - reducible l_i^2, $l_i l_j$
$\uparrow 3 + \uparrow 3 = 6$
irreducible $= 9 - 6 = 3$

$x^2 + x + 2 \rightarrow$ irreducible

$x^2 + 2x + 2$

$x^2 + 1$

$\frac{\mathbb{F}_3[x]}{\langle x^2+x+2\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle}$ we want to find an isomorphism

$\uparrow$

$\mathbb{F}_3[x] \longrightarrow \mathbb{F}_3[x]$

$x \longmapsto ax + b$

if deg 3 then we look at deg 2 polynomial

$\alpha(x)^2 + 1 = 0$ ← $x^2 + x + 2 = 0$

$(ax+b)^2 + 1 = 0$

$a^2x^2 + b^2 + 2abx + 1 = 0$

$a^2(-x-2) + b^2 + 2ab\,x + 1 = 0$

$-2a^2 + b^2 + 1 = 0$

$-a^2 + 2ab = 0 \quad (a \neq 0)$

$-a + 2b = 0$

$\Rightarrow 2b = a$

$b=1$ $a=2$ / $b=2$ $a=1$ work

$x \to 2x+1$ } Both isomorphisms
$x \to x+2$ }

Eg: deg 3 over $\mathbb{F}_3[x]$ irred

$\frac{\mathbb{F}_3[x]}{\langle x^3-x+1\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^3+2x^2+1\rangle}$ $\quad x \longrightarrow \alpha(x) = ax^2 + bx + c$ s.t when $x^3 - x + 1 = 0$

we want $\underbrace{\alpha(x)^3 + 2\alpha(x)^2 + 1 = 0}_{\text{as char} = 3}$

$\Rightarrow ax^6 + bx^3 + c + 2(ax^2 + bx + c)^2 + 1 = 0$

$\Rightarrow ax^6 + bx^3 + c + 2(a^2x^4 + b^2x^2 + c^2 + 2abx^3 + 2bcx + 2ac(x^2)) + 1 = 0$

Algebraically closed fields:

$\mathbb{C}$, $\mathbb{R}^{alg} = \{$algebraic complex numbers$\}$

$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$!

Field of puiseux series $\mathbb{C}((x^{1/n})) = \left\{ \sum_{\substack{i \geq k \\ k \in \mathbb{Z}}} c_i x^{i/n} \right\}$ ← least exponent in $x^{1/n}$

$\bigcup_{n \geq 1} \mathbb{C}((x^{1/n}))$: algebraically closed field

$\mathbb{C}(X)$ ⊂ $\mathbb{C}(X)^{alg}$ = alg closure of $\mathbb{C}(X)$

$1 < [F : F] < \infty \Rightarrow$
1. $char(F) = 0$
2. $[E : F] = 2$
3. $F = F(\sqrt{-1})$
4. F is ordered