MA 414 - Tutorials

Tutorial-1 :

1. $x^3+px+q=(x-x_1)(x-x_2)(x-x_3)$

$x_1+x_2+x_3=0 \quad x_1x_2+x_2x_3+x_3x_1=p \quad x_1x_2x_3=-q$

$\Delta=\prod_{i<j}(x_i-x_j)^2=[(x_1-x_2)(x_2-x_3)(x_1-x_3)]^2$

a) $\Delta=-(4p^3+27q^2)$

b) cubic has rep roots iff $\Delta=0$

c) $f(x)=x^3+px+q\in\mathbb{R}[x]$ then
f has 3 distinct roots
iff $\Delta>0$

d) f has only one real iff $\Delta<0$

if $x_i=0$ wlog $i=3$ then $x_1x_2=p \quad q=0 \quad \Delta=(x_1-x_2)^2(x_1)^2(x_2)^2$
$=\left[(x_1+x_2)^2-4x_1x_2\right]p^2$
$=-4p3=-4p3-27q^2$

so let $x_i\neq 0:2$

$(x_1-x_2)=(x_1+x_2)^2-4x_1x_2$

$=x_3^2+\frac{4q}{x_3} \qquad x_1x_2+x_3(-x_3)=p$

$-x_3^2=p-x_1x_2$

$=\frac{x_3^3+4q}{x_3} \qquad -x_3^3=px_3-x_1x_2x_3=px_3+q$

$=\frac{-px_3-q+4q}{x_3}$

$=\frac{3q-px_3}{x_3}$

$=\frac{-p\left[x_3-\frac{3q}{p}\right]}{x_3}$

then
$\Delta=\frac{-p3}{\pi x_i}\prod(x_i-3\frac{q}{p})$ as $x_i\neq 0\ \forall i$

now $\lambda=\frac{3q}{p}$ then $\lambda^3+p\lambda+q=(\lambda-x_1)(\lambda-x_2)(\lambda-x_3)$

$=-\pi(x_i-\lambda)$

$\Rightarrow \Delta=p^3(\lambda^3+p\lambda+q)$

$=-\frac{p3}{q}\left[27\frac{q^3}{p3}+3p\frac{q}{q}+q\right]$

$=-p^3\left[\frac{27q^2}{p3}+4\right]$

$=-\left[4p^3+27q^2\right]$

now, if $x_i=x_j$ for some $i\neq j$ (i.e repeated roots)
then wlog $i<j$
$x_i-x_j=0 \Rightarrow \Delta=\prod_{i<j}(x_i-x_j)^2=0$

also if $\Delta=0$ then
$x_1-x_2=0$ or $x_2-x_3=0$ or $x_1-x_3=0$

$\Rightarrow \exists$ repeated root

if f has 3 distinct real roots then

$x_1 - x_2 \neq 0,\ x_2 - x_3 \neq 0,\ x_1 - x_3 \neq 0 \quad \in \mathbb{R}$

$\Rightarrow (x_1-x_2)^2 > 0, (x_2-x_3)^2 > 0, (x_1-x_3)^2 > 0$

$\Rightarrow \Delta > 0$

also if $\Delta > 0$ then $(x_1-x_2) \neq 0,\ (x_2-x_3) \neq 0,\ (x_1-x_3) \neq 0$

$\Rightarrow x_1 \neq x_2 \neq x_3$

$\Rightarrow f$ has 3 distinct roots

now if f has only one real root then

$x_2 = x + iy$ be a complex root $\quad y \neq 0 \in \mathbb{R}$

then other must be

$x_3 = x - iy$

$\Rightarrow (x_2-x_3)^2 = (2iy)^2 = -4y^2 < 0$ as $y^2 > 0$

($\because f \in \mathbb{R}[x]$ and complex conjugate theorem)2

if $\Delta < 0$ then $\exists (i,j)$ pair s.t $(x_i - x_j)^2 < 0$ as $\Delta < 0$ for $i < j$

$\Rightarrow x_i - x_j = iy$ for some $y \neq 0$

$\Rightarrow x_i, x_j$ are complex conjugate roots

if all three terms of Δ is < 0 then all 3 are complex conjugate of each other and unique, this is not possible,

so one real and 2 complex roots

($\because f \in \mathbb{R}[x]$ and complex conjugate theorm)

2. $x^3 - 6x + 9 = 0$

now already

$-27 + 18 + 9 = 0$

$\Rightarrow x = -3$ is a root

$(x^3 + 3x^2) - 3x^2 - 9x + 3x + 9 = 0$

$\Rightarrow x^2(x+3) - 3x(x+3) + 3(x+3) = 0$

$\Rightarrow (x^2 - 3x + 3)(x+3) = 0$

so $x = -3$ is a double

and

$x = \frac{3 \pm \sqrt{9-12}}{2}$

$= \frac{3 \pm \sqrt{3}i}{2}$ ↪ other 2 roots

now, $x^3 - 6x + 9 = 0$

let $x = T + U$

then $x^3 = T^3 + U^3 + 3TU(T+U)$

$\Rightarrow T^3 + U^3 + 3TU(T+U) - 6T - 6U + 9 = 0$

$\Rightarrow (T^3 + U^3 + 9) + (T+U)(3TU - 6) = 0$

then $(T^3+U^3+9)+x(3TU-6)=0$

$\Rightarrow T^3+U^3=-9$ —— ①

$3TU=6$

$TU=2$

$\Rightarrow T^3U^3=8$ —— ②

from ①, ② $z^2+9z+8=0$ has roots T^3, U^3 ($\because$ sum and product)

$$\Rightarrow z=\frac{-9\pm\sqrt{81-32}}{2}$$

$$=\frac{-9\pm\sqrt{49}}{2}$$

$$=\frac{-9\pm7}{2}$$

$$=-1,-8$$

so, $T^3, U^3=-1,-8$

then $T, U=-\omega^i, -2\omega^j$ $\quad 0\le i, j\le 2$

where $x=T+U$ as T, U also satisfy ② we need $(i,j)=(0,0),(1,2)$ or $(2,1)$

$\Rightarrow x_1=-1-2=-3$

$x_2=-\omega-2\omega^2$ $\qquad \omega=\frac{-1+i\sqrt{3}}{2}$

$x_3=-\omega^2-2\omega$ $\qquad \omega^2=\frac{-1-i\sqrt{3}}{2}$

$$\Rightarrow x_2=-\left(\frac{-1+i\sqrt{3}}{2}\right)-2\left(\frac{-1-i\sqrt{3}}{2}\right)$$

$$=\frac{1-i\sqrt{3}}{2}+\frac{2+2i\sqrt{3}}{2}$$

$$=\frac{3+i\sqrt{3}}{2}$$

similarly $x_3=-\omega^2-2\omega=-\left(\frac{-1-i\sqrt{3}}{2}\right)-2\left(\frac{-1+i\sqrt{3}}{2}\right)$

$$=\frac{1+i\sqrt{3}}{2}+\frac{2-2i\sqrt{3}}{2}$$

$$=\frac{3-i\sqrt{3}}{2}$$

3. $x^3-6x+4=0$, $x^3+px+q=0$

$\Delta=-(4p^3+27q^2)$

$=-(4(-6)^3+27(4)^2)=432>0$

as $x^3-6x+4\in\mathbb{R}[x]$ from above we will have 3 distinct solution

now, $x^3-6x+4=0$

$8-12+4=0\Rightarrow x=2$ is a root

now, $x^3-2x^2+2x^2-4x-2x+4=0$

$\Rightarrow x^2(x-2)+2x(x-2)-2(x-2)=0$

$\Rightarrow x=2,\ x^2+2x-2=0$

$$x=\frac{-2\pm\sqrt{4+8}}{2}$$

$$=-\frac{x\pm 2\sqrt{3}}{2}$$

$$x_2, x_3 = -1\pm\sqrt{3}$$

now as $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3<0$

$$T=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

$$U=\sqrt[3]{\frac{-q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

$$x_1=T+U,\quad x_2=T\omega+U\omega^2,\quad x_3=T\omega^2+U\omega$$

now, $x_2+x_3=-2$ from our original argumet

and $x_1=2$, so $x_1=T+U$

as $x_2+x_3=T(\omega+\omega^2)+U(\omega^2+\omega)$

$=-T-U=-(T+U)=-x_1$

$=-2$

so, $2=\sqrt[3]{-2+2i}+\sqrt[3]{-2-2i}$

4. To prove: $z\in\mathbb{Q}$ is not conjugate to any $z'\in\mathbb{C}$ if $z\neq z'$ over $\mathbb{Q}$

proof: let $z'=x+iy\in\mathbb{C}$

then $f(t)=t-z\in\mathbb{Q}[t]$

s.t

$f(z)=0$ but

$f(z')=z'-z\neq 0$

$\Rightarrow \exists\ f\in\mathbb{Q}[t]$ s.t

$f(z)=0$ but $f(z')\neq 0$

$\Rightarrow z, z'$ not conjugate over $\mathbb{Q}$

5.(a) To prove: if k-tuples of complex numbers $(z_1, z_2, \ldots z_k)$ and $(z_1', \ldots z_k')$ are conjugate over $\mathbb{Q}$ then z_i, z_i' are conjugate over $\mathbb{Q}$ for $i=1,2..k$

proof:

let $f\in\mathbb{Q}[t]$ s.t $f(z_i)=0$, then now let

$$f(t_1,t_2,\ldots t_k)=f(t_i)\in\mathbb{Q}[t_1,t_2,\ldots t_k]$$

then

$f(z_1,z_2,\ldots z_k)=f(z_i)=0$ ($\because$ defination of conjugates)

$\Rightarrow f(z_1', z_2', \ldots z_k')=0 \Rightarrow f(z_i')=0$

$\Rightarrow f(z_i')=0\ \forall\ f\in\mathbb{Q}[t]$

so, (z_i, z_i') are conjugate over $\mathbb{Q}$

this is for $i=1,2\ldots k$

(b) To prove: $(z_1, z_2, \ldots z_k)$ and $(\bar{z}_1, \bar{z}_2, \ldots \bar{z}_k)$ are conjugate over $\mathbb{Q}$

proof: for $f(t_1, t_2, \ldots t_k) \in \mathbb{Q}[t_1, t_2, \ldots t_k]$

we have

$\overline{\omega_1 + \omega_2} = \overline{\omega_1} + \overline{\omega_2}$

$\overline{\omega_1 \omega_2} = \overline{\omega_1} \cdot \overline{\omega_2}$

so, by induction $\overline{\omega_1 + \omega_2 + \cdots + \omega_k} = \overline{\omega_1} + \cdots + \overline{\omega_k}$

$\overline{\omega_1 \cdot \omega_2 \cdots \omega_k} = \overline{\omega_1} \cdot \overline{\omega_2} \cdots \overline{\omega_k}$

and $a = \bar{a}$ if $a \in \mathbb{Q}$

so, if $f(t_1, t_2, \ldots t_k) = \sum_{i=1}^{k} \sum_{j=1}^{n_j} a_{i,j} t_i^j + c$

$a_{i,j}$ and $c \in \mathbb{Q}$

then $\overline{f(t_1, t_2, \ldots t_k)} = \sum_{i=1}^{k} \sum_{j=1}^{n_j} \bar{a}_{i,j} (\bar{t}_i)^j + c$

$= f(\bar{t}_1, \ldots \bar{t}_k)$

now if $f(z_1, z_2, \ldots z_k) = 0$

then $\overline{f(z_1, \ldots z_k)} = f(\bar{z}_1, \ldots \bar{z}_k) = 0$

$\Rightarrow \forall f \in \mathbb{Q}[t_1, t_2, \ldots t_k]$

$f(z_1, z_2, \ldots z_k) = 0$ iff $f(\bar{z}_1, \ldots \bar{z}_k) = 0$

so $(z_1, z_2, \ldots z_k)$ and $(\bar{z}_1, \ldots \bar{z}_k)$ conjugates over $\mathbb{Q}$

6. To prove: for $f \in \mathbb{Q}[t]$, $\mathrm{gal}(f|\mathbb{Q})$ is a subgroup of S_k where $\alpha_1, \ldots \alpha_k$ are distinct roots of f in $\mathbb{C}$

$\mathrm{gal}(f|\mathbb{Q}) = \{\sigma \in S_k \mid (\alpha_1, \alpha_2, \ldots \alpha_k)$ and $(\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(k)})$ are conjugate over $\mathbb{Q}\}$

proof: now $\mathrm{id} \in \mathrm{gal}(f|\mathbb{Q})$ is trivial as $(\alpha_1, \alpha_2, \ldots \alpha_k)$ and $(\alpha_1, \alpha_2, \ldots \alpha_k)$ are conjugates over $\mathbb{Q}$ — (1)

now, for $\sigma_1, \sigma_2 \in \mathrm{gal}(f|\mathbb{Q})$

let $f(t_1, t_2, \ldots t_k) \in \mathbb{Q}[t_1, t_2, \ldots t_k]$

then $\exists f'(t_1, t_2, \ldots t_k) \in \mathbb{Q}[t_1, t_2, \ldots t_k]$ s.t

$f'(t_1, t_2, \ldots t_k) = f(t_{\sigma_1(1)}, \ldots t_{\sigma_1(k)})$

($\because$ swapping variables)

now $f(\alpha_1, \alpha_2 \ldots \alpha_k) = 0$

$\Leftrightarrow f(\alpha_{\sigma_1(1)}, \ldots \alpha_{\sigma_1(k)}) = 0$

$\Leftrightarrow f'(\alpha_1, \alpha_2, \ldots \alpha_k) = 0$

$\Leftrightarrow f'(\alpha_{\sigma_2(1)}, \ldots \alpha_{\sigma_2(k)}) = 0$

$\Leftrightarrow f(\alpha_{\sigma_1 \cdot \sigma_2(1)}, \ldots \alpha_{\sigma_1 \cdot \sigma_2(k)}) = 0$

So, $\forall f \in \mathbb{Q}[t_1, t_2, \ldots t_k]$

$f(\alpha_1, \ldots \alpha_k) = 0 \Leftrightarrow f(\alpha_{\sigma_1 \cdot \sigma_2(1)}, \ldots \alpha_{\sigma_1 \cdot \sigma_2(k)}) = 0$

$\Rightarrow \sigma_1 \circ \sigma_2 \in gal(f|\mathbb{Q})$ — ②

Now, for $\sigma \in gal(f|\mathbb{Q})$

for $f(t_1, t_2 \ldots t_k) \in \mathbb{Q}[t_1, t_2, \ldots t_k]$

$\exists$ s.t $f'(t_1, t_2, \ldots t_k) \in \mathbb{Q}[t_1 \ldots t_k]$

$f'(t_1, t_2, \ldots t_k) = f(t_{\sigma^{-1}(1)}, \ldots t_{\sigma^{-1}(k)})$

($\because$ swapping variables)

Now,

$f(\alpha_1, \alpha_2 \ldots \alpha_k) = 0$

$\Leftrightarrow f'(\alpha_{\sigma(1)}, \ldots \alpha_{\sigma(k)}) = 0$ ($\because f'(\alpha_{\sigma(1)} \ldots \alpha_{\sigma(k)}) = f(\alpha_1, \ldots \alpha_k)$)

$\Leftrightarrow f'(\alpha_1, \alpha_2 \ldots \alpha_k) = 0$

$\Leftrightarrow f(\alpha_{\sigma^{-1}(1)}, \ldots \alpha_{\sigma^{-1}(k)}) = 0$

So, $\forall f \in \mathbb{Q}[t_1 \ldots t_k]$, $f(\alpha_1, \ldots \alpha_k) = 0$ iff $f(\alpha_{\sigma^{-1}(1)} \ldots \alpha_{\sigma^{-1}(k)}) = 0$

$\Rightarrow \sigma^{-1} \in gal(f|\mathbb{Q})$ — ③

from ①, ②, ③ $gal(f|\mathbb{Q})$ is a subgroup of S_k

Tutorial-2 :

1. $\varphi_i : K \to L$ $\quad i \in I$ $\quad K, L$ fields
   ↑ field homomorphism

$$E = \{x \in K \mid \varphi_i(x) = \varphi_j(x) \ \forall i,j\}$$

To prove: E is subfield of K

proof: as $\varphi_i(1_K) = 1_L = \varphi_j(1_K) \ \forall i,j$

$\Rightarrow 1_K \in E$ — ①

for $x, y \in E$, $\phi_i(x-y) = \phi_i(x) - \phi_i(y)$

$= \phi_j(x) - \phi_j(y)$

$= \phi_j(x-y)$

$\forall i, j$

$\Rightarrow x - y \in E$ — ②

now, $\phi_i(xy^{-1}) = \phi_i(x)\,\phi_i(y^{-1}) = (\phi_i(x))(\phi_i(y))^{-1}$

$= (\phi_j(x))(\phi_j(y))^{-1}$

$= \phi_j(xy^{-1}) \ \forall i,j$

$\Rightarrow xy^{-1} \in E$ — ③

from ①, ②, ③ E is a subfield of K

2. $id, K : \mathbb{C} \to \mathbb{C}$ homorphism

$K(z) = \bar{z}$
$id(z) = z$

now, $Eq(\{id, x\}) = \{z \in \mathbb{C} \mid id(z) = K(z)\}$

$= \{z \in \mathbb{C} \mid z = \bar{z}\}$

$= \{z \in \mathbb{C} \mid z \in \mathbb{R}\}$

$= \{z \in \mathbb{R}\}$

$= \mathbb{R}$

3. R is ID

To prove: $char(R) = 0$ or p for p a prime number

proof:

$char(R) = 0$ or n

if $char(R) = n \neq 0$ then $n \in \mathbb{N}$

let $n = ab \quad 1 < a, b < n$

then from definition of $char(R)$

as $\varphi : \mathbb{Z} \to R$

$1 \mapsto 1_R$

$2 \mapsto 2_R$

$ker(\varphi) = n.\mathbb{Z} \Rightarrow n.1_R = 0 \Rightarrow ab.1_R = 0$

$\Rightarrow (a.1_R)(b.1_R) = 0$

$\Rightarrow a.1_R = 0$ or $b.1_R = 0$

but then $char(R) = a$ or b

$< n$

↑ smallest such

this is a contradiction, so, $n \in \mathbb{N}$ s.t
$\nexists a, b \quad 1<a,b<n$
$n = a.b$
$\Rightarrow n$ is prime

4. R is finite ID $\Rightarrow$ char(R) = 0 or p (from before)
now, if char(R) = 0 then

$$\varphi : \mathbb{Z} \longrightarrow R$$
$$1 \longmapsto 1_R$$

then as $char(R)=0 \Rightarrow ker(\varphi) = \{0\}$
or φ is one-one
then n
$\sum_{i=1} 1_R = n.1_R$ be s.t $\varphi(n) = n.1_R$
as all $\varphi(i)$ differ
(1_R) has infinite elements
$\Rightarrow R$ has infinite elements
this is a contradiction, so
$char(R) \neq 0$
$\Rightarrow char(R) = p$ for some prime p

now, let $a \neq 0$, $\varphi_a : R \longrightarrow R$
$x \longmapsto ax$
then $\varphi_a(x) = \varphi_a(y)$
$\Rightarrow ax = ay$
$\Rightarrow a(x-y) = 0$
$\Rightarrow x - y = 0$ ($\because a \neq 0$ and R is ID)
$\Rightarrow x = y$
so, φ_a is one-one
also as R is finite $\Rightarrow \varphi_a$ is surjective ($\because$ trivial)
now for $1 \in R \; \exists \, x \in R$ s.t $\varphi_a(x) = 1$
$\Rightarrow ax = 1$
$\Rightarrow x = a^{-1}$
so, $\forall a \neq 0$, $\exists$ inverse of a
$\Rightarrow R$ is a field

as $char(R) = p$

$$\varphi : \mathbb{Z} \longrightarrow R$$
$$1 \longmapsto 1_R \qquad ker(\varphi) = p\mathbb{Z}$$

$$\mathbb{Z}/ker(\varphi) \cong img(\varphi)$$
$$\Rightarrow \mathbb{Z}/p\mathbb{Z} \cong img(\varphi)$$

$\exists$ copy K of $\mathbb{Z}/p\mathbb{Z}$ in R

then K is a subfield of R ($\because K \cong \mathbb{Z}/p\mathbb{Z}$)
$\forall a, b \in K$, $\forall x, y \in R$, $ax + by \in R$
$\Rightarrow R$ is a v.s over K
since R is finite, $dim(R) = n$
then let $\{v_1, v_2, \ldots v_n\} \subseteq R$ be basis of R
$\sum_{i=1}^{n} c_i v_i$, $c_i \in K$ spans entire space R

$\Rightarrow |R| = p^n$ as $|K| = p$

5. 9 element, 25 element, 27 element

$x^2+1=0$ is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$

as $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

$(\bar{0})^2+\bar{1} = \bar{1} \neq 0$

$(\bar{1})^2+\bar{1} = \bar{2} \neq 0$

$(\bar{2})^2+\bar{1} = \bar{1}+\bar{1} = \bar{2} \neq 0$

$x^2+1=0$ has no roots in $\mathbb{Z}/3\mathbb{Z}$ ($\because$ deg ≤ 3)

$\Rightarrow x^2+1$ irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$

$\Rightarrow \langle x^2+1 \rangle$ is maximal

$\Rightarrow \frac{\mathbb{Z}/3\mathbb{Z}[x]}{\langle x^2+1 \rangle}$ is field ($\because \langle x^2+1 \rangle$ maximal iff $\mathbb{Z}/3\mathbb{Z}[x]$ field) as $\mathbb{Z}/3\mathbb{Z}[x]$ is PID ($\because \mathbb{Z}/3\mathbb{Z}$ PID)

now, $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{\langle x^2+1 \rangle} = \{a+bx+\langle x^2+1 \rangle\}$

$a, b \in \mathbb{Z}/3\mathbb{Z}$

$\Rightarrow \left| \frac{\mathbb{Z}/3\mathbb{Z}[x]}{\langle x^2+1 \rangle} \right| = 9$

now, similarly x^2-3 is irreducible in $\mathbb{Z}/5\mathbb{Z}[x]$ as

$(\bar{0})^2-\bar{3} = -\bar{3} = \bar{2}$

$(\bar{1})^2-\bar{3} = -\bar{2} = \bar{3}$

$(\bar{2})^2-\bar{3} = \bar{1}$

$(\bar{3})^2-\bar{3} = \bar{1}$

$(\bar{4})^2-\bar{3} = \bar{3}$

i.e x^2-3 has no roots in $\mathbb{Z}/5\mathbb{Z}$

and similar to above ($\because$ deg ≤ 3)

$\frac{\mathbb{Z}/5\mathbb{Z}[x]}{\langle x^2-3 \rangle}$ is a field and $\left| \frac{\mathbb{Z}/5\mathbb{Z}[x]}{\langle x^2-3 \rangle} \right| = 25$

now for 27: let $x^3+\bar{2}x+\bar{1} \in \mathbb{Z}/3\mathbb{Z}[x]$

then

$(\bar{0})^3+\bar{2}\cdot\bar{0}+\bar{1} = \bar{1}$

$(\bar{1})^3+\bar{2}\cdot\bar{1}+\bar{1} = \bar{1}$

$(\bar{2})^3+\bar{2}\cdot\bar{2}+\bar{1} = \bar{1}$

so, x^3+2x+1 irreducible on $\mathbb{Z}/3\mathbb{Z}[x]$ ($\because$ deg ≤ 3)

$\Rightarrow \dfrac{\mathbb{Z}/3\mathbb{Z}[x]}{\langle x^3+2x+1\rangle}$ is a field ($\because$ similar to above)

and $\left|\dfrac{\mathbb{Z}/3\mathbb{Z}[x]}{\langle x^3+2x+1\rangle}\right| = 3^3 = 27$

6. K, L fields $\varphi: K \to L$ homomorphism

let $\Psi: \mathbb{Z} \to K$ homomorphism
then $\forall z \in \ker(\Psi)$

$\Psi(z) = 0_K \Rightarrow \varphi(\Psi(z)) = 0_L$
$\Rightarrow z \in \ker(\varphi \circ \Psi)$

now, $\varphi: K \to L$ homomorphism
$1_K \to 1_L$

$\forall z \in \ker(\varphi \circ \Psi)$

$\varphi \circ \Psi: \mathbb{Z} \to R \to L$
$1 \mapsto 1_R \mapsto 1_L$
$2 \mapsto 2_R \mapsto 2_L$
$\vdots \quad \vdots \quad \vdots$

$\varphi \circ \Psi(z) = 0_L$
$\Rightarrow \Psi(z) \in \ker(\varphi)$ as K, L are fields $\ker(\varphi) = 0 = \{0_K\}$
as if not
then as $\ker(\varphi)$ is ideal of a field
$\Rightarrow \ker(\varphi) = K$
($\because 1 \in \ker(\varphi)$ as if $a \neq 0 \in \ker(\varphi)$ then $a^{-1}.a \in \ker(\varphi)$)
K

but $\varphi: K \to L$
$1_K \to 1_L$ so, $1_K \notin \ker(\varphi)$

$\Rightarrow \Psi(z) \in \{0_K\}$
$\Rightarrow \Psi(z) = 0_K$
$\Rightarrow z \in \ker \Psi$

so, $\ker(\Psi) = \ker(\varphi \circ \Psi)$
$\Rightarrow \operatorname{char}(1) = \operatorname{char}(L)$ as $\Psi: \mathbb{Z} \to K$, $\tilde{\Psi}: \mathbb{Z} \to L$ (s.t $\Psi = \varphi \circ \Psi$) has same kernel and $\varphi \circ \Psi$ is homomorphism

7. $qf(\mathbb{Z}/p\mathbb{Z}[t])$ is a field and trivial infinite as $\mathbb{Z}/p\mathbb{Z}[t]$ infinite

$\Psi: \mathbb{Z} \to qf(\mathbb{Z}/p\mathbb{Z}[t])$ ← homomorphism, and everything else 0

$1 \mapsto 1$
$\vdots$
$p \mapsto 0$

$\Psi(p) = 0 \Rightarrow p.\mathbb{Z} \subseteq \ker(\Psi)$
and trivial to see, no $n < p$ $n \in \mathbb{N}$ will give $\Psi(n) = 0$
$\Rightarrow \operatorname{char}(qf(\mathbb{Z}/p\mathbb{Z}[t])) = p$

8. To prove: if $\text{char}(K)=0$ then prime subfield of K is $\mathbb{Q}$ and if $\text{char}(K)=0$ then prime subfield of K is $\mathbb{Z}/p\mathbb{Z}$

proof: as K is a field $\Rightarrow K$ is ID
$\Rightarrow \text{char}(K)=0$ or p (p prime in $\mathbb{Z}$)

Let $\psi: \mathbb{Z} \to K$ be homomorphism
$1 \mapsto 1_K$

then let $\ker(\psi) = n.\mathbb{Z}$ for $n \in \{0, p \mid \forall p \in \text{prime}\}$

$\psi : \mathbb{Z} \longrightarrow K$

$\pi \downarrow \quad \nearrow$

$\mathbb{Z}/n.\mathbb{Z}$

$\mathbb{Z}/n.\mathbb{Z} \cong \text{img}(\psi) \subset K$

as $\tilde{\psi}: \mathbb{Z}/n.\mathbb{Z} \to K$ is

now if $n=p$ then

$\tilde{\psi}: \mathbb{Z}/p\mathbb{Z} \longrightarrow K$ is injective

and so, $\mathbb{Z}/p\mathbb{Z} \cong \text{img}(\tilde{\psi}) \subset K$

↑ smallest subfield in K (∵ definition of char)

↙ cannot be smaller as then $\text{char}(K) < p$

if $n=0$, then $\tilde{\psi}: \mathbb{Z} \to K$ is injective

and so, $\mathbb{Z} \cong \text{img}(\tilde{\psi}) \subset K$

↑ subring

smallest subfield on $\mathbb{Z} = \mathbb{Z}\left[\frac{1}{n} \mid n>1\right]$

$= \mathbb{Q}$

So, if K is a field, then it contains exactly one of the prime subfields

9. sets: $\phi, \{1\}, \{1,2\}, \ldots \{1,2,\ldots 7\}$
total 8 with <8 elements
trivial to see, that they are isomorphic to other sets with $n<8$ elements
$n(S)=8$

group: if S is a group s.t. $|S|=p$ (p is prime)
then as every element's order divides p
$\forall a \in S \quad a^p = e$ then if $a \neq e$
$\Rightarrow i \mid p$
$\Rightarrow i = 1$ or p as p is prime
$\Rightarrow i = p$ as $a \neq e$
So, order of every non identity in $S = e$
$\Rightarrow S$ is cyclic of order p
i.e $S = \langle a \rangle$

$\varphi : (\mathbb{Z}/p\mathbb{Z}, +) \longrightarrow S$

$\bar{0} \longmapsto e$
$\bar{1} \longmapsto a$
$\bar{2} \longmapsto a^2$
$\vdots$
$\overline{p-1} \longmapsto a^{p-1}$

φ is homomorphism as $\varphi(0) = e$

for $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$

$\varphi(\bar{a}+\bar{b}) = a^{\bar{a}+\bar{b}}$
$= a^{\bar{a}} \cdot a^{\bar{b}}$
$= \varphi(\bar{a}) \cdot \varphi(\bar{b})$
↑ is + in $\langle a \rangle$

so, φ is homomorphic

also φ is one-one as, $\varphi(\bar{x}) = \varphi(\bar{y})$
$\Rightarrow a^{\bar{x}} = a^{\bar{y}}$
$\Rightarrow a^{(\bar{x}-\bar{y})} = e$
$\Rightarrow \bar{x}-\bar{y} \mid p$
$\Rightarrow \bar{x}-\bar{y} = \bar{0}$
$\Rightarrow \bar{x} = \bar{y}$

φ is onto, as $\forall\ y \in \langle a \rangle$, $y = a^{\bar{i}}$ for $\bar{i} \in \{0, 1, .. p-1\}$

$\exists\ \bar{i} \in \mathbb{Z}/p\mathbb{Z}$ s.t $\varphi(\bar{i}) = a^{\bar{i}} = y$

so, φ is isomorphism

$\Rightarrow S \cong (\mathbb{Z}/p\mathbb{Z}, +)$

so, for $|S|=1$, we have trivial $S = \{e\}$ as our unique group for isomorphism

$|S| = 2$ ($\because 2$ is a prime)
$\Rightarrow S \cong \mathbb{Z}/2\mathbb{Z}$

$|S| = 3$
$\Rightarrow S \cong \mathbb{Z}/3\mathbb{Z}$

$|S| = 5$
$\Rightarrow S \cong \mathbb{Z}/5\mathbb{Z}$

$|S| = 7$
$\Rightarrow S \cong \mathbb{Z}/7\mathbb{Z}$

now, if $|S|=4$ then we want to find groups of order 4

any group of order 4 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

as, if G has order 4, any element of G can have order 1, 2, 3 or 4 if $\exists$ element of order 4 then

$G \cong \mathbb{Z}/4\mathbb{Z}$

if not, then all elements have order 1, 2
$\Rightarrow$ non identity elements of G have order 2
$\Rightarrow g^2 = e \ \forall g \in G$

let $x, y \neq e \in G$ then
$x^2 = e$
$y^2 = e$
$(xy)^2 = e$

$\Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, so x, y commute

$\Rightarrow$ any group with all non identity elements of order 2 is abelian

$f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow G$

$f(a \bmod 2, b \bmod 2) = x^a y^b$

$(0,0) \longmapsto 1$
$(1,0) \longmapsto x$
$(0,1) \longmapsto y$
$(1,1) \longmapsto xy$

f is homomorphism as, $f(\bar{a}, \bar{b}) f(\bar{c}, \bar{d}) = (x^a y^b)(x^c y^d)$
$= x^{a+c} y^{b+d}$
$= f(\bar{a} + \bar{c}, \bar{b} + \bar{d})$
$= f(\overline{a+c}, \overline{b+d})$

and $f(0,0) = 1$

also trivial to see, f is a bijection ($\because$ 4 elements in both sets and one-one, onto follows)

$\Rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong G$

so if $|S| = 4$ then
$S \cong \mathbb{Z}/4\mathbb{Z}$ or $S \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

now, if $|S| = 6$ then
for this, if a group has even order then it contains an element of order 2

as let G $g \in G$ and g^{-1} $\{g, g^{-1}\}$ ← has 2 elements, if $g = g^{-1}$ then $g^2 = e$

now, $|G| = 2 \,|\text{pairs } \{g, g^{-1}\};\ g \neq g^{-1}|$
$+ \,|\{g \in G \mid g = g^{-1}\}|$

left side is even as G has even order

$$|G| = 2\,|\underbrace{\text{pairs } \{g, g^{-1}\}}_{g \neq g^{-1}}| + |\{g \in G \mid g = g^{-1}\}|$$

even $\Rightarrow |\{g \in G \mid g = g^{-1}\}|$ is even

and $e \in \{g \in G \mid g = g^{-1}\}$

$\Rightarrow \exists g \in G$ s.t $g = g^{-1}$ $g \neq e$

$\Rightarrow g^2 = e$ or $\exists$ element in G with order 2

now, $|G| = 6$ then $G \cong \mathbb{Z}/6\mathbb{Z}$ or S_3 as

Case I: G is abelian, then if all non-identity elements have order 2

$y, x \neq e$ s.t $y^2 = e$ G is abelian $\Rightarrow \{e, x, y, xy\}$ subgroup of G (∵ above)

but this violates Lagrange's theorm as $4 \nmid 6$

so, $\exists x \in G$ s.t $x^3 = 1$ or $x^6 = 1$

now, if $x^6 = 1$ then $G \cong \mathbb{Z}/6\mathbb{Z}$

if $x^3 = 1$ then as $\exists y \in G$ s.t $y^2 = 1$ (∵ above)

yx is s.t $y^2 = e$ $x^3 = e$

$$(yx)^2 = yx\,yx = y^2x^2 = x^2 \neq e$$

as $y = y^{-1}$ $xy = yx$

$$(yx)^3 = x^2\,yx = yx^3 = y^3x^3 = y \neq e$$

$$(yx)^6 = y^2 = e$$

$\Rightarrow yx$ is order 6

$\Rightarrow G \cong \mathbb{Z}/6\mathbb{Z}$

Case II: If G is non-abelian then $\exists y \in G$ s.t $y \neq e$, $y^2 = e$ (∵ above)

If all order 2 then abelian so, $\exists$ element with order 3 or 6 but not 6 as then G is abelian

so, $\exists x \in G$ s.t $x \neq e$, $x^3 = e$

now, let $H = \langle y \rangle = \{e, y\}$

H has 3 left cosets as $x \notin H$, $x^2 \notin H$

$H,\ xH,\ x^2H$

$\forall g \in G$ let $l_g : \{H, xH, x^2H\} \to \{H, xH, x^2H\}$

$l_g(cH) = gcH$ for left coset cH

call l_g is a permutation as $\exists\, l_{g^{-1}}$

so, if we labell $\{H, xH, x^2H\}$ as $\{1,2,3\}$ then l_g can be placed inside S_3

$G \to S_3$
$g \mapsto l_g$ is a homomorphism as

$l_g \circ l_{g'} = l_{gg'}$ as for any left coset cH

$(l_g \circ l_{g'})(cH) = g(g'cH) = (gg')cH = l_{gg'}(cH)$
(homomorphism)

also, $G \to S_3$ by $g \mapsto l_g$ is between finite group of equal size so if we show injective or surjective, then we are done

l_x: $H \to xH$
$xH \to x^2H$
$x^2H \to H$

so, img of $G \to S_3$ contains 3 cycle

now l_y, as $y \in H$ $l_y(H) = yH = H$ ($\because H = \{e, y\}$, $y^2 = e$)

l_y is a permutation if $l_y(xH) \neq x^2H$

then $l_y(xH) = xH$

$yxH = xH$
$\Rightarrow \{yx, yxy\} = \{x, xy\}$

yx is x or xy

if $yx = x$ then $y = e$ contradiction

if $yx = xy$ then x and y commute and so, yx has order 6 as

$(yx)^2 = (xy)^2 = xyyx = x^2 \neq e$

$(yx)^3 = x^2xy = y \neq e$

$(yx)^6 = y^2 = e$

but then $G \cong \mathbb{Z}/6\mathbb{Z}$ contradiction as G is non-abelian

$\Rightarrow l_y(xH) = x^2H$ or $\exists$ transposition in img of $G \to S_3$

now image contains transposition and element of order 3
$\Rightarrow \forall \sigma \in S_3$ we can write σ as combination of l_x and l_y

$\Rightarrow G \cong S_3$

so, $n(G) = |\{\{e\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, S_3\}|$
$= 9$

for Rings: if $|R|=p$ then (even if not p and some n then one of rings of $\mathbb{Z}/n\mathbb{Z}$)

$(R,+) \cong (\mathbb{Z}/p\mathbb{Z}, +)$

now def $\psi: (\mathbb{Z}/p\mathbb{Z}, +) \longrightarrow (R,+)$ group homomorphism

then $\psi(\bar{0}) = 0_R$ (∵ property of group homomorphism)

$\exists\ \bar{a} \in (\mathbb{Z}/p\mathbb{Z}, +)$ s.t

$\psi(\bar{a}) = 1_R$ (∵ $\exists\ 1_R \in R$)

(∵ ψ is surjective)

↑ R is ring with identity as if not then one more $a \times b = 0$ possible

now, $\varphi: \mathbb{Z}/p\mathbb{Z} \longrightarrow R$

$x \longmapsto x\,\psi(\bar{a})$

this is s.t $\varphi(\bar{1}) = (1)\psi(\bar{a})$

$= (1).1_R$

$= 1_R$

$\varphi(\bar{0}) = 0$

$\varphi(\bar{c}+\bar{d}) = (c+d)\,\psi(\bar{a})$

$= (c+d).1_R$

$= c.1_R + d.1_R$

$= \varphi(\bar{c}) + \varphi(\bar{a})$

$\varphi(\bar{c}.\bar{d}) = cd.1_R$

$= (c\,1_R)(d\,1_R)$

$= \varphi(\bar{c})\,\varphi(\bar{a})$

φ is ring homomorphism

now φ is one-one as:

$\ker(\varphi) = \{ \bar{x} \in \mathbb{Z}/p\mathbb{Z} \mid x.1_R = 0 \}$

$1_R + 1_R + \cdots + 1_R = 0$ if $x > 0$

$1_R + 1_R + \cdots 1_R = 0$

but as only when $x = 0, p, 2p, \ldots$

(∵ ψ is isomorphism)

$\Rightarrow \ker(\varphi) = \{0\}$

φ is one-one

and as both finite ⇒ φ is ring isomorphism

$\Rightarrow (R,+,\cdot) \cong \mathbb{Z}/p\mathbb{Z}$

now if $|R|=4$ then if we assume R is commutative with identity

then as $|R|=4$

then $(R,+) \cong (\mathbb{Z}/4\mathbb{Z}, +) \rightarrow R \cong \mathbb{Z}/4\mathbb{Z}$ from previous

or $(R,+) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$

$\Rightarrow (R,+) \cong (\mathbb{F}_2 \times \mathbb{F}_2, +)$

$\mathbb{F}_2 \times \mathbb{F}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$R = \{0, a, 1+a, 1\}$

now,

case I: $a^2 = 0$

$(a)(1+a) = a$

$(1+a)^2 = (1+a+a) = 1$

$\rightarrow \mathbb{Z}/4\mathbb{Z}$

case II: $a^2 = 1$

$(a)(1+a) = 1+a$

$(1+a)^2 = 1+a^2+a+a = 0$

$\rightarrow L = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{Z}/2\mathbb{Z} \right\}$

case III: $a^2 = a$

$(a)(1+a) = a+a = 0$

$(1+a)^2 = 1+a^2+a+a = 1+a2 = 1+a$

$\rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

case IV: $a^2 = 1+a$

$a(1+a) = a+a^2 = a+1+a = 1$

$(1+a)^2 = 1+a^2+a+a = 1+a+a+a+1 = a$

$\rightarrow \mathbb{F}_4$

so, for $|R|=4$ we have

$R \cong \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, L, \mathbb{F}_4$

now if $|R|=6$ then

$(R,+) \cong (\mathbb{Z}/6\mathbb{Z}, +)$ or S_3

now as S_3 has no $\times$ operation, from above only rings of $|R|=6$ can be $\mathbb{Z}/6\mathbb{Z}$

so, $n(R) = 1 + 4 + 1 + 4$ ← from $|R|=4$

1 ← from $|R|=1$

1 ← from $|R|=6$

4 ← from $|R|=2,3,5,7$

$\Rightarrow n(R) = 10$

now, finite ID ⇔ field

so, $|R|=1$ trivial

$|R|=p$ then $R \cong \mathbb{Z}/p\mathbb{Z}$ (field)

(commutative ring)

$|R|=4$ then case I: $R \cong \mathbb{Z}/4\mathbb{Z}$

not a field as

$(\bar{2})(\bar{2})=\bar{0}$ but $\bar{2}\neq 0$

$\Rightarrow$ R not ID

case II: $R \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$(1,0).(0,1)=(0,0)$

but $(1,0) \neq (0,0)$

$(0,1) \neq (0,0)$

$\Rightarrow$ R not ID

case III: $R \cong L$

but $(1+a)(1+a)=0$

from above

but $1+a \neq 0$

so R not ID

case IV: $R \cong \mathbb{F}_4$

field

$|R|=6$ then $R \cong \mathbb{Z}/6\mathbb{Z}$ not field as $\bar{2}.\bar{3}=\bar{0}$

but $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$

now, $n(D)=n(F)=1+4+1$ ($|R|=4$; $1 \to |R|=1$; $|R|=2,3,5,7$)

$=6$

we also know that finite fields are of p^n order

so, 6 not possible

1. $V \to$ vector space over $\mathbb{R}$

$\varphi: V \to V$ surjective linear map is isomorphism

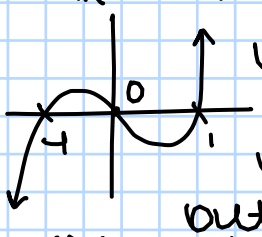
if V was infinite dimension

let $V=\mathbb{R}$

then $\mathbb{R}$ is vector space over $\mathbb{R}$

and, $\varphi: \mathbb{R} \to \mathbb{R}$

be



$\varphi(x)=(x)(x-1)(x+1)$

trivial to see surjective from graph

$\varphi(1)=\varphi(-1)$

but $1 \neq -1$

φ is not isomorphism

now, if V was finite dimensional vector space over $\mathbb{R}$ then let

$$\{v_1, v_2, \ldots v_n\} = \text{span } V$$

$\varphi: V \longrightarrow V$ is surjective linear map then

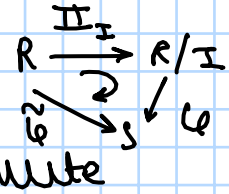
$$\dim(\underbrace{\text{img}(\varphi)}_{n \ (\because \text{surjective})}) + \dim(\ker(\varphi)) = n$$

$$\Rightarrow \dim(\ker(\varphi)) = 0$$
$$\Rightarrow \varphi \text{ is one-one}$$
$$\Rightarrow \varphi \text{ is isomorphism}$$

2. R, S commutative rings

I ideal of R $\quad \varphi: R/I \longrightarrow S$ Ring homomorphism

$\exists\ \tilde{\varphi}: R \longrightarrow S$ Homomorphism $\quad \ker(\tilde{\varphi}) = I$ and



commute

$R = \mathbb{Z}/_{9\mathbb{Z}} \quad I = 2\mathbb{Z}/_{9\mathbb{Z}} \quad S = (0)$

$$\varphi: \frac{\mathbb{Z}/_{9\mathbb{Z}}}{2\mathbb{Z}/_{9\mathbb{Z}}} \longrightarrow (0)$$

$$\varphi: \{\bar{0}, \bar{1}, \bar{3}, \bar{5}, \bar{7}\} \longrightarrow (0)$$

$$\Pi_I: \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\} \longrightarrow \{\bar{0}, \bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$
$$\bar{0}\ \bar{1}\ \bar{0}\ \bar{3}\ \bar{0}\ \bar{5}\ \bar{0}\ \bar{7}\ \bar{0}$$

but $\quad \tilde{\varphi}: R \longrightarrow S$
$\tilde{\varphi}(\gamma) = 0 \quad \forall \gamma \in R$

trivial to see this commutes but

$\ker \tilde{\varphi} \neq I$ but R

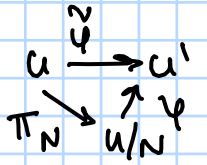
in all cases

if φ is injective then

$\ker(\varphi) = 0$
and so, $\ker(\varphi \circ \Pi_I) = \ker(\Pi_I) = I$

3. G, G' groups and N-normal subgroup of G

$\varphi: G/N \longrightarrow G'$ group homomorphism
then $\exists\ \tilde{\varphi}: G \to G'$ s.t $\ker \tilde{\varphi} = N$ and



commute

same as before $G = \mathbb{Z}/9\mathbb{Z}$, $N = 3\mathbb{Z}/9\mathbb{Z}$ $G' = \{0\}$

wrt $+$, then similar to above counter example

so, we need φ to be one-one

N is normal as G is commutative

4. A_4 is order 1, 3 double transpose, 8 3-cycles
e order 2 order 3

if $\exists$ H s.t $|H|=6$ and subgroup
then A_6 not cyclic
$\Rightarrow H \cong S_3$
$\Rightarrow$ H contains 3 elements of order 2 (max)
but S_3 has 4
this is a contradiction

so, (i) is not true
if n = prime or G abelian then trivially true
↑ cauchy's theorem ↑ cauchy theorem for abelian groups

again in (ii), $G = A_4$ then as A_4 is not cyclic
there is no element of A_4 with order 12
$n = 12$ as $12 \mid |G| = 12$

If n = prime (by cauchy)
or G abelian, this holds

5. we have seen this before $n(4) = 9$

6. Basic group smallest order $= \{\bar{0}, \bar{1}\} = \mathbb{Z}/2\mathbb{Z}$

$|\mathbb{Z}/2\mathbb{Z}| = 2 \neq 60$

smallest non-abelian case is A_5

7. we have proved for case of finite then
but
$\mathbb{Z}$ is ID Not field

8. $n \in \mathbb{N}_{\neq 1,2}$ $n = 6$
then $\exists$ char$(F) = p \neq 0$
($\because$ F is finite)
but then from previous argument
$F = p^n$ as $6 \neq p^n$ for all p
not possible

so, $|F| = p^\alpha$ for any prime, $\alpha \in \mathbb{N}_{\neq 0}$

9. $(\mathbb{R}, +) \longrightarrow (\mathbb{C}, +)$ are non-isomorphic
is false as $(\mathbb{R}, +) \cong (\mathbb{C}, +)$
as both VS over $\mathbb{Q}$
and dim $\mathbb{R}$ has same card as dim $\mathbb{C}$
($\because |\mathbb{R}| = |\mathbb{C}|$, done in class)
but for $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ we have if $\exists$ isomorphism
then

$\psi : \mathbb{R}^* \longrightarrow \mathbb{C}^*$

St $\exists\ \alpha \in \mathbb{R}^*$

$\psi(\alpha) = i$

$\psi(\alpha) \cdot \psi(\alpha) = i \cdot i$

$\psi(\alpha^2) = -1$

$\Rightarrow \psi(-\alpha^2) = 1$

$\Rightarrow \psi(-\alpha^2) = \psi(1)$

$\Rightarrow -\alpha^2 = 1$

this is a contradiction

same for R, $\mathbb{C}$ as rings

10. no of subsets of $\mathbb{Z}$ is same as subgroups of $(\mathbb{Z}, +)$

all subgroups of $\mathbb{Z}$ are of form $n\mathbb{Z}$, $n \in \mathbb{N} \cup \{0\}$

as $H \neq \{0\}$ ($n = 0$ trivial)

let $n = \min\{m \mid m \in H, m > 0\}$

$H \neq n\mathbb{Z}$

then $\exists\ k \in H \setminus n\mathbb{Z}$ $\quad k = q \cdot n + r$

but $r = k - q \cdot n \in H$

$r < n \Rightarrow r = 0$

$\Rightarrow k = qn$

this is a contradiction

∴, card of subgroups of $\mathbb{Z}$ is $|\mathbb{N}|$

but

card of subsets of $\mathbb{Z}$ $= \text{card of } P(\mathbb{Z})$

$= |P(\mathbb{N})|$

but $|P(\mathbb{N})| > |\mathbb{N}|$

∴, the statment is card is diffent

11. $(\mathbb{Q}, +)$ has uncountable many subgroups

as for $P = \{p_1, p_2 .. p_k \mid \text{primes}\}$

$\mathbb{Q}\left[\frac{1}{p}\right]$ = subgroup where denominator is some form of $p_1^{r_1} \cdot p_k^{r_k}$

but no of subsets like P is $|P(\mathbb{N})|$

Tutorial-3:

1. $R[t]$ pigeonhole

3. show $\text{ker}\,\alpha = 0$

4. $F \to$ field, $t \in F(t) = qf(F[t])$
   then $\forall n \geq 2$, $\exists r(t) \in F(t)$ s.t $r(t)^n = t$

   if $\exists\ (r(t))^n = t$

   $$\left(\frac{b(t)}{a(t)}\right)^n = t$$

   $$b(t)^n = t\,a(t)^n$$

   $d_1 n = d_2 n + 1$
   $\Rightarrow n \mid 1 \quad n \geq 2$
   not possible

5. R is a ring

   ($\Rightarrow$) R is a field, $R[t]$ is a domain
   let I be ideal by $f_1, f_2, \ldots f_n \in R[t]$
   $I \neq R[t]$
   let $d \in I$ be a polynomial with least degree

   consider $r_i^\circ = f_i \bmod d$
   $f_i = d\,q_i + r_i$, $f_i \in I$ $d \in I \Rightarrow r_i \in I$

6. F is a field $G \leq F^*$
   $|G| < \infty$ G is cyclic

   F^* is abelian $\Rightarrow G$ is finite abelian group
   $\Rightarrow G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ $d_1, d_2, \ldots d_k \in \mathbb{Z}$
   $d_1 \mid d_2 \mid \ldots \mid d_k$
   (: structure theorem)

   $\Rightarrow g^{d_k} = 1 \quad \forall g \in G$

   $\Rightarrow x^{d_k} - 1 \in F[x]$ has atmost d_k roots in F
   ($\because F$ is a field)

   $\Rightarrow |G| \leq d_k$

   but $d_k \leq |G| = d_1 d_2 \ldots d_k$
   $\Rightarrow d_1 = d_2 \cdots = d_{k-1} = 1$

   $\Rightarrow G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \cong \mathbb{Z}/d_k\mathbb{Z}$
   $\Rightarrow G$ is cyclic

9. $x^n + p$ by gauss lemma / Eisenstine criterion
   irred in $\mathbb{Z}$
   $\Rightarrow$ irred in $\mathbb{Q}$
   Pair infinite

13. if $F^* = \langle g \rangle$ cyclic char $\neq 2$ then $-1 = g^n$ $g^{2n} = 1$ generator once generates finite many

$\{1, g_1 \cdots g^{2n-1}\}$

for char $= 2$ $\quad -1 = 1$ $\quad g^0 \to$ no contradiction

$\mathbb{F}_2 \hookrightarrow \mathbb{F} = \langle g \rangle$ $\quad g$ cannot be root (if so then field extension is finite)

if $f(x) \in \mathbb{F}_2[x]$, $f(g) = 0$ $\quad \mathbb{F} = \mathbb{F}_2(g)$ $\quad F = \mathbb{F}_2(g)$

$\mathbb{F}$ finite

$\mathbb{F}_2$

finite as $\mathbb{F}_2$ is finite

if no root : $1 + g = g^n$ $\mathbb{F}_2$

1. finite ring R

To prove: $\exists$ distinct polynomials in $R[t]$ giving same function

proof: let $R = \{r_1, r_2, \ldots r_n\}$

then

$$f_p(t) = r_p \prod_{i=1}^{n} (t - r_p)$$

is s.t $f_i(t) \neq f_j(t)$ for $i \neq j$

but

$f_i(r) = f_j(r) \; \forall r \in R$ $\quad (= 0)$

also from pigeonhole principle this follows

2. $\phi : R \to S$ $\quad \forall s \in S$ $\exists$ unique ring homomorphism $\tilde{\phi} : R[t] \to S$ s.t $\tilde{\phi} = \phi$ on R, $\tilde{\phi}(t) = s$

now let $\tilde{\phi}_1 : R[t] \to S$

$\tilde{\phi}_2 : R[t] \to S$ be two such ring homomorphisms

then $\tilde{\phi}_1(f(t)) = \tilde{\phi}_1\left(\sum_{i=0}^{n} a_i t^i\right)$

$$= \sum_{i=0}^{n} a_i \tilde{\phi}_1(t^i)$$

$$= \sum_{i=0}^{n} a_i s^i$$

$$= \sum_{i=0}^{n} a_i \tilde{\phi}_2(t^i)$$

$$= \sum_{i=0}^{n} \tilde{\phi}_2(a_i t^i)$$

$$= \tilde{\phi}_2(f(t))$$

so, $\forall f(t) \in R[t]$, $\quad \tilde{\phi}_1(f(t)) = \tilde{\phi}_2(f(t))$

$\Rightarrow \tilde{\phi}_1 = \tilde{\phi}_2$ or $\tilde{\phi}$ is unique

3. R is ring $\quad c \in R$

To prove: $\phi_c : R[t] \longrightarrow R[t] \quad \phi_c = id$ on $R \quad \phi_c(t) = t^2 + c$
is injective ring homomorphism

proof: ϕ_c is ring homomorphism as

$$\phi_c(e) = e, \quad \phi_c(0) = 0$$

$$\phi_c(f(t)) = \phi_c\left(\sum_{i=0}^{n} a_i t^i\right)$$

$$= \sum_{i=0}^{n} a_i (t^2 + c)^i$$

then $\phi_c(f(t) + g(t)) = \phi_c\left(\sum_{i=0}^{n} a_i t^i + \sum_{i=0}^{m} b_i t^i\right)$

$$= \sum_{i=0}^{n} a_i (t^2 + c)^i + \sum_{i=0}^{m} b_i (t^2 + c)^i$$

$$= \phi_c(f(t)) + \phi_c(g(t))$$

similarly, $\phi_c(f(t) \cdot g(t)) = \phi_c\left(\sum_{j=0}^{m}\sum_{i=0}^{n} a_i b_j t^{i+j}\right)$

$$= \sum_{j=0}^{m}\sum_{i=0}^{n} a_i b_j \phi_c(t^{i+j})$$

$$= \sum_{j=0}^{m}\sum_{i=0}^{n} a_i b_j (t^2 + c)^{i+j}$$

$$= \left(\sum_{i=0}^{n} a_i (t^2 + c)^i\right)\left(\sum_{j=0}^{m} b_j (t^2 + c)^i\right)$$

$$= \phi_c(f(t))\, \phi_c(g(t))$$

so, ϕ_c is ring-homomorphism

$$\ker(\phi_c) = \{ f(t) \in R[t] \mid \phi_c(f(t)) \equiv 0 \}$$

$$\text{i.e } \sum_{i=0}^{n} a_i (t^2 + c)^i = 0$$

$$\Rightarrow \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{i} \binom{i}{j} t^{2j} c^{i-j} \right) = 0$$

all terms 0

$\Rightarrow$ highest power term is

$$a_n t^{2(n)} c^{n-n} = 0$$

$$\Rightarrow a_n t^{2n} = 0 \quad \forall t \in R$$

$$\Rightarrow a_n = 0$$

so, function of n degree $a_n \neq 0$, but $a_n = 0$
$\Rightarrow a_i = 0 \ \forall i$ ($\because$ this contradicts)

$\forall f,\ f \equiv 0$ iff $f \in \ker(\phi_c)$

$\Rightarrow \ker(\phi_c) = 0$

so, ϕ_c is one-one function

also we saw that degree of f_t becomes $2n$ if deg was n

then $t \in R[t]$ s.t

no $f(t) \in R[t]$

$\phi_c(f(t)) = t$

as t was degree 1 but if f was deg 0 then deg max is 0

if f was deg 1 then

$f(x) = ax + b \qquad a \neq 0$

$\phi_1(f(t)) = a(t^2 + c) + b$

$= at^2 + c'$ deg 2 as $a \neq 0$

so, ϕ_c is not surjective

4. if $\exists\ f(t) \in \mathbb{F}(t)$ s.t $\forall\ n > 2$

$(f(t))^n = t$ then as $f(t) \in \mathbb{F}(t)$

$\exists\ r(t), g(t)$ s.t $g(t) \neq 0$

$\frac{r(t)}{g(t)} = f(t)$

$r, g \in \mathbb{F}[t]$

$\Rightarrow \frac{(r(t))^n}{(g(t))^n} = t \Rightarrow (r(t))^n = t(g(t))^n$

so, $\deg(r) \times n = 1 + \deg(g) \times n$

$\Rightarrow n(\deg(r) - \deg(g)) = 1$

$\Rightarrow n \mid 1$ or $0 = 1$

$\Rightarrow n = 1$ this is a contradiction or $0 = 1$

so, no n^{th} root $f(t)$ exist $\forall\ n > 2$

5. ($\Rightarrow$) given R is a field

$R[t]$ is ID, let I be an ideal generated by $f_1, f_2, \ldots f_n \in R[t]$

$I \neq R[t]$

let $d \in I$ be non-constant polynomial with least degree, let $r_i \equiv f_i \bmod d$

$f_i = dq_i + r_i$, $f_i \in I$, $d \in I \Rightarrow r_i \in I$

$\because$ division of polynomial over field

as $\deg r_i < \deg d$, $\deg r_i \neq 0$ then this is a contradiction

$\Rightarrow \deg r_i = 0$

if $r_i = c \quad c \neq 0$ then $\langle r_i \rangle = I = R[t]$

but as $I \neq R[t] \Rightarrow r_i = 0$

now, $d|f_i \ \forall i \Rightarrow f_i \in (d) \Rightarrow I \subseteq (d)$
but $d \in I \Rightarrow (d) \subseteq I$
so, $(d) = I$
Or every ideal is Principal

$\Rightarrow R[t]$ is PID

($\Leftarrow$) $R[t]$ is PID, let ideal be (t)
then $\frac{R[t]}{(t)} \cong R$
if (t) is maximal, then

$\frac{R[t]}{(t)}$ is field $\Rightarrow R$ is field

if $\exists M = (f) \neq R[t]$ s.t $(t) \subset M$ $f \neq \lambda t$ $\lambda \in R^*$
if $\deg f > 1$ then
$t \notin (f) \Rightarrow \deg f = 0$ or 1

if $\deg f = 0$ then $(f) = R[t]$, so

$\deg f = 1 \Rightarrow f = at + b$ some $a, b \in R$

if $t \in (f)$ then $\exists c \in R$ s.t $cf = t$ as both have same degree

$\Rightarrow t = cf \Rightarrow t = cat + cb$
$\Rightarrow ca = 1, \ cb = 0$
$b = 0$
so, $f = at$
but as a is unit
$M = (t)$
$\Rightarrow (f) = (t)$ or (t) is maximal

6. F field $u \leq F^*$ $|u| < \infty$ then u is cyclic

F^* abelian $\Rightarrow u$ is finite abelian group

$\Rightarrow u \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$

$d_1, d_2, \ldots d_k \in \mathbb{N}$
$d_1 | d_2 | \ldots d_k$ ($\because$ structure theorem)

then $g^{d_i} = 1$
but $d_i | d_k$

$\Rightarrow g^{d_k} = 1 \ \forall g \in u$

but $x^{d_k} - 1 \in F[x]$ has atmost d_k roots ($\because F$ is field)

$\Rightarrow |u| \leq d_k$
but $d_k \leq |u| \leq d_k \Rightarrow |u| = d_k$
and
$d_1 d_2 \ldots d_{k+1} = 1$
$\Rightarrow d_1 = d_2 = \cdots = d_{k+1} = 1$

$\Rightarrow G \cong \mathbb{Z}/d_K\mathbb{Z}$

$\Rightarrow G$ is cyclic

now, $\mathbb{F}_p^{*2}$ is cyclic subgroup of $\mathbb{F}_p^*$ of index 2 ($p>2$)

as $\phi: \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$

$\phi(a) = a^2$ is group homomorphism (trivial)

$\Rightarrow \operatorname{img}\phi = \mathbb{F}_p^{*2}$ subgroup of $\mathbb{F}_p^*$

$\Rightarrow (\mathbb{F}_p^*)^2$ is cyclic

index of $(\mathbb{F}_p^*)^2 = |\ker(\phi)| = |\{a \in \mathbb{F}_p^* \mid a^2 = 1\}|$

but $x^2 - 1 \in \mathbb{F}_p^*[x]$ has almost 2 roots

so, $|\{a \in \mathbb{F}_p^* \mid a^2 = 1\}| \leq 2$

but $\exists\ 1$ s.t $1^2 = 1$, $(-1)^2 = 1$

so, $\ker(\phi) = \{1, -1\}$

and so, index of $\mathbb{F}_p^* = |\{1, -1\}| = 2$

now, we have to show that if a, b are non-squares in $\mathbb{F}_p^*$ then ab is square

let $\mathbb{F}_p^* = \langle g \rangle$ $g \in \mathbb{F}_p^*$, let a, b be non-squares

$\Rightarrow a = g^{2m+1}$, $b = g^{2n+1}$ some $m, n \in \mathbb{Z}$

$ab = g^{2(m+n+1)} = (g^{m+n+1})^2$

$\Rightarrow ab$ is square

also index of $(\mathbb{F}_p^*)^2 = 2$ so, $(\mathbb{F}_p^*)^2 \cup p(\mathbb{F}_p^*)^2 = \mathbb{F}_p^*$

$\mathbb{F}_p^* = \langle p \rangle$

so, if $a, b \in p(\mathbb{F}_p^*)^2$ same $ab \in p^2(\mathbb{F}_p^*)^2 = (\mathbb{F}_p^*)^2$

7. To prove: $\mathbb{N}$ has infinitely many primes

proof: if $\mathbb{N}$ has finitely many primes, then

$\{p_1, p_2, \ldots, p_n\}$ = set of primes

let $N = \prod_{i=1}^{n} p_i + 1$

by fundamental theorem of arithmetic

$\exists\ p_K$ s.t $p_K \mid N \Rightarrow p_K \mid (\prod p_i + 1) - (\prod p_i)$ as $p_K \mid \prod p_i$

$\Rightarrow p_K \mid 1$ this is a contradiction

8. To prove: for any field F, $F[t]$ has infinitely many irreducible polynomials

Proof: If not then let $\{p_1(t), \dots p_n(t)\}$ be set of polynomials ($\deg \geq 1$)

$$f(t) = \prod_{i=1}^{n} p_i(t) + 1$$ then as $F[t]$ is ED ($\because F$ is field)

by fundamental theorem of arithmetic

$\exists\ p_i(t)$ s.t

$$p_i(t) \mid f(t) \text{ as } p_i(t) \mid \prod_{i=1}^{n} p_i(t)$$

$$\Rightarrow p_i(t) \mid N - \prod_{i=1}^{n} p_i(t)$$

$$\Rightarrow p_i(t) \mid 1$$

this is a contradiction

9. To prove: $\forall n \geq 1$, $\mathbb{Q}[t]$ has infinitely many irreducible polynomials

proof:

$x^n + p$ is s.t $a_n = 1$ $p \nmid 1$, $p \mid a_i$ $\forall\ i = 0, 1, \dots n-1$

$$p^2 \nmid a_0 = p$$

So, by eisthis criteria $x^n + p$ is irreducible in $\mathbb{Q}[t]$

as there are infinte many primes, we have infinite many degree n polynomials in $\mathbb{Q}[t]$

10. $P(t) \in \mathbb{R}[t]$

if $P(t)$ is irreducible with $\deg > 2$

then

in $\mathbb{C}[t]$, by fundamental theorem of algebra

$$P(t) = \alpha(t-\alpha_1)(t-\alpha_2)(t-\alpha_3)$$

now as irreducible $\alpha_1, \alpha_2, \alpha_3$ all in $\mathbb{C}$

but

by complex conjugate theorem

$$P(\alpha_1) = 0 \Rightarrow P(\bar{\alpha}_1) = 0$$

as $\alpha_1 \in \mathbb{C} \setminus \mathbb{R}$

$\bar{\alpha}_1 \neq \alpha_1$

So, $P(t) = f(t)[t-\alpha_1][t-\bar{\alpha}_1]$

$t^2 + \alpha_1^2 \in \mathbb{R}[t]$

So, $P(t)$ is reducible

this is a contradiction

So, if $P(t)$ is irreducible then $\deg \leq 2$

11. $f(t) = t^4 - 10t^2 + 1 \in \mathbb{Q}[t]$ is irreducible

if reducible

then $\exists\ f_1, f_2 \in \mathbb{Z}[t]$

s.t

$\deg f_1 + \deg f_2 = 4$, $\deg f_i \geq 1$

$f = f_1 f_2$

if $\deg f_1 = 1$ (w.l.o.g)

then $f(t) = \underbrace{(t+\alpha)}_{\in \mathbb{Z}[t]}\underbrace{(t^3+\beta t^2+ct+d)}_{\in \mathbb{Z}[t]}$

$= t^4 - 10t^2 + 1$

$t^4 + \beta t^3 + ct^2 + dt + \alpha t^3 + \alpha\beta t^2 + \alpha ct + \alpha d = t^4 - 10t^2 + 1$

$\beta + \alpha = 0,\ c + \alpha\beta = -10,\ d + \alpha c = 0,\ \alpha d = 1$

$\alpha d = 1 \Rightarrow \alpha = 1, d = 1$

$\beta = -\alpha \Rightarrow \beta = -1$

$c - 1 = -10 \Rightarrow c = -9$

but then $d + \alpha c \neq 0$ this is a contradiction

if $\deg f_1 = 2$ then

$t^4 - 10t^2 + 1 = (t^2 + \alpha t + \beta)(t^2 + ct + d)$

$= t^4 + ct^3 + dt^2 + \alpha t^3 + \alpha ct^2 + \alpha dt + \beta t^2 + \beta ct + \beta d$

$c + \alpha = 0$

$-10 = d + \alpha c + \beta$

$0 = \alpha d + \beta c$

$1 = \beta d \Rightarrow \beta = 1, d = 1$

$0 = \alpha + c \qquad -10 = 1 + \alpha c + 1$

$\alpha c = -12 \qquad -12 = \alpha c$

$\alpha = -c$

$-\alpha^2 = -12$

$\alpha^2 = 12$ not possible, contradiction as $\alpha \in \mathbb{Z}$

so, f is irreducible in $\mathbb{Z}[t]$

$\Rightarrow f$ is irreducible in $\mathbb{Q}[t]$ ($\because$ gauss)

12. F^* is cyclic as a multiplicative subgroup from (6)

now, as F is finite field it has char $p \neq 0$ prime

if $p = 2$ then

$$\phi : F \longrightarrow F$$
$$a \longmapsto a^2$$

$\phi(rs) = r^2 s^2$

$\phi(1) = 1,\ \phi(0) = 0$

$\phi(r+s) = (r+s)^2 = r^2 + 2rs + s^2$

↳ But char $2 \Rightarrow 2rs = 0$

so, field generated by $\{0,1\}$

$= r^2 + s^2$

so, $\phi(r^{-1}) = (r^{-1})^2 = (\phi(r))^{-1}$, so ϕ is field Homomorphism

$\ker(\phi) = 0$ ($\because \phi$ is field Homomorphism)

and as F is finite $\Rightarrow \phi$ is isomorphism

or, $\forall a \in F, \exists x \in F$ s.t

$$\phi(x) = a \Rightarrow x^2 = a$$
$$\Rightarrow a = x^2 + 0^2$$

so, $\forall a \in F$, a can be written as square of 2

if $P > 2$: $\phi : F^\times \longrightarrow F^\times$, $a \longmapsto a^2$

$\text{img}(\phi)$ = subset of F that can be written as a^2 for some $a \in F$

$\phi(a) = \phi(b)$ then

$$a^2 - b^2 = 0$$
$$\Rightarrow (a-b)(a+b) = 0$$
$$\Rightarrow a = b \text{ or } a = -b$$

$b \neq 0$, $P > 0$ $b \neq -b \Rightarrow \phi$ is two-to-one map, $2|\text{img}(\phi)| = |F|$

so, $\frac{|F^\times|}{2} = \frac{|F|-1}{2}$ square elements in $F^\times$

0 is also square in F

$\frac{|F|-1}{2} + 1 = \frac{|F|+1}{2}$ squares in F

$A = \{a^2 \mid a \in F\}$

$|A| = \frac{|F|+1}{2}$

$x \in F$, $B = \{x - b^2 \mid b \in F\}$

then $|B| = |A|$ is trivial

$\Rightarrow |B| = \frac{|F|+1}{2}$

and $|A| + |B| = |F| + 1$ both subsets in F

so, $A \cap B \neq \phi$

$\exists a, b \in F$ s.t $a^2 = x - b^2$

$\Rightarrow x = a^2 + b^2$

13. F is infinite field, then F^* is not cyclic

If $\text{char } F \neq 2$ then if F^* is cyclic

$\exists x$

$\langle x \rangle = F^*$

$\Rightarrow \exists n \in \mathbb{N}$ s.t

$x^n = -1 \neq 1$ ($\because P > 2$)

$\Rightarrow x^{2n} = 1$

so, F^* is finite field (this is a contradiction)

if $P = 2$: F^* is cyclic then $F^* = \langle x \rangle$ $x \neq 1 = -1$

$1 + x \in F^*$ ($\because x \neq 1 = -1$)

$\Rightarrow 1 + x = x^n$ for some $n \in \mathbb{N}$

or x is algebraic over $\mathbb{F}_2$ or F

but then $\min_{\mathbb{F}_2}(x) = f(t) \in \mathbb{F}_2[t]$

then $x \in \mathbb{F}_2(x)$ ← field with finite elements

as $\mathbb{F}_2(x) \cong \frac{\mathbb{F}_2[t]}{(\min_{\mathbb{F}_2}(x))}$

$\Rightarrow \mathbb{F}_2(x)^\times$ is cyclic

$\Rightarrow x^n = 1$ or x has finite order

this is a contradiction

so, $p \neq 2$, $p = 2 \Rightarrow \forall F$ we get contradiction

14. (a) $f, g \in \mathbb{Q}[t]$

false as $f = t$, $g = t$

$\deg(f-g) = 0 < 1$

(b) $f, g \in \mathbb{Q}[t] \setminus \{0\}$

$f \mid g \Rightarrow \deg(f) < \deg(g)$

false as $f = g$ also possible

(c) $f \in \mathbb{Z}[t]$ irreducible over $\mathbb{R}[t]$

false:

$f(t) = 2(t-1)$

↓ reducible over $\mathbb{Z}[t]$

but irreducible over $\mathbb{R}[t]$ ($\because \deg 1$)

(d) (i) t^4+1 is irreducible in $\mathbb{Z}[t]$

as ① monic

so, if $\exists f_1, f_2$

$t^4+1 = f_1 f_2$ then $f_1 \deg \geq 1$, $f_2 \deg \geq 1$

but $t^4+1 = (t^2+at+b)(t^2+ct+d)$

$= t^4 + ct^3 + at^3 + dt^2 + act^2 + bt^2 + adt + bct + bd$

$a+c=0 \Rightarrow a=-c$

$d+ac+b=0 \quad d-a^2+b=0 \Rightarrow 2=a^2$ ← contradiction

$ad+bc=0$

$bd=1 \Rightarrow b=d=1$ or $-1 \Rightarrow b=d=1$ ↩

if $(t^4+1) = (t^3+at^2+bt+c)(t+d)$

$$= t^4 + dt^3 + at^3 + adt^2 + bt^2 + bdt + ct + dc$$

$dc = 1 \Rightarrow d = c = 1$ or -1 $\quad a + d = 0$, $a = -d$

as $a = -d$, $-a^2 + b = 0$, $a^2 = b$

$bd + c = 0 \Rightarrow -a^3 + c = 0 \Rightarrow +a^3 = +c$

let $c = 1$ then $a = -1$ as $a = -d$

$c = -1$ then $a = 1$ as $a = -d$

this is a contradiction

(ii) $t^3 - 7t^2 + 3t + 3$

$= t^3 - t^2 - 6t^2 + 6t - 3t + 3$

$= t^2(t-1) - 6t(t-1) - 3(t-1)$

$= (t^2 - 6t - 3)(t-1)$

reducible

(iii) $t^5 + t^4 + t^3 + t^2 + t + 1$

is irreducible over $\mathbb{Q}$

as, if reducible then reducible over $\mathbb{Z}[t]$ as $\gcd(1, \dots 1) = 1$, monic

if $\exists f_1, f_2$

$t^5 + \dots + 1 = f_1 f_2$ → deg 4, → deg 1

$= (t + a_1)(t^4 + b_1 t^3 + b_2 t^2 + b_3 t + b_4)$

$= t^5 + b_1 t^4 + b_2 t^3 + b_3 t^2 + b_4 t + a_1 t^4 + a_1 b_1 t^3 + a_1 b_2 t^2 + a_1 b_3 t + a_1 b_4$

$b_1 + a_1 = 1$	$b_1 = 0$ if $a_1 = 1$
$b_2 + a_1 b_1 = 1$	$b_2 = 1$
$b_3 + a_1 b_2 = 1$	$b_3 = 0$
$b_4 + a_1 b_3 = 1$	$b_4 = 1$

$a_1 b_4 = 1 \Rightarrow a_1 = 1 = b_4$ or $a_1 = -1 = b_4$

$(t+1)(t^4 + t^2 + 1)$

$= t^5 + t^3 + t + t^4 + t^2 + 1$

$\Rightarrow$ if is reducible

15. (a) $\mathbb{R} \to \mathbb{R} \setminus \{0\}$ bijection

$\mathbb{R} \to \mathbb{R} \setminus \mathbb{Z}$

let $\{x_1, x_2, \dots\}$ be some countable collection in $\mathbb{R}$ s.t $x_1 = 0$

then let $x_1 \to x_2$

$x_2 \to x_3$

$\Rightarrow$ function s.t $f(x_i) = x_{i+1}$

$\Psi: \mathbb{R} \to \mathbb{R}\setminus\{0\}$

$\Psi|_{\mathbb{R}\setminus\{x_1, x_2 \dots\}} = id$

$\Psi|_{\{x_1, \dots\}} = f(x)$

trivial to see this is bijection

similarly we make $\{x_{1,1} \dots\}$

$\{x_{2,1} \dots\}$

$\vdots$

$\{x_{i,1} \dots\}\ \forall i \in \mathbb{Z}$

s.t. f_ρ is above described function

then $\Psi: \mathbb{R} \to \mathbb{R}\setminus\mathbb{Z}$

$\Psi|_{\mathbb{R}\setminus \text{all seq}} = id$

$\Psi|_{\text{some seq}_\rho} = f_\rho$

trivial to see bijection

(b) F is a field $\Rightarrow$ F[X] is ED

$\Rightarrow$ F[X] is UFD ($\because$ ED $\Rightarrow$ UFD)

(c) as both vector space of $|\mathbb{R}| = |\mathbb{C}|$ dim over $\mathbb{Q}$ they are isomorphic

but over ring $\exists$ contradiction

$-a^2 = 1$

(d) same contradiction, if so, then $\exists \Psi$ isomorphism

$\Psi: \mathbb{R}^* \to \mathbb{C}^*$

$\Psi(a) = i$ for some $a \in \mathbb{R}^*$

$\Psi(a^2) = -1$

$\Psi(-a^2) = 1$

$\Psi(1) = 1 \Rightarrow 1 = -a^2$

(f) X is infinite set, then $|X| = |X \times X|$ as

$\Sigma = \{(A, \sigma) \mid \sigma: A \to A \times A$ is a bijection $A \subseteq X\}$

$(A, \sigma) \leq (B, \mu)$ when

$\mu|_A = \sigma \quad A \subseteq B$

$\Sigma \neq \emptyset$ as X is infinite, $\exists \{x_1 \dots\} \subseteq X$ (A)

$\sigma: A \to A \times A$ is $\sigma: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ bijection



$\{(A_i, \sigma_i) \mid i \in I\}$ $A = \bigcup_{i \in I} A_i$, $\sigma|_{A_i} = \sigma_i$ → maximal element

$\exists$, by Zorn Lemma $\exists$ maximal M

if $M \neq X$ ① $X \setminus M$ true

and $\exists \{x_1 \dots\} \subseteq X \setminus M$ s.t. A

$\psi: A \to A \times A$ is $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ bijection

this is contradiction

② if $X \setminus M$ is finite true from before $\{x_1 \dots x_n\}$ can be trivially added it on M by taking a sequence ($\because M$ is infinite) and shifting then by n

$\therefore M = X$

$\therefore \exists \sigma: X \to X \times X$ bijection

(e) $\mathbb{Q}_{>0}$ is free abelian under multiplication as by fundamental theorem of arithmetic

$\forall n \in \mathbb{N}$ $n = p_1^{r_1} \dots p_k^{r_k}$

$\frac{n}{m} \in \mathbb{Q}_{>0}$ $\gcd(n, m) = 1$

$\frac{n}{m} = \frac{p_1^{r_1} \dots p_k^{r_k}}{q_1^{r_1'} \dots q_\ell^{r_\ell'}}$ $p_i \neq q_i$ ($\because \gcd = 1$)

all $\frac{n}{m}$ of this form in $\mathbb{Q}_{>0}$

$\therefore$ basis of $\mathbb{Q}_{>0}$ is combination of elements in $\{p, \frac{1}{p} \mid p \text{ prime}\}$

trivially a basis by fundamental theorem of arithmetic

as ① it says

② for any $\frac{p_1^{r_1} \dots p_k^{r_k}}{q_1^{r_1'} \dots q_\ell^{r_\ell'}} = 1$

$\Rightarrow p_1^{r_1} \dots p_k^{r_k} = q_1^{r_1'} \dots q_\ell^{r_\ell'}$ ($\because$ UFD property)

$\exists p_i \mid q_j \Rightarrow p_i = q_j \Rightarrow p_2^{r_2} \dots p_k^{r_k} = (\dots)$

next term

as all primes unique factorization pairs

$1 = 1$ $p_i = q_j$

Tutorial-4:

1. (i) 2 cases $\begin{matrix}1+3\\2+2\end{matrix}\}$ → show both contradiction or $f(t) \leftrightarrow f(t+1)$

3. no. of irred monic deg ≤ 5 in $\mathbb{F}_3[t]$

$\mathbb{F}_p[X]$ p prime

irred of deg n N_0 = No of irred / $\mathbb{F}_p[X]$

$\prod\prod f(X)$ $\quad$ $x^{p^n} - x = \prod\prod f(X)$
d|n f irred of deg d $\quad$ d|n f irred deg d

$$p^n = \sum_{d|n} d \cdot N_d$$

$f(n) = \sum_{d|n} g(d)$ $\quad$ $\mu(1)=1$
$\mu(p_1 \dots p_d) = (-1)^d$
$\mu(\dots) = 0$
} möbius function

möbius inversion ↓

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

so, $p^n = \sum_{d|n} d \cdot N_d$

$$\Rightarrow n \cdot N_n = \sum_{d|n} \mu(d) p^{n/d}$$

if $\mathbb{F}_3$ i.e $p=3$ as $N \leq 5 \rightarrow N_1, N_2, N_3, N_4, N_5$ and add all

also N_q q = prime

$$q N_q = \sum_{d|q} \mu(d) p^{q/d} = \mu(1)p^q + \mu(q)p^1$$
$$= p^q - p$$

$$\Rightarrow N_q = \frac{p^q - p}{q}$$

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

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \frac{1}{\sqrt{2}+\sqrt{3}} \times \frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \sqrt{3}-\sqrt{2}$$

$\alpha^4 = 2$
$f(x) = p(x)q(x) + r(x)$

11. $K = \mathbb{R}(X + \frac{1}{X})$ $\quad$ $M = \mathbb{R}(X)$ $\quad$ $\alpha = X$ $\quad$ $[M:K] = 2$

as $X \notin \mathbb{R}(X+\frac{1}{X})$ as if it was then

$M = \mathbb{R}(X)$ $\quad$ $t^2 - (X+\frac{1}{X})t + 1$
|
$K = \mathbb{R}(X+\frac{1}{X})$ $\quad$ 2 degree polynomial
X is root

$[R(x): R(x+\frac{1}{x})] \leq 2$

$x = \frac{f(x+y_x)}{g(x+y_x)}$ if $x \in R(x+\frac{1}{x})$

$\frac{1}{x} = \frac{f(\frac{1}{x}+x)}{g(\frac{1}{x}+x)} = x$ but $x \neq \frac{1}{x}$ so $x \notin R(x+\frac{1}{x})$

$\Rightarrow [R(x): R(x+\frac{1}{x})] = 2$

$R[x]$ — $R[x^2+\frac{1}{x^2}]$ $\to (x+\frac{1}{x})^2 - 2$ so,

$R[x]$ — $R[x+\frac{1}{x}]$ (2) — $R[x^2+\frac{1}{x^2}]$ (2) as $x^2+\frac{1}{x^2} = (x+\frac{1}{x})^2 - 2$

$x^2+\frac{1}{x^2} = t^2-2$

and $x+\frac{1}{x} \notin R[x^2+\frac{1}{x^2}]$

as if so then

$x+\frac{1}{x} = \frac{f(x^2+\frac{1}{x^2})}{g(x^2+\frac{1}{x^2})}$

$-x-\frac{1}{x} = x+\frac{1}{x}$ not true

14. $\alpha \in K(x) \setminus K$ $\alpha = \frac{p(x)}{q(x)}$ $(p,q)=1$

$n := \max\{\deg p, \deg q\}$

$K(x)$ $\alpha = p(x)/q(x)$

$K(\alpha)$ $\alpha q(x) - p(x) = 0$

$f(t) = \alpha q(t) - p(t) \in K(\alpha)[t]$

x is root of $f(t)$

$\Rightarrow x$ is alg over $K(\alpha$

$f(t) \in K[\alpha][t]$ $\alpha q(t) - p(t) = K[t][\alpha]$

as, $\alpha q(t) - p(t) \in K(\alpha)[t]$

irred $\Leftrightarrow$ ($\because$ gauss)

$f(t) \in K[\alpha][t]$

irred $f(\alpha, t) = g(\alpha, t) h(\alpha, t)$

1. (i) as f is primitive

f is irred in $\mathbb{Z}[x]$ iff f is irred in $\mathbb{Q}[t]$

now, in $\mathbb{Z}/_{2\mathbb{Z}}$: $\bar{f}(x) = x^4 + x + 1$

$\bar{f}(\bar{0}) = \bar{1}$

$\bar{f}(\bar{1}) = \bar{1}$ $\Rightarrow$ $\bar{f}$ has no linear factor in $\mathbb{Z}/_{2\mathbb{Z}}[x]$

then if f is reducible in $\mathbb{Z}/_{2\mathbb{Z}}[x]$ then

f is combination of 2, 2deg irreducible in $\mathbb{Z}/_{2\mathbb{Z}}[x]$

but out of $x^2+x+0 \to$ reducible, only x^2+x+1 is irreducible
$x^2+x+1 \to$ irreducible
$x^2+0 \to$ reducible
$x^2+1 \to$ reducible

but $(x^2+x+1)(x^2+x+1)$
$= x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1$
$= x^4 + x^2 + 1$
$\neq x^4 + x + 1$

so, $f(x)$ is irreducible in $\mathbb{Z}/_{2\mathbb{Z}}[x]$

$\Rightarrow f(x)$ irreducible in $\mathbb{Z}[x]$ ($\because$ mod p irreducibility)

(ii) $x^5 + x^2 + 1 = f(x)$
then as f is primitive

$f(x)$ irred in $\mathbb{Q}[x]$ iff it is in $\mathbb{Z}[x]$

now $\bar{f}(x)$ in $\mathbb{Z}/_{2\mathbb{Z}}$ is $x^5 + x^2 + 1 = \bar{f}(x)$

$\bar{f}(\bar{0}) = \bar{1}$, $\bar{f}(\bar{1}) = \bar{1}$

$\Rightarrow f$ has no linear factor

$\Rightarrow f$ is product of two polynomials in $\mathbb{Z}/_{5\mathbb{Z}}[t]$
of deg 2 and deg 3
both irreducible

$\bar{f}(x) = (x^2 + x + 1)(x^3 + ax^2 + bx + c) = x^5 + x^2 + 1$

from (i) only irred 2 deg

$c = \bar{1}$

then $x + bx = 0$, $b = \bar{1}$

$x^5 + x^4 + ax^3 = x^2$, $a = \bar{1}$

$\Rightarrow x^3+x^2+x+1 = g(x) \quad g(\bar{1})=\bar{0}$

but still this is not irreducible, as 3 deg with linear factor

$\Rightarrow f$ is irred in $\mathbb{Z}/2\mathbb{Z}[x]$

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

2. $f \in \mathbb{Q}[t]$ monic
$g \in \mathbb{Z}[t]$ monic $\Rightarrow g \in \mathbb{Q}[t]$ monic

$f \mid g$ in $\mathbb{Q}[t]$

$g = f.h$ for $f \in \mathbb{Q}[t]$, $h \in \mathbb{Q}[t]$

as f is monic, h also monic

now, $f.h \in \mathbb{Z}[t]$

now, by theorem done in class, $\exists\, n_1, n_2 \in \mathbb{N}$ s.t

$f = \frac{1}{n_1}\tilde{f}$, $h = \frac{1}{n_2}\tilde{h}$ where $\tilde{f}, \tilde{h}$ are primitive in $\mathbb{Z}[t]$

$\Rightarrow f.h = \frac{1}{n_1 n_2}\tilde{f}\tilde{h}$ as $\tilde{f}, \tilde{h}$ both primitive

by gauss, $\tilde{f}\tilde{h}$ also primitive

$\Rightarrow \frac{1}{n_1 n_2}\tilde{f}\tilde{h} = g \in \mathbb{Z}[t]$

$\Rightarrow \tilde{f}\tilde{h} = g\,(n_1 n_2)$

$\Rightarrow (n_1 n_2)\, g$ is primitive as $\tilde{f}\tilde{h}$ primitive

$\Rightarrow (n_1, n_2) = 1$ as gcd(coef of g) $= 1$

(∵ g is primitive as monic)

$\Rightarrow n_1 = n_2 = 1$

so, $f = \tilde{f} \in \mathbb{Z}[t]$

3. deg ≤ 5 in $\mathbb{F}_3[t]$

no of irred of deg $n = N_n = \frac{1}{n}\sum_{d \mid n} \mu(d)\,(p)^{n/d}$

$$\mu(d) = \begin{cases} 1 & ; \ d = 1 \\ (-1)^k & ; \ d = p_1 \cdots p_k \text{ all distinct} \\ 0 & ; \ \text{otherwise} \end{cases}$$

$N_1 = \frac{1}{1}\mu(1)(3)^{1/1} = 3$

$N_2 = \frac{1}{2}\left[\mu(1)(3)^2 + \mu(2)(3)^1\right]$

$= \frac{1}{2}\left[3^2 - 3\right] = 3$

$N_3 = \frac{1}{3}\left[3^3 - 3\right] = 3^2 - 1 = 8$

$$N_4 = \frac{1}{4}\left[3^4 - 3^2 + 0\right] = 18$$

$$N_5 = \frac{1}{5}\left[3^5 - 3\right] = 48$$

$$N_1 + N_2 + N_3 + N_4 + N_5 = 80$$

4. $\mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$

$|<\infty$

$\mathbb{Q}(\sqrt[3]{2})$ $f(x) = x^2 - 2$

$|<\infty$ $f(x) = x^3 - 2$

$\mathbb{Q}$

$\Rightarrow [\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) : \mathbb{Q}] < \infty$

$\Rightarrow [\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}) : \mathbb{Q}] < \infty$

$\sqrt{\pi}+2$ is not algebraic as if so

then $\exists f(x) \in \mathbb{Q}[x]$ s.t

$f(\sqrt{\pi}+2) = 0$

$\Rightarrow f(x+2) = g(x) \in \mathbb{Q}[x]$ s.t

$g(\sqrt{\pi}) = 0$

$\Rightarrow \sqrt{\pi}$ is algebraic

but then $\sqrt{\pi} \times \sqrt{\pi} = \pi$ algebraic ($\because$ closed under multiplication)

π is not algebraic

so, $\sqrt{\pi}+2$ not algebraic

similarly if $(1+e)^2$ is algebraic then

$f((1+e)^2) = 0$ for some $f \in \mathbb{Q}[x]$

let $f(x^2) = g(x) \in \mathbb{Q}[x]$

$\Rightarrow g(1+e) = 0 \Rightarrow 1+e$ is algebraic

$\Rightarrow 1+e-1$ is algebraic ($\because$ closed under subtraction)

$\Rightarrow e$ is algebraic, this is a contradiction

so, $(1+e)^2$ not algebraic

$\pi^2 + e^2$, πe not as can be by polynomial with rational coeff

so not algebraic

5. $a+bi \in \mathbb{C}$ algebraic iff a, b algebraic

($\Rightarrow$) $a+bi$ algebraic then $p(z) = 0$

for some $p \in \mathbb{Q}[t]$ $z = a+ib$

$\overline{p(z)} = p(\bar{z}) = 0$

$\Rightarrow a - ib$ is algebraic

$\Rightarrow \frac{a - ib + a + ib}{2}$ algebraic ($\because \overline{\mathbb{Q}}$ is a field)

$\Rightarrow a$ is algebraic

similarly b is algebraic

($\Leftarrow$) a, i, b all algebraic as $x^2 + 1 = 0$, $(i)^2 + 1 = 0$

$\Rightarrow a + ib$ is algebraic

6. $r \in \mathbb{Q}$, $\sin r\pi$, $\cos r\pi$

let $r = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$

then $e^{i\pi(r)} = e^{i\pi(m/n)}$

$= z$

then $(z)^n = e^{i\pi m}$

$\Rightarrow (z)^{2n} = e^{2m\pi i} = 1$

or $f(t) = t^{2n} - 1$ has root $z = e^{i\pi(m/n)} = e^{i\pi r}$

$\Rightarrow \cos r\pi + i \sin r\pi$ is algebraic

then from above $\cos r\pi$, $\sin r\pi$ is algebraic

7. $L = \mathbb{Q}[\alpha]$ $\alpha = \sqrt[3]{2}$ $t^3 - 2 = f(t)$ monic irred

then, $\frac{1}{\alpha} = \frac{\alpha^2}{\alpha^3} = \frac{\alpha^2}{2}$

$\alpha + 1 \overline{)\ \alpha^2 - \alpha + 1}$

$\alpha^3 - 2$

$\alpha^3 + \alpha^2$

$-\alpha^2 - 2$

$-\alpha^2 - \alpha$

$\alpha - 2$

$\alpha + 1$

-3

$\Rightarrow (\alpha + 1)(\alpha^2 - \alpha + 1) - 3 = \alpha^3 - 2$

$\Rightarrow (\bar{\alpha} + 1)(\bar{\alpha}^2 - \bar{\alpha} + 1) - 3 = 0$

$\Rightarrow (1 + \bar{\alpha})^{-1} = \frac{(\bar{\alpha}^2 - \bar{\alpha} + 1)}{3}$

$\alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$

$\frac{1}{\alpha^2 + \alpha + 1} = \frac{\alpha - 1}{\alpha^3 - 1} = \alpha - 1$

$\frac{1 + \alpha}{\alpha^2 + \alpha + 1} = (\alpha - 1)(\alpha + 1)$

$= \alpha^2 - 1$

8. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{3}-\sqrt{2}}{3-2} = \sqrt{3}-\sqrt{2}$$

$$\frac{1}{1+\sqrt{2}+\sqrt{3}} \times \frac{((1+\sqrt{2})-\sqrt{3})}{((1+\sqrt{2})-\sqrt{3})} = \frac{1+\sqrt{2}-\sqrt{3}}{(1+\sqrt{2})^2-3}$$

$$= \frac{1+\sqrt{2}-\sqrt{3}}{1+2+2\sqrt{2}-3}$$

$$= \frac{\sqrt{2}+2-\sqrt{6}}{4}$$

$$= \frac{1}{2} + \frac{1}{4}\cdot\sqrt{2} + 0\cdot\sqrt{3} - \frac{1}{4}\sqrt{6}$$

$$\frac{\sqrt{2}+\sqrt{3}}{1+\sqrt{2}+\sqrt{3}+\sqrt{6}} = \frac{(\sqrt{2}+\sqrt{3})}{(1+\sqrt{2})(1+\sqrt{3})}$$

$$= \frac{(\sqrt{2}+\sqrt{3})(\sqrt{2}-1)(\sqrt{3}-1)}{(2-1)(3-1)}$$

$$= \frac{1}{2}\left[(\sqrt{2}+\sqrt{3})(\sqrt{6}-\sqrt{2}-\sqrt{3}+1)\right]$$

$$= \frac{1}{2}\left[3\sqrt{3}-5-2\sqrt{6}+4\sqrt{2}\right]$$

9. $L = \mathbb{F}_2(\alpha)$ $\alpha^4+\alpha+1=0$

$\alpha^4+\alpha=-1=1$

$\alpha(\alpha^3+1)=1$

$\Rightarrow \frac{1}{\alpha} = \alpha^3+1$

$$(\alpha^2+\alpha+1)(\alpha^2+\alpha)$$

$$= \alpha^4+\alpha^3+\alpha^3+\alpha^2+\alpha^2+\alpha$$

$$= \alpha^4+\alpha = -\alpha+\alpha+1$$

$$\Rightarrow (\alpha^2+\alpha+1)^{-1} \overset{=1}{=} \alpha^2+\alpha$$

$$\alpha^5 = \alpha(\alpha^4) = \alpha(\alpha+1) = \alpha^2+\alpha$$

$$\alpha^{15} = (\alpha^2+\alpha)^3$$

$$= (\alpha^2+\alpha)(\alpha^2+\alpha)^2$$

$$= (\alpha^2+\alpha)(\alpha^4+\alpha^2)$$

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

$$= \alpha^4+\alpha^3+\alpha^2+\alpha^3+\alpha^2+\alpha = 1$$

10.(a) $\alpha = \sqrt{2} + \sqrt[3]{2}$ over $\mathbb{Q}$

$(\alpha - \sqrt{2})^3 = 2$

$\Rightarrow \alpha^3 - 2\sqrt{2} - 3(\alpha)(\sqrt{2})(\alpha - \sqrt{2}) = 2$

$\Rightarrow \alpha^3 - 2\sqrt{2} - 3\sqrt{2}\alpha^2 + 6\alpha = 2$

$\Rightarrow \alpha^3 + 6\alpha - 2 = \sqrt{2}(2 + 3\alpha^2)$

$\Rightarrow (\alpha^3 + 6\alpha - 2)^2 = 2(2 + 3\alpha^2)^2$

$\Rightarrow \alpha^6 + 36\alpha^2 + 4 + 12\alpha^4 - 24\alpha - 4\alpha^3 = 2(4 + 9\alpha^4 + 12\alpha^2)$
$= 8 + 18\alpha^4 + 24\alpha^2$

$\alpha^6 - 6\alpha^4 - 4\alpha^3 + 12\alpha^2 - 24\alpha - 4 = 0$

now by construction irreducible + monic

$\alpha = \sqrt[3]{\sqrt{3} + 1}$

$\alpha^3 = \sqrt{3} + 1$

$\alpha^3 + 1 = \sqrt{3}$

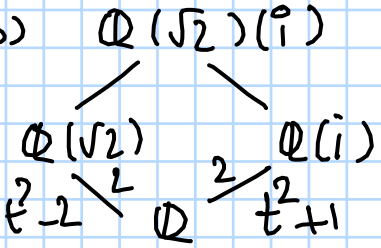
$(\alpha^3 - 1)^2 = 3$

$\Rightarrow \alpha^6 + 1 - 2\alpha^3 = 3$

$\Rightarrow \alpha^6 - 2\alpha^3 - 2 = 0$

by construction irreducible + monic

(b)



$\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{2})(i)$
$\mathbb{Q}(i) \neq \mathbb{Q}(\sqrt{2})(i)$
as $\sqrt{2} \notin \mathbb{Q}(i)$, $i \notin \mathbb{Q}(\sqrt{2})$ } Both trivial

so, $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(i)] > 1$

and $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(i)] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
(∵ theorem done in class)

$\Rightarrow [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(i)] = 2$

so, minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(i)$ has deg 2

$\Rightarrow t^2 - 2 \in \mathbb{Q}(i)[t]$ is a polynomial
① which is monic
② has deg 2

has root $\sqrt{2}$,
also, if not irreducible
then
$t^2 - 2 = (t + \alpha)(t + \beta)$ $\alpha, \beta \in \mathbb{Q}(i)$
$\alpha = a + ib$
$\beta = c + id$

$\Rightarrow t^2-2 = (t+a+ib)(t+c+id)$
$= t^2 + ct + idt + at + ac + adi + ibt + ibc - d$

$c + id + a + ib = 0$
$a + c = 0 \quad b + d = 0$
$ac + adi + ibc - d = -2$
$ad + bc = 0$
$a = -c \quad b = -d$
$-ab - ab = 0 \Rightarrow a = 0, b = 0$
this is a contradiction

so, t^2-2 is monic, ind s.t $\alpha^2 - 2 = 0$

$\alpha = \sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$

$t^3 - 2$ is s.t ① monic
② $\alpha^3 - 2 = 0$
and if $t^3 - 2 = (t+\alpha)(t^2 + \beta t + \varphi)$

$\alpha, \beta, \varphi \in \mathbb{Q}(\sqrt{2})$
$\alpha = a_1 + a_2\sqrt{2}$
$\beta = b_1 + b_2\sqrt{2}$
$\varphi = c_1 + c_2\sqrt{2}$

$(t + a_1 + \sqrt{2}a_2)(t^2 + b_1 t + b_2\sqrt{2}t + c_1 + c_2\sqrt{2}) = t^3 - 2$

$a_1 + \sqrt{2}a_2 + b_1 + b_2\sqrt{2} = 0 \quad \{1, \sqrt{2}\}$ lin ind
$c_1 + c_2\sqrt{2} + (a_1 + \sqrt{2}a_2)^2 (1) = 0$

$a_1 + b_1 = 0 \quad a_2 + b_2 = 0$
$(a_1 + \sqrt{2}a_2)(c_1 + c_2\sqrt{2}) = -2$
$\Rightarrow (a_1 + \sqrt{2}a_2)^3 = -2$
$\Rightarrow a_1 + \sqrt{2}a_2 = -(2)^{1/3}$
$\Rightarrow -a_1 - \sqrt{2}a_2 = (2)^{1/3}$

but $(2)^{1/3} \notin \mathbb{Q}(\sqrt{2})$ this is a contradiction

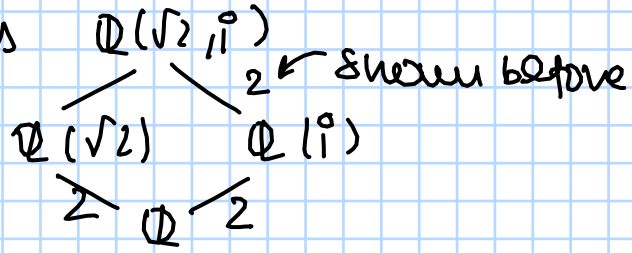
as if $(2)^{1/3} \in \mathbb{Q}(\sqrt{2})$ then

$2^{1/3} = \alpha + \beta\sqrt{2} \quad \alpha, \beta \in \mathbb{Q}$
$\Rightarrow 2 = \alpha^3 + 2\beta^3\sqrt{2} + 3\alpha\beta(\alpha + \beta\sqrt{2})$

then to fix rational = irrational
$\beta = 0$
this is a contradiction

11. (a) $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]=4$

as



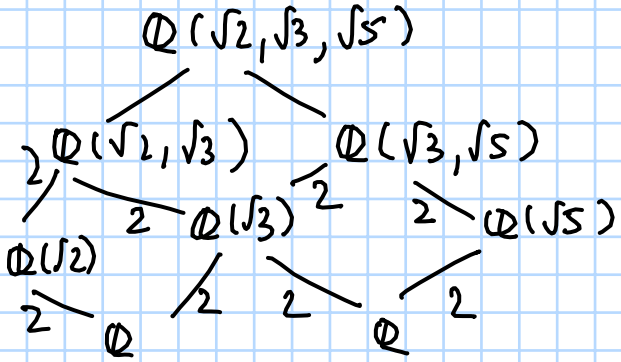
$\Rightarrow [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]=4$ by tower property

basis of $\mathbb{Q}(\sqrt{2})=\{1,\sqrt{2}\}$

basis of $\mathbb{Q}(i)=\{1,i\}$

basis of $\mathbb{Q}(\sqrt{2})(i)=\{1,i,\sqrt{2}i,\sqrt{2}\}$

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



$\sqrt{2}\notin\mathbb{Q}(\sqrt{3})\Rightarrow[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})]>1$

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

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

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

as if so, then $\sqrt{5}=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

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

$$5=a^2+2b^2+3c^2+2ab\sqrt{2}+2ac\sqrt{3}+\cdots$$

$a^2+2b^2+3c^2$: Rational

$2ab\sqrt{2}+2ac\sqrt{3}+\cdots$: irrational

all $ab=0$

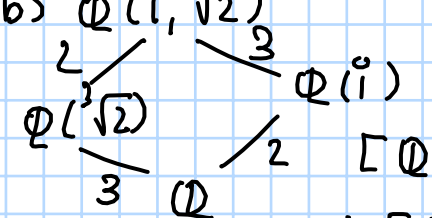
$ab=0$, $bc=0$, $\vdots$

this is a contradiction

so, similar to before $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}]=8$

basis is just combination of $\{1,\sqrt{2}\}$ $\{1,\sqrt{3}\}$ $\{1,\sqrt{5}\}$

(b)



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

$\Rightarrow[\mathbb{Q}(i,\sqrt[3]{2}):\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]\leq 6$

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

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

$= 2[\mathbb{Q}(i,\sqrt[3]{2}):\mathbb{Q}(i)] < 6$

$\Rightarrow 3 \mid [\mathbb{Q}(i,\sqrt[3]{2}):\mathbb{Q}(i)]$

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

So, $[\mathbb{Q}(\underset{3}{\sqrt[3]{2}}, \underset{2}{i}):\mathbb{Q}] = 6$

& basis is combination of $\{1,i\}$ and $\{1,(2)^{1/3},(2)^{2/3}\}$

$\mathbb{Q}(\sqrt[3]{2}+2\sqrt[3]{4})$

$= \mathbb{Q}(\underbrace{\sqrt[3]{2}+2(\sqrt[3]{2})^2}_{\alpha})$

now as $\alpha \in \mathbb{Q}(\sqrt[3]{2})$

$\Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\underset{\beta}{\sqrt[3]{2}})$

also, $\alpha = \beta + 2\beta^2$

$\alpha^2 = \beta^2(1+2\beta)^2 = \beta^2(1+4\beta^2+4\beta)$

$\alpha^2 = \beta^2 + 8\beta + 8$

$\frac{\alpha}{2} = \frac{\beta}{2} + \beta^2$

$\alpha^2 = \left(\frac{\alpha}{2} - \frac{\beta}{2}\right) + 8\beta + 8$

$2\alpha^2 = \alpha - \beta + 16\beta + 16$

$2\alpha^2 - \alpha = 15\beta + 16$

$2\alpha^2 - \alpha - 16 = 15\beta$

$\beta = \frac{2\alpha^2 - \alpha - 16}{15}$

$\Rightarrow \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$

So, $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$

i.e $\mathbb{Q}(\alpha) = \mathbb{Q}((2)^{1/3})$

$[\mathbb{Q}(\alpha):\mathbb{Q}] = 3, \quad \{1, \beta, \beta^2\}$

(c) $\mathbb{R}(X)$ and $\mathbb{R}(X+\frac{1}{X})$ $\qquad$ $\mathbb{R}(X)$

$\mathbb{R}(X+\frac{1}{X})$

if $X \in \mathbb{R}(X+\frac{1}{X})$ then

$$X = \frac{f\left(X+\frac{1}{X}\right)}{g\left(X+\frac{1}{X}\right)}$$

$$\Rightarrow \frac{1}{X} = \frac{f\left(X+\frac{1}{X}\right)}{g\left(X+\frac{1}{X}\right)}$$

$\Rightarrow \frac{1}{X} = X$ this is a contradiction

so, $[\mathbb{R}(X) : \mathbb{R}(X+\frac{1}{X})] > 1$

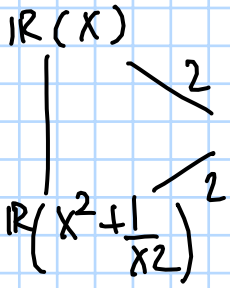
now, as $t^2 - \left(X+\frac{1}{X}\right)t + 1 = f(t) \in \mathbb{R}\left(X+\frac{1}{X}\right)[t]$

s.t $f(X) = 0$

$\Rightarrow [\mathbb{R}(X) : \mathbb{R}(X+\frac{1}{X})] \leq 2$

$\Rightarrow [\mathbb{R}(X) : \mathbb{R}(X+\frac{1}{X})] = 2$

so, $\{1, X\}$ basis



now, if $X+\frac{1}{X} = \frac{f\left(X^2+\frac{1}{X^2}\right)}{g\left(X^2+\frac{1}{X^2}\right)}$

then $-X-\frac{1}{X} = \frac{f\left(X^2+\frac{1}{X^2}\right)}{g\left(X^2+\frac{1}{X^2}\right)}$

but $-X-\frac{1}{X} \neq X+\frac{1}{X}$

also, $t^2 - \left(X^2+\frac{1}{X^2}\right) - 2 = 0$

is s.t $\left(X+\frac{1}{X}\right)$ is a root

so, from previous proof $[\mathbb{R}(X+\frac{1}{X}) : \mathbb{R}(X^2+\frac{1}{X^2})] = 2$

$\Rightarrow [\mathbb{R}(X) : \mathbb{R}\left(x^2 + \frac{1}{x^2}\right)] = 4$

$\{1, X, X^2, X^3\}$ basis as lin ind

(d) $\mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$ over $\mathbb{Q}(\sqrt{3})$

$\alpha = \sqrt[3]{1+\sqrt{3}}$

$\alpha^3 = 1+\sqrt{3}$

$\alpha^3 - 1 - \sqrt{3} = 0$

So, $f(t) = t^3 - 1 - \sqrt{3} \in \mathbb{Q}[\sqrt{3}][t]$

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

also, f is irreducible ← field

as $\frac{\mathbb{Q}(\sqrt{3})}{\langle \sqrt{3}+1 \rangle} \cong \mathbb{Q}$ field

$\Rightarrow \sqrt{3}+1$ prime in $\mathbb{Q}(\sqrt{3})$

$\Rightarrow$ by Eisenstein criterion f is irreducible

So, $[\mathbb{Q}(\sqrt[3]{1+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})] = 3$

α

$\{1, \alpha, \alpha^2\}$ basis

(e) $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$ $\quad \alpha^4 + \alpha + 1 = 0$

$f(t) = t^4 + t + 1$ irreducible monic over $\mathbb{F}_2(t)$ same before

So, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$

$\Rightarrow \{1, \alpha, \alpha^2, \alpha^3\}$ basis

(f) $\mathbb{F}_3(\alpha)$ $\quad \alpha^3 + \alpha^2 + 2 = 0$

$f(t) = t^3 + t^2 + 2$

$f(\bar{0}) = \bar{2}$

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

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

f deg ≤ 3 irred iff no roots in field

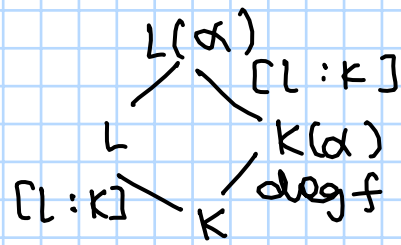
So, f is irreducible

$\Rightarrow [\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$

$\{1, \alpha, \alpha^2\}$ basis

12. To prove: $f \in K[x]$ irreducible over K and L/K is field extension with $\deg(f)$ and $[L:K]$ relatively prime then f is irreducible over L

proof:



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

$[L(\alpha):L] \leq [K(\alpha):K] = \deg f$ ($\because$ done in class)

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

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

$[L(\alpha):L][L:K] = \deg f\ [L(\alpha):K(\alpha)]$

$\Rightarrow [L:K] \mid [L(\alpha):K(\alpha)]$

$\leq [L:K]$

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

$\Rightarrow [L(\alpha):L] = \deg f$

also if g is minimal polynomial of α in $L[t]$ then

as f is irreducible, $\tilde{f} = f/\alpha$ be monic $\alpha \in K$

as $\tilde{f} \in K[t] \subseteq L[t]$

irreducible $\Rightarrow g \mid \tilde{f}$

$\deg g = \deg \tilde{f} = \deg f$

$\Rightarrow g = \tilde{f}$ as both monic

$\therefore$ g is irreducible over $L[t]$

13.



basis $= \{1, \alpha\}$

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

now, $\alpha^2 + b\alpha + c = 0$ for some $b_1 \in \mathbb{Q}$ (α not in $\mathbb{Q}$)

also let $b = \frac{b_1}{b_2}$ $c = \frac{c_1}{c_2}$

$\alpha^2 + \frac{b_1}{b_2}\alpha + \frac{c_1}{c_2} = 0 \Rightarrow k_1\alpha^2 + k_2\alpha + k_3 = 0$ $k_1, k_2, k_3 \in \mathbb{Z}$, $k_1 \neq 0$

$\Rightarrow \alpha = \frac{-k_2 \pm \sqrt{k_2^2 - 4k_1k_3}}{2}$

↑ not in $\mathbb{Q}$

so, $K = \mathbb{Q}(\sqrt{k_2^2 - 4k_1k_3})$

let $d = k_2^2 - 4k_1k_3$

square free as $\alpha \notin \mathbb{Q}$

if $\exists\, d_1, d_2$ s.t

$K = \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$

then $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_2}) \Rightarrow \sqrt{d_1} = \alpha + \beta\sqrt{d_2}$

$\Rightarrow d_1 = \alpha^2 + \beta^2 d_2 + 2\alpha\beta\sqrt{d_2}$

$\Rightarrow \underbrace{d_1 - \alpha^2 - \beta^2 d_2}_{\text{rational}} = \underbrace{2\alpha\beta\sqrt{d_2}}_{\text{irrational}}$

$\Rightarrow \alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$

$\beta = 0$ not possible, so $\alpha = 0$

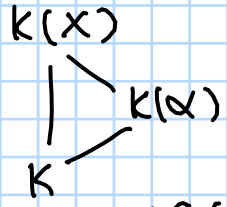
also $d_1 - \beta^2 d_2 = 0$

$\Rightarrow d_1 = \beta^2 d_2$ both square free

$\Rightarrow d_1/d_2 = \beta^2 = 1$

$\Rightarrow d_1 = d_2$

14.



$\alpha = \frac{p(X)}{q(X)}$ $\quad p, q \in K[X]$

$\gcd(p, q) = 1$

$\alpha q(X) - p(X) = 0$

i.e $f(t) = \alpha q(t) - p(t) \in K[\alpha][t]$

if $\exists\, g, h$ s.t $g(t)h(t) = f(t)$

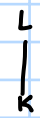
$g \mid q$ and $g \mid p$ but $\gcd(q, p) = 1$

$\Rightarrow f$ is irreducible over $K[\alpha][t]$

$\Rightarrow f$ is irreducible over $k(\alpha)[t]$

so, $\deg f = \max\{\deg g, \deg p\} = [k(X) : k(\alpha)]$

15.





(a) $\alpha \in M_1M_2$ then $\alpha = f(\alpha_1, \alpha_2, \ldots \alpha_m, \beta_1, \beta_2, \ldots \beta_n)$

for $f \in K[t_1, t_2, \ldots t_{m+n}]$

$\alpha_1, \alpha_2, \ldots \alpha_m \in M_1$ ($\because$ by defn of M_1M_2)

$\beta_1, \beta_2, \ldots \beta_n \in M_2$

now, as $\{\alpha_1, \alpha_2, \ldots \alpha_m, \beta_1, \ldots \beta_n\}$ algebric over K

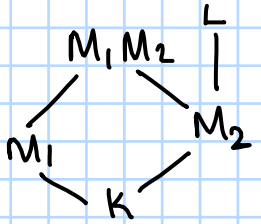
$\Rightarrow f(\alpha_1, \alpha_2, \ldots \alpha_m, \beta_1, \ldots \beta_n)$ algebric over k

($\because$ algebric elements form a field)

$\Rightarrow \alpha$ is algebric

(b) now if $[M_1 : K] < \infty$

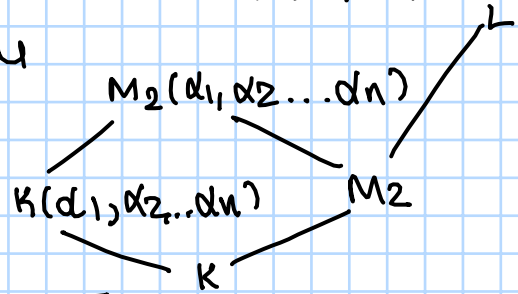
$[M_2 : K] < \infty$



now, $M_1 = K(\alpha_1, \alpha_2, \ldots \alpha_n)$

$M_2 = K(\beta_1, \beta_2, \ldots \beta_m)$

then



$[M_2(\alpha_1) : M_2] \leq [K(\alpha_1) : K]$

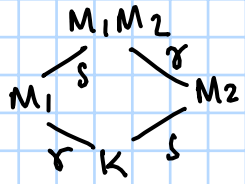
$[M_2(\alpha_1)(\alpha_2) : M_2(\alpha_1)] \leq [K(\alpha_1)(\alpha_2) : K(\alpha_1)]$

$\vdots$

$\Rightarrow [M_1M_2 : M_2] \leq [M_1 : K] < \infty$

$\Rightarrow [M_1M_2 : K] < \infty$

(c)



$[M_1M_2 : M_2][M_2 : K]$ $< \infty$ from before

$= [M_1M_2 : M_1][M_1 : K]$

$< \infty$ from before

$\Rightarrow [M_1 : K] \mid [M_1M_2 : M_2] \leq [M_1 : K]$

done before

$\Rightarrow [M_1M_2 : M_2] = [M_1 : K]$

similarly $[M_1M_2 : M_1] = s$

so, $[M_1M_2 : K] = rs$ by tower

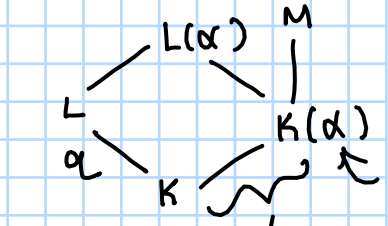
also, $[M_1 \cap M_2 : K][M_1M_2 : K] = [M_1 : K][M_2 : K]$

$\Rightarrow [M_1 \cap M_2 : K] rs = r.s$

$\Rightarrow [M_1 \cap M_2 : K] = 1$

$\Rightarrow M_1 \cap M_2 = K$ ($\because$ theorem done in class)

16. $f \in K[x]$ irreducible of deg p (p is prime)



let minimal polynomial of α over $K = f$ (by scaling constants)

then minimal polynomial of α over $L = g$

$\min_K \alpha = f$

$\min_L \alpha = g$

now, $\psi : K[t] \longrightarrow M$

$\cap\, t \longmapsto \alpha$

$\tilde{\psi} : L[t]$

$t \longmapsto \alpha$

then, $h(t) \xrightarrow{\psi} h(\alpha)$ commutes

$h(t) \xrightarrow{\tilde{\psi}} h(\alpha)$

$\Rightarrow \ker(\psi) \subseteq \ker(\tilde{\psi})$

$\Rightarrow \langle \min_K \alpha \rangle \subseteq \langle \min_L \alpha \rangle$

$\Rightarrow \langle f \rangle \subseteq \langle g \rangle$

$\Rightarrow g \mid f$

as f is reducible

$\deg g < \deg f = p$

now, $(\deg g)(q) = (p)[L(\alpha) : K(\alpha)]$

$p \mid (\deg g)(q)$ but $p \nmid (\deg g)$ as $\deg g < p$

$\Rightarrow p \mid q \Rightarrow p = q$ as both primes

17. $[K(\alpha): K]$ is odd

$K(\alpha)$ — odd — $K(\alpha^2)$ — odd — K (odd)

also $f(x) = x^2 - \alpha^2 \in K(\alpha^2)[x]$ s.t. $f(\alpha) = 0$

$\Rightarrow [K(\alpha): K(\alpha^2)] \leq 2$ but $\neq 2$ as odd

$\Rightarrow [K(\alpha): K(\alpha^2)] = 1$

$\Rightarrow K(\alpha) = K(\alpha^2)$

$\alpha^2 + \alpha + 1 = 0$ in $\mathbb{Q}[t]$

then trivial to see

$\mathbb{Q}(\alpha^2) = \mathbb{Q}(-1-\alpha) = \mathbb{Q}(\alpha)$

but $[\mathbb{Q}(\alpha^2): \mathbb{Q}(\alpha)] = 2$

as $t^2 + t + 1 = f(t)$ is irreducible in $\mathbb{Q}(\alpha)$

as if not then $t^2 + t + 1 = (t+a)(t+b)$

$= t^2 + (a+b)t + ab$

$a + b = 1$

$ab = 1$

$a + \frac{1}{a} = 1$

$a^2 + 1 = a$

$(a + b\alpha)^2 + 1 = a + b\alpha$

$a^2 + b^2\alpha^2 + 2ab\alpha + 1 = a + b\alpha$

$a^2 - b^2 - b^2\alpha + 2ab\alpha + 1 = a + b\alpha$

$-b^2 + 2ab = b$

$-b + 2a = 1$

$a^2 - b^2 + 1 = a$

$2a - b = 1$

$a^2 - b^2 + 1 = a$

$a^2 - (2a-1)^2 + 1 = a$

$a^2 - (4a^2 + 1 - 4a) + 1 = a$

$-3a^2 + 4a = a$

$-3a + 4 = 1$

$a = 5/3$

$2a - b = 1 \Rightarrow b = 2(5/3) - 3/3$

$b = 7/3$

$a = 5/3 + 7/3\alpha \quad b = 5/3 - 7/3\alpha$

but $a + b \neq 1$ this is a contradiction

18. $\mathbb{C}$ — finite degree

then let L be generated by $\alpha_1 \dots \alpha_n$

$\mathbb{C}(\alpha_1)$ / $\mathbb{C}$ is finite

$\Rightarrow \alpha_1$ is algebric

$\Rightarrow \alpha_1 \in \mathbb{C}$ ($\because \mathbb{C}$ is algebrically closed)

$\Rightarrow C(\alpha_1) = \mathbb{C}$

similarly $\forall i,\ \alpha_i \in \mathbb{C} \Rightarrow L = \mathbb{C}$

19. L / $\mathbb{R}$ ($r \infty$)

now, let L be generated by $\{\alpha_1, \alpha_2 \dots \alpha_n\}$

then if $\alpha_1, \alpha_2 \dots \alpha_n \in \mathbb{R}$
then $L = \mathbb{R}$

if $\exists \alpha_i \in \mathbb{C} \setminus \mathbb{R}$
then $\alpha_i = a + ib$
$\alpha_i - a = ib \in L$
$b \quad \mathbb{C} \subseteq L$

$\Rightarrow L = \mathbb{C}$ ($\because \mathbb{C}$ is algebrically closed) ($\because$ before)

20. $\alpha^4 + \alpha + 1 = f(\alpha)$
irreducible over $\mathbb{Q}$

$\mathbb{Q}(\alpha)$ / $\mathbb{Q}$: $4 \mid 2 \mid 4$ but

then let $\mathbb{Q}(\alpha)$ / M / $\mathbb{Q}$ → basis $\{1, \alpha, \alpha^2, \alpha^3\}$

$[M : \mathbb{Q}] = 2 \Rightarrow M = \mathbb{Q}(\sqrt{d})$
d is squarefree integer

if $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{d})] = 2$ i.e $\sqrt{d} \notin \mathbb{Q}(\alpha)$

then $\exists\ f(x) = x^2 + ax + b$
$a, b \in \mathbb{Q}(\sqrt{d})$
s.t
$0 = \alpha^2 + a\alpha + b$

$-\alpha^2 = (a_1 + \sqrt{d}\, a_2)\alpha + (b_1 + \sqrt{d}\, b_2)$

$-\alpha^2 - a_1\alpha - b_1 = \sqrt{d}(a_2\alpha + b_2)$

$-\alpha^2 - a_1\alpha - b_1 \in \mathbb{Q}(\alpha)$, $a_2\alpha + b_2 \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt{d} \in \mathbb{Q}(\alpha)$
this is a contradiction

21.

$\alpha \in L$ | K

$f(x) \in L[x]$ ↑ well algebraic over K

$f(\alpha) = 0$

$f(x) = \sum_{i=0}^{n} a_i x^i$

L | $K(a_0, a_1 \dots a_n) = E$ | K

$f(x) \in E[x] \Rightarrow \alpha$ is algebraic over E

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

$E(\alpha)$ | $< \infty \Rightarrow \alpha$ is algebraic over K

E | $< \infty$

K

now,

$K(\alpha)$ | $< \infty$ | K

$K(\alpha)$ | $K(\alpha^2)$ | K) finite

$\Rightarrow [K(\alpha^2) : K] < \infty$

$\Rightarrow \alpha^2$ algebraic over K

$K(\sqrt[3]{\alpha})$ | $K(\alpha)$ | K) as $g(t) = t^3 - \alpha \in K(\alpha)[t]$

$[K(\sqrt[3]{\alpha}) : K] \leq 3$

$\Rightarrow [K(\sqrt[3]{\alpha}) : K] < \infty$

$\Rightarrow \sqrt[3]{\alpha}$ is algebraic

22.

L | K $\quad \bar{K} = \{\alpha \in L$ algebraic $/ K$

if $\forall$ α algebraic $/ \bar{K} \in \bar{K}$ then we are done

let $f(t) = a_0 + a_1 t + \cdots a_n t^n \in \bar{K}[t]$

then if α is a root of $f(t)$

then

$$K(a_0, a_1 \ldots a_n, \alpha)$$
$$| \leq \deg f$$
$$K(a_0, \ldots a_n)$$
$$|_K < \infty \quad \text{all algebraic } /K$$

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

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

$\Rightarrow \alpha$ is algebraic $/K$

$\Rightarrow \alpha \in \bar{K}$

Tutorial-5:

last question in midsem was $GL_2(M)$ ← commutative ring, → $\det = 1$

$GL_n(A)$ with $1 \neq 0$

$GL_n(A) = \{ A : n \times n \text{ matrix which is invertible} \}$

$= \{ A : \det(A) = \text{unit in } A \}$ ← this is the definition

$A \xrightarrow{\varphi} B$ ring homomorphism

$GL_n(\varphi) : GL_n(A) \longrightarrow GL_n(B)$

$A = (a_{ij}) \longmapsto (\varphi(a_{ij}))$

$BA = AB = Id$

$\varphi(B)\varphi(A) = \varphi(Id) = Id$

$GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$

$GL_2(\varphi)$

$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ $\quad p > 2$

$A \xrightarrow{\varphi} B$ ← if this becomes surjective

$GL_n(A) \xrightarrow{GL_n(\varphi)} GL_n(B)$

$\det \downarrow$ $\qquad$ $\det \downarrow$

$U(A) \xrightarrow{\varphi} U(B)$

always surjective as $\begin{bmatrix} 1 & 0 \\ & \ddots \\ & & 1 \end{bmatrix} \longrightarrow u$

then $U(A) \longrightarrow U(B)$ ↑ surjective

$U(\mathbb{Z}) = \pm 1$

$U(\mathbb{Z}/p\mathbb{Z}) = \{ \bar{1}, \bar{2}, \ldots \overline{p-1} \}$

this is not possible for $p > 2$

$\mathbb{Z}, p\mathbb{Z}$ is one such case

now, let A: any ring, m: maximal ideal

then, $SL_n(A) \longrightarrow SL_n(A/m)$ is surjective ——— (1)

$\varphi : A \longmapsto A/m$ (surjective map)

now, $\sigma \in GL_n(A)$, $u = \det \sigma \in U(A)$

$\sigma = \begin{pmatrix} u & & \\ & 1 & \\ & & \ddots \end{pmatrix} \sigma_1$ $\qquad \det(\sigma) = u \det(\sigma_1)$

$\Rightarrow \sigma_1 \in SL_n(A)$ $\quad (\because \det(\sigma_1) = 1)$

if we assume ①, then

$$GL_n(A) \xrightarrow{GL_n(\varphi)} GL_n(A/M) \text{ is surjective}$$

$$\text{iff } U(A) \xrightarrow{\varphi} U(A/M) \text{ is surjective}$$

as let $\bar{\sigma} \in GL_n(A/M)$

$\det \bar{\sigma} = \bar{u} \in U(A/M)$

$$\bar{\sigma} = \begin{pmatrix} \bar{u} & 0 \\ 0 & I_{n-1} \end{pmatrix} \underbrace{\begin{pmatrix} \bar{u}^{-1} & \\ & I_{n-1} \end{pmatrix} \bar{\sigma}}_{\sigma_1 \in SL_n(A/M)}$$

($\Rightarrow$) $GL_n(\varphi)$ is surjective

$\Rightarrow \varphi : U(A) \to U(A/M)$ is surjective (this follows from previous)

($\Leftarrow$) Assume $\varphi : U(A) \to U(A/M)$ is surjective

$\Rightarrow \exists u \in U(A)$ s.t $\varphi(u) = \bar{u}$

also by ① $\exists \theta \in SL_n(A)$ s.t $\varphi(\theta) = \sigma_1$

then

$$\begin{pmatrix} u & 0 \\ 0 & I_{n-1} \end{pmatrix} \theta \xrightarrow{\varphi} \bar{\sigma}$$

$\Rightarrow GL_n(A) \xrightarrow{\varphi} GL_n(A/M)$ is surjective

now, lets show ①, $A/M = K$ field

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+\alpha c & b+\alpha d \\ c & d \end{pmatrix}$$

elementary matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \alpha a + b \\ c & \alpha c + d \end{pmatrix}$$

elementary matrices

trivial to see $\begin{pmatrix} 1 & \kappa \\ 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$

i.e $SL_n(A) \to SL_n(A/M)$ lifts elementary matrices

now, $E_n(A)$ = subgroup of $SL_n(A)$ generated by elementary matrices

$$\sigma_{ij}(\alpha)_{i \neq j} = \begin{bmatrix} 1 & & & \\ & \ddots & (\alpha) & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \leftarrow i^{th}, \quad n \times n$$

$$(\sigma_{ij}(\alpha))^{-1} = \sigma_{ij}(-\alpha)$$

If $E_n(A) = SL_n(A)$ for $A \in \{$field, euclidean domain, local ring$\}$

(all are maximal ideals)

$SL_2(K[x,y]) \neq E_2(K[x,y])$

as $K[x,y]$ not ED

$SL_n(K[x_1,x_2..x_n]) = E_n(K[x_1,...x_n])$ $\forall n \geq 3$

} so there are more examples in which $A \in$ {fields, ...}

field:

$$\sigma = \begin{pmatrix} a_{11} \cdots a_{1n} \\ \vdots \\ a_{n1} \cdots a_{nn} \end{pmatrix} \in SL_n(K)$$

$Q_r \sigma \varphi_1 \varphi_2 \ldots \varphi_s = I \Rightarrow \sigma = (Q_1 \ldots Q_r)^{-1}(\varphi_1 \varphi_2 \ldots \varphi_s)^{-1}$

$\Rightarrow \sigma \in E_n(K)$

Q_p: elementary matrices

now, $(a_{11}\ a_{12}\ a_{13} \ldots a_{1n}) \in K^n \setminus (0)$

↑ not the zero vector

as K is a field

wlog $a_{11} \neq 0$ as $a_{11} \neq 0$ we will just do row/column operation to make $a_{11} \neq 0$ (if it was 0)

then

$$\sigma \begin{pmatrix} a_{11} & a_{12} \ldots & a_{1n} \\ a_{21} & & \vdots \\ a_{31} & & \vdots \\ \vdots & & \\ a_{n1} & \cdots\cdots & a_{nn} \end{pmatrix} \rightarrow \begin{pmatrix} a_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & \square \\ 0 & \end{pmatrix} \rightarrow \text{By induction}$$

and for $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \rightarrow \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} \rightarrow \begin{pmatrix} a-(b(ab^{-1})-1) & b \\ -(b(ab^{-1})-1) & b \end{pmatrix}$

$\in SL_2(K)$ $b = a^{-1}$

$$= \begin{pmatrix} 1 & b \\ -a+1 & b \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ * & c \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 0 \\ 0 & c' \end{pmatrix}$$

$c' = 1$ as $\det = 1$

so true for n, then by induction true

local ring: $\exists$ one element in $(a_{11}\ a_{12}\ a_{13} \ldots a_{1n})$ not in maximal ideal

wlog a_{11} is unit

then case $n=2$ $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is seen

ED: $\begin{pmatrix} a_{11} \cdots a_{1n} \\ \vdots \quad \vdots \\ a_{n1} \cdots a_{nn} \end{pmatrix}$ $\exists N: A \rightarrow \mathbb{N}_{\geq 0}$ norm

a_{1b}

$a = qb + r$

$r \neq 0$ or $N(r) < N(b)$

now, from $(a_{11}\ a_{12} \ldots a_{1n})$ → pick the element with smallest

norm

wlog $N(a_{11})$ is smallest among all $N(a_{ij})$ (as we can interchange rows/cols)

then $a_{12} = q a_{11} + r$ (or $r = 0$ or $N(r) < N(a_{11})$)

$$\begin{pmatrix} a_{11} & \cdots \\ \vdots & \\ \cdots & \end{pmatrix} \to \begin{pmatrix} r_{11} & r_{12} & \cdots \\ \vdots & & \\ \cdots & & \end{pmatrix}$$

pick smallest N $\longrightarrow$ then $N(r_{11}) = 1$ (wlog)

as we can interchange rows/cols

i.e r_{11} non to be unit as all non-zero

then $\begin{pmatrix} a_{11} & 0 \cdots 0 \\ 0 & \square \\ \vdots & \\ 0 & \end{pmatrix}$ (a_{11} unit) by induction true as $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$E_2(K[x,y])$ is not a normal subgroup of $SL_2(K[x,y])$

but $E_n(A)$ is a normal subgroup of $SL_n(A)$ $n \geq 3$

1. $\phi : R \to S$

(a) r unit r^{-1} exist

then $\phi(r) \cdot \phi(r^{-1}) = \phi(1)$

$(\phi(r))^{-1} = \phi(r^{-1})$

$\Rightarrow \phi(r)$ is a unit

(b) $S = \{1\}$ $R = (\mathbb{Z}, +, \cdot)$

then

$\phi : \mathbb{Z} \to S$

s.t $\phi(2) = 1$ (1: unit; 2: not a unit)

(c) $R = \mathbb{Z}/6\mathbb{Z}$ $S = \mathbb{Z}/3\mathbb{Z}$

then $r = \bar{2} \in \mathbb{Z}/6\mathbb{Z}$ s.t

$a = \bar{3}$ $\phi = id$

$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ but $\phi(r) = \bar{2}$ not zero divisor as $\mathbb{Z}/p\mathbb{Z}$ is ID

(d) $R = \mathbb{Z}$ $S = \mathbb{Z}/6\mathbb{Z}$

$\phi : R \to S$ $\phi(x) = \bar{x}$

$r = 2$ now divisor but $\bar{2} \cdot \bar{3} = \bar{0}$

(e) $R = \mathbb{Z}$ $S = \mathbb{Q}$ then $\phi : R \to S$ $\phi(x) = x$ trivial $2 \in R, S$

(f) $R=S=\mathbb{Z}$ $\phi(x)=x$

$r=4$ true trivial

(g) $r\neq 0$ $r^n=0$ $n\neq 1,2$

does not exist

$\phi(r^n) \overset{cas}{=} \phi(0)=0=(\phi(r))^n$

(h)

$\phi: \mathbb{Z}\to \mathbb{Z}/4\mathbb{Z}$

$r=2$ $\phi(r)=\bar{r}$

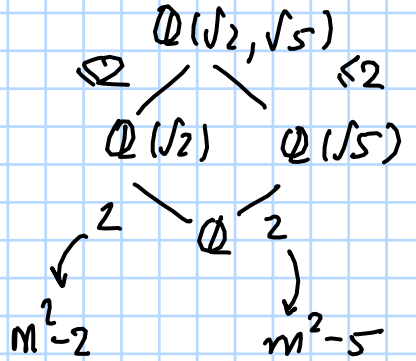
$\phi(12)=\bar{2}$ $\phi(2^8)=(\bar{2})^8=\bar{0}$

2. $f\in K[t]$ $K=\mathbb{Q}$ $\mathbb{Q}(i)$

(a) roots are $\pm\sqrt{2}, \pm\sqrt{5}$

$K=\mathbb{Q}$

$\mathrm{spl}_K f = \mathbb{Q}(\sqrt{2},\sqrt{5})$



≤ 2 but $\sqrt{5}\notin \mathbb{Q}(\sqrt{2})$ as if so then

$5=a^2+2b^2$ $2ab=0$

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

by either include

then by tower, $[\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}]=4$

also basis $\{1,\sqrt{2},\sqrt{5},\sqrt{10}\}$ as linearly independent and spans

$a+\sqrt{2}b+\sqrt{5}c+\sqrt{10}d=0$

$a+\sqrt{2}b+\sqrt{5}(c+\sqrt{2}d)=0$; basis of $\mathbb{Q}(\sqrt{5})$ $\{1,\sqrt{5}\}$

$a+\sqrt{2}b=0 \Rightarrow a=0, b=0$ } basis of $\mathbb{Q}(\sqrt{2})$ $\{1,\sqrt{2}\}$

$c+\sqrt{2}d=0 \Rightarrow c=0, d=0$ }

$\sqrt{2},\sqrt{5}\notin \mathbb{Q}(i) \Rightarrow \mathrm{spl}_{\mathbb{Q}(i)} f = \mathbb{Q}(i,\sqrt{2},\sqrt{5})$

$[\mathbb{Q}(i,\sqrt{2},\sqrt{5}):\mathbb{Q}(i)]=4$, same as above

(b) $t^4+1 \Rightarrow$ $f(t)=0$

$1=e^{2\pi i}$ $\zeta_n=e^{2\pi i/n}$

$\zeta^n=1$ $\zeta^m\neq 1$ $1\leq m<n$

now, $t^4+1=0 \Rightarrow t^8=1 \Rightarrow \zeta_8=e^{2\pi i/8}$ is root

$[\mathrm{spl}(\zeta_8):\mathbb{Q}]=\phi(8)=2^3-2^2=4$

as $\zeta_8 = \frac{1+i}{\sqrt{2}}$ $\operatorname{spl}_{\mathbb{Q}} f = \mathbb{Q}(i,\sqrt{2})$

Basis $= \{1, i, \sqrt{2}, i\sqrt{2}\}$

$\operatorname{spl}_{\mathbb{Q}(i)} f = \mathbb{Q}(\sqrt{2}, i)$ $i \in \mathbb{Q}(i) \Rightarrow [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)] = 2$ basis $\{1, \sqrt{2}\}$

(c) $f = t^4 + 4$ roots $= \{1 \pm i, -1 \pm i\}$

all roots in $\mathbb{Q}(i)$

$\operatorname{spl}_{\mathbb{Q}} f = \mathbb{Q}(i)$ $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ $\{1, i\}$ basis

$\operatorname{spl}_{\mathbb{Q}(i)} f = \mathbb{Q}(i)$ $[\mathbb{Q}(i) : \mathbb{Q}(i)] = 1$ $\{1\}$ basis

(d) $t^3 - 2 = f$ by eisitive irreducible

α root

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

$\alpha = (2)^{\frac{1}{3}}$

Other roots $= \alpha\omega, \alpha\omega^2$

$\operatorname{spl}_{\mathbb{Q}} f = \mathbb{Q}(\alpha, \omega)$ $\omega \notin \mathbb{Q}(\alpha)$

as minimal polynomial of ω over $\mathbb{Q}(\alpha)$ is $t^2 + t + 1$ irreducible over $\mathbb{Q}(\alpha)$

$\Rightarrow [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

$\Rightarrow [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$ $\{1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}$ basis

$\operatorname{spl}_{\mathbb{Q}(i)} f = \mathbb{Q}(\alpha, \omega, i)$ as $\omega = \frac{-1 \pm i\sqrt{3}}{2}$ $\sqrt{3} \notin \mathbb{Q}(i)$ $\alpha \notin \mathbb{Q}(i, \sqrt{3})$

$\Rightarrow [\mathbb{Q}(\alpha, \omega, i) : \mathbb{Q}(i)] = 6$ same basis

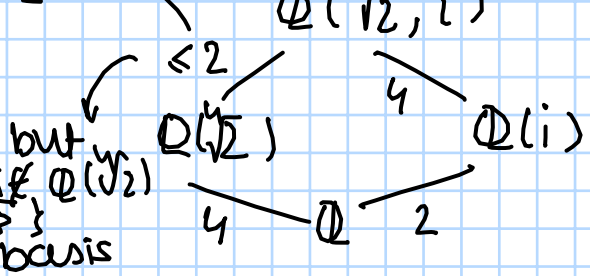
(e) $f = t^4 - 2$ roots: $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$

$\operatorname{spl}_{\mathbb{Q}} f = \mathbb{Q}(\sqrt[4]{2}, i)$ $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ ($\because t^4 - 2$ is irreducible by $P = 2$ after factorising

$\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ and $i \notin \mathbb{Q}(\sqrt[4]{2})$

$\Rightarrow [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$

$\Rightarrow [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$



so, $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{8}\}$ basis

$\operatorname{spl}_{\mathbb{Q}(i)} f = \mathbb{Q}(\sqrt[4]{2}, i)$

by above diagram $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$

basis $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}\}$

(f) $t^4+t^2-1=f \Rightarrow t^2=\frac{-1\pm\sqrt{5}}{2}$

$\alpha=\sqrt{\frac{\sqrt{5}-1}{2}} \quad \beta=\sqrt{\frac{\sqrt{5}+1}{2}}$

$\alpha^2+\beta^2=\sqrt{5} \quad \alpha\beta=1$

so, $\mathrm{spl}_{\mathbb{Q}} f=\mathbb{Q}(\alpha,i)$ as t^4+t^2+1

$\downarrow$

t^4+t^2+1 in $\mathbb{Z}/3\mathbb{Z}$

$\bar{f}(\bar{0})=\bar{1}=\bar{2}$

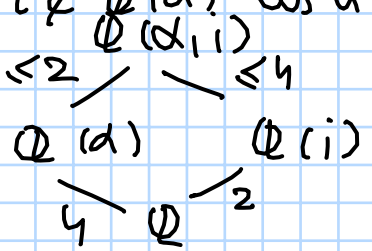
$\bar{f}(\bar{1})=\bar{1}+\bar{1}+\bar{1}=\bar{1}$

$\bar{f}(\bar{2})=\bar{16}+\bar{4}+\bar{1}=\bar{20}+\bar{1}=\bar{19}=\bar{1}$

so, irreducible $\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}]=4$

$i\notin\mathbb{Q}(\alpha)$ as $\alpha\in\mathbb{R} \Rightarrow [\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]=2$

$\Rightarrow [\mathbb{Q}(\alpha,i):\mathbb{Q}]=8$



so, $\{1,\alpha,\alpha^2,\alpha^3, i\alpha, i\alpha^2, i\alpha^3\}$

over $\mathbb{Q}(i)$ from above figure $[\mathbb{Q}(\alpha,i):\mathbb{Q}(i)]=4$

$\{1,\alpha,\alpha^2,\alpha^3\}$ basis

3. (a) $t^4-2=f$ is irreducible $p=2$

and $f(\sqrt[4]{2})=0=f(i\sqrt[4]{2})$

$\Rightarrow \frac{\mathbb{Q}[t]}{\langle f\rangle}\cong\mathbb{Q}(\sqrt[4]{2})\cong\mathbb{Q}(i\sqrt[4]{2})$

(b) NO, if $\exists\ \phi:\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{Q}(\sqrt{3})$

s.t $\phi|_{\mathbb{Q}}=id$

then $\phi(2)=2$

$(\phi(\sqrt{2}))^2=\phi(2)=2$

so, $\exists\ x\in\mathbb{Q}(\sqrt{3})$ s.t $x^2=2$

$x=a+b\sqrt{3}$

$\Rightarrow (a+b\sqrt{3})^2=2$

$\Rightarrow a^2+3b^2+2ab\sqrt{3}=2$

$\downarrow$

$ab=0 \Rightarrow a=0$ or $b=0$

leads to a contradiction

(c) as π is transcendental
$\Rightarrow \pi^2$ also transcendental

as if not true $\exists f \in \mathbb{Q}[t]$ s.t
$f(\pi^2)=0$

but let $f(x^2)=g(x) \in \mathbb{Q}[\pi]$
then $g(\pi)=f(\pi^2)=0$
not possible

similarly $\sqrt{\pi^2+1}$ not possible

so, both $\pi, \sqrt{\pi^2+1}$ are transcendental
$\Rightarrow \mathbb{Q}(\pi) \cong \mathbb{Q}(t) \cong \mathbb{Q}(\sqrt{\pi^2+1})$
$\Rightarrow \mathbb{Q}(\pi) \cong \mathbb{Q}(\sqrt{\pi^2+1})$

4. $\rho_5 \notin \mathbb{Q}(\rho_7)$
if $\rho_5 \in \mathbb{Q}(\rho_7)$ then

$\mathbb{Q}(\rho_7)$ — $\phi(7)=6$
$\mathbb{Q}(\rho_5)$ — $\phi(5)=4$
$\mathbb{Q}$

but $4 \nmid 6$ so, $\rho_5 \notin \mathbb{Q}(\rho_7)$

5. $\rho_4 = e^{2\pi i/4} = e^{\pi i/2} = i \to t^2+1$ irreducible by mod 3

$\rho_6 = e^{2\pi i/6} = e^{\pi i/3}$ $[\mathbb{Q}(\rho_6):\mathbb{Q}] = \phi(6)=2$ $t^2-t+1=f$ irreducible shown by mod 2

$\rho_8 = e^{2\pi i/8} = e^{\pi i/4}$ $[\mathbb{Q}(\rho_8):\mathbb{Q}] = \phi(8)=4$ $t^4+1=f$ irreducible by mod 3 after factoring

$\rho_9 = e^{2\pi i/9}$ $\phi(9)=6$ $\to x^3 = \frac{-1+i\sqrt{3}}{2} \Rightarrow x^6+x^3+1=f$

$\rho_{10} = e^{2\pi i/10} = e^{\pi i/5}$ $\phi(10)=4 \Rightarrow x^4-x^3+x^2-x+1$ min (∵ existing with $p=5$, $t \to t+1$)

ρ_{12} $\phi(12)=4 \to e^{\pi i/6} = \frac{\sqrt{3}+i}{2} = x \Rightarrow x^4-x^2+1=f$

6. $\rho_6 = e^{\pi i/3} = \frac{1+i\sqrt{3}}{2}$ $\rho_3 = \frac{1+i\sqrt{3}}{2}$ $\rho_6 - \rho_3 = 1 \Rightarrow m(t) = t-(1+\rho_3)$

$[K:\mathbb{Q}][M:K] = [M:\mathbb{Q}]$ $K = \mathbb{Q}(\rho_3)$ $\phi(3)=2$

$\phi(9)=6$	2	3	6
$\phi(12)=4$	2	2	4

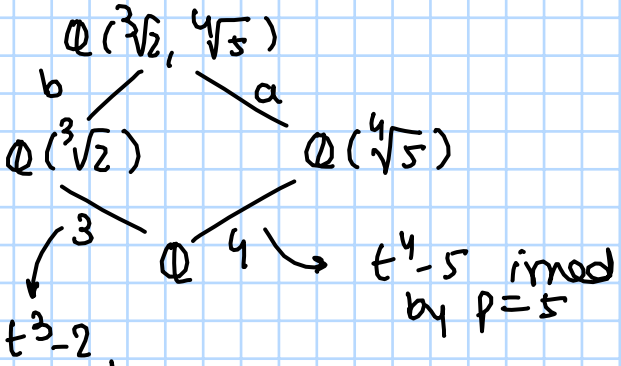
for φ_9: as $[M:K]=3$

$(\varphi_9)^3=\varphi_3 \Rightarrow t^3-\varphi_3=m(t)$

for φ_{12}: as $[M:K]=2$

& $(\varphi_{12})^2=\varphi_6=\varphi_3+1 \Rightarrow m(t)=x^2-(\varphi_3+1)$

7.



also $4a=3b$ $a|3$ $a<3 \Rightarrow a=1,3$ $\Rightarrow a=3$

$\Rightarrow b=4$

so, $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}):\mathbb{Q}]=12$

$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$

$\{1, \sqrt{6}, \sqrt{10}, \sqrt{15}\}$ $\sqrt{60}$, $\sqrt{150}$, $\sqrt{90}$

$\sqrt{60} \to 2\sqrt{15}$, $\sqrt{150} \to 5\sqrt{6}$, $\sqrt{90} \to 3\sqrt{10}$

and $\sqrt{60}=2\sqrt{15}$

so, $\sqrt{15} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$ also, $\sqrt{10} \notin \mathbb{Q}(\sqrt{6})$ as

$10=a^2+6b^2+2ab\sqrt{6}$ contradiction

($2ab\sqrt{6} \to 0$)

$\Rightarrow [\mathbb{Q}(\sqrt{10}, \sqrt{6}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{10}, \sqrt{6}):\mathbb{Q}(\sqrt{6})]\,[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]$

$= 2 \cdot 2 = 4$

8. $f=t^4+2t^3+6t^2+t+9$ irred $\mathbb{Q}$

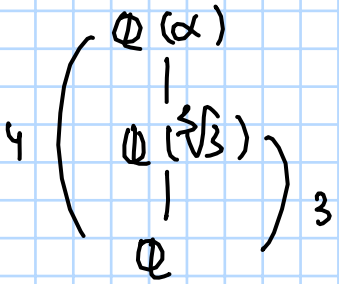
$\to \bar{t}^4+\bar{t}+\bar{1}$ $\bar{f}(\bar{0})=1\neq 0$, $\bar{f}(\bar{1})=1\neq 0$

so, no roots in $\mathbb{Z}/2\mathbb{Z}$, now over irred of deg 2 $= t^2+t+1$ in $\mathbb{Z}/2\mathbb{Z}$

but $(t^2+t^2+1)^2=t^4+t^2+1 \neq t^4+t+1$

so, f must be factored in $\mathbb{Z}/2\mathbb{Z}$, by mod p irred $f(t)$ irred over $\mathbb{Q}$

now, if α is a root if $\sqrt[3]{3} \in \mathbb{Q}(\alpha)$ then



3∤4 so not possible

9. $\mathbb{Q}(i\sqrt{2})$

if $i \in \mathbb{Q}(i\sqrt{2})$

then

$i = a + i\sqrt{2}b$

$-1 = a^2 - 2b^2 + 2ab\sqrt{2}i$

$ab = 0 \Rightarrow a = 0$ or $b = 0$

not possible

$\Rightarrow i \notin \mathbb{Q}(\sqrt{2}i)$

(ii) $x^4 + 2 = 0$ minimal by $p = 2$

$\alpha = (-2)^{1/4}$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

as $\alpha^2 = i\sqrt{2}$ if $i \in \mathbb{Q}(\alpha)$

$\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\alpha)$ ($\because i \in \mathbb{Q}(\alpha)$ so $i\sqrt{2}/i \in \mathbb{Q}(\alpha)$)

also $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4 \Rightarrow \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\alpha)$

but $\alpha \notin \mathbb{Q}(i, \sqrt{2})$ as if so then

$\alpha = a + ib + \sqrt{2}c + i\sqrt{2}d$

$\alpha^2 = i\sqrt{2} = (a + ib + \sqrt{2}c + i\sqrt{2}d)^2$

$i\sqrt{2} = a^2 - b^2 + 2c^2 - 2d^2 + 2abi \rightarrow a = 0$ or $b = 0$

$+ 2\sqrt{2}ibc$

$+ 2\sqrt{2}ac \rightarrow a = 0$ or $c = 0$

$+ 2\sqrt{2}iad$

$+ 4icd \rightarrow a = 0$ or $d = 0$ or $d = 0$

if $a \neq 0$ then not possible

but if $a = 0$ then $i\sqrt{2} = -b^2 + 2c^2 - 2d^2 + 2\sqrt{2}ibc$

$2bc = 1 \quad bc = 1/2$

$2c^2 - 2d^2 - b^2 = 0$ not possible

$2(1/2b)^2 - 2d^2 - b^2 = 0$

so, $\alpha \notin \mathbb{Q}(i, \sqrt{2})$ so, $i \notin \mathbb{Q}(\alpha)$ as

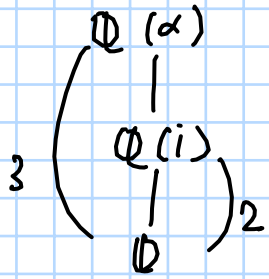
$\frac{1}{2b^2} - b^2 = 2d^2$

$\frac{1}{b^2} - 2b^2 = 4d^2$ $d=0$ trivially

(iii) $x^3+x+1=0$ $\mathbb{Q}(\alpha)$

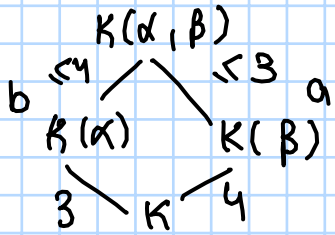
irred as $\mathbb{Z}/2\mathbb{Z}$ no roots

if $i \in \mathbb{Q}(\alpha)$



2∤3 so $i \notin \mathbb{Q}(\alpha)$

10.



$4a = 3b$

$a|3 \Rightarrow a=3$ $a \leq 3$

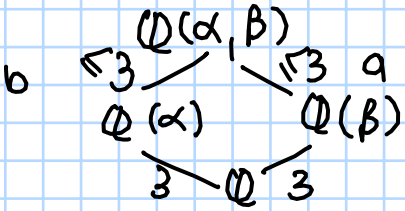
$\Rightarrow b=4$

so, $[K(\alpha,\beta):K] = 12$

11. $\alpha, \beta \in \mathbb{C}$

$[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$

$[\mathbb{Q}(\beta):\mathbb{Q}] = 3$

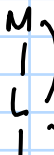


$3a = 3b \Rightarrow a=b$ and $a \leq 3$

so, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = \{3.1, 3.2, 3.3\}$

$= \{3, 6, 9\}$

12.



M algebraic / L algebraic

we want to show that

$\forall \alpha \in M$

$\exists f \in K[t]$ s.t

$f(\alpha) = 0$

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

now, $\forall \alpha \in M$, $[L(\alpha):L] < \infty$

so, $\exists f \in L[t]$ s.t

$f(\alpha) = 0$ $f(t) = \sum a_i^{\circ} t^{i^{\circ}}$

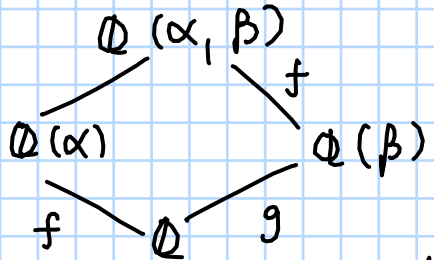
$a_i^{\circ} \in L \Rightarrow [K(a_i):K] < \infty \ \forall i$ as $\alpha \in K(a_1, a_2 \ldots a_n)$

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

13. $\forall \alpha, \beta \in \mathbb{C}$ $\min_{\mathbb{Q}} \alpha = f \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$

$\min_{\mathbb{Q}} \beta = g \Rightarrow \mathbb{Q}(\beta) = \mathbb{Q}[\beta]$

($\Rightarrow$) f is irred over $\mathbb{Q}(\beta)$ and $f(\alpha) = 0$ $\Rightarrow \min_{\mathbb{Q}(\beta)} \alpha = f$



Now let $\min_{\mathbb{Q}(\alpha)} \beta = g'$ then $g' | g$ ($\because$ done in class)

$\deg(f)\deg(g') = \deg(f)\deg(g)$

$\Rightarrow \deg g' = \deg g$

$\Rightarrow g' = g$

$\therefore$ g is irred over $\mathbb{Q}(\alpha)$

($\Leftarrow$) follows similarly

14. M_1, M_2

$\pi^{1/2}, \pi^5$ both transidental

$\Rightarrow \mathbb{Q}(\pi^{1/2}) \cong \mathbb{Q}(\pi^5)$

but, $K = \mathbb{Q}(\pi^{10}) \Rightarrow \dim_K M_1 = 20$

$\dim_K M_2 = 2$

not K isomorphic

15. $\alpha_1, \alpha_2, \ldots \alpha_n \in M$ algebric $/K$

true $\exists f_1 = \min_K \alpha_i$

$\Rightarrow \frac{K[t]}{\langle f_1 \rangle} \cong \mathbb{Q}[\alpha_i] = \mathbb{Q}(\alpha_i)$ $\therefore$ true for $n = 1$

($\because$ field as $\langle f_1 \rangle$ is maximal)

now if true till α_{n+1} then

$K[\alpha_1 \ldots \alpha_n] = K[\alpha_1 \ldots \alpha_{n+1}][\alpha_n]$

α_n alg $/ K[\alpha_1 \ldots \alpha_{n+1}]$

$= K[\alpha_1 \ldots \alpha_{n+1}](\alpha_n)$

$= K(\alpha_1)(\alpha_2) \ldots (\alpha_{n+1})(\alpha_n)$

($\because$ induction)

by induction true $\forall n$

16. $\alpha = \omega \quad \beta = \omega^2$

$\{1, \omega, \omega^2\} = \{\alpha^i \beta^j \mid i, j \in \{0,1,2\}\}$

17. $1 + \cos\theta = 2\cos^2\frac{\theta}{2}$

$1 + \cos 30^\circ = 2\cos^2 15^\circ$

$1 + \sqrt{3}/2 = 2\cos^2 15^\circ$

$\left(\frac{1}{2} + \frac{\sqrt{3}}{4}\right)^{\frac{1}{2}} = \cos 15^\circ$

18. 5 gon $\frac{2\pi}{5}$

$[\mathbb{Q}(e^{2\pi i/5}) : \mathbb{Q}] = 5 - 1 = 4$

now $e^{2\pi i/5}$ is s.t minimal polynomial is of deg 4 so constructable

19. $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}] = 6 \neq 2^m$

similar for form

$10 \neq 2^n$ form

so not constructable

20. 9 gon is constructable

as $\phi(9) = 8 = 2^3$

21. as $C = \bigcup_{i=1}^{\infty} C_i$

$C_1 = \{0, 1\}$ $C_2 =$ constructable by C_1

as $\forall c \in C \Rightarrow c \in C_i \Rightarrow \sqrt{c} \in C_{i+1}$

$C = \bigcup_{i=1}^{\infty} C_i$ is smallest since by construction

22. same as before as our first construction does not change

23. $\phi : SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{F}_p)$

↳ Homomorphism by reducing matrix to modulo p

$A \in SL_2(\mathbb{Z})$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $ad - bc = 1, a, b, c, d \in \mathbb{Z}$

now $Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \in SL_2(\mathbb{F}_p)$ $y_{11}y_{22} - y_{12}y_{21} = 1$

then $\exists \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \in SL_2(\mathbb{Z})$ s.t. $\phi\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$

so linear isomorphism

same for SL_n

Tutorial-6:

$\alpha \in L$, L/K: $\min_K \alpha$ splits in $L \Rightarrow L|_K$ is normal

$\forall \alpha \in L$

if (N → smallest such normal s.t $N|_L$, $N|_K$ normal; L → Not normal; K)

N is unique upto isomorphism

$L = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ then $N = spl_K(f_1, f_2 \ldots f_n)$, $f_i = \min_K \alpha_i$, $K(\alpha_1, \alpha_2 \ldots \alpha_n)$, K

smallest such normal

2. L/M Normal, M/K Normal

$L = \mathbb{Q}(2^{1/4})$

$M = \mathbb{Q}(2^{1/2})$

$K = \mathbb{Q}$

$\mathbb{Q}(2^{1/4})$, $\mathbb{Q}$ not normal as $f(t) = t^4 - 2$ in $\mathbb{Q}$ is s.t

$= (t - 2^{1/4})(t + 2^{1/4})$

$(t - i2^{1/4})(t + i2^{1/4})$

$i \notin \mathbb{Q}(2^{1/4})$

$L|_M$ is normal as $\forall \alpha \in L$, $\min_K \alpha$ splits in L

$\Rightarrow \min_M \alpha$ splits in L as it divides $\min_K \alpha$

L/M Normal, M/K not normal as counterexample done

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

as, $K \subset M \subset L$

$f \in K[t] \Rightarrow f \in M[t]$

3. L/K, $L|_K$ normal, invalid

$\alpha, \beta \in L$ s.t $f \in K[t]$

$f(\alpha) = 0$, $f(\beta) = 0$

$\exists \bar{\sigma}$ s.t $\bar{\sigma}: L \to \bar{K}$

L, normal, $\bar{K}$, embedding

$\sigma: M \to \bar{K}$, K

$\bar{\sigma}: L \to \bar{K}$

$\bar{\sigma}|_K = id_K$ $\bar{\sigma}|_M = \sigma$

$\sigma : K(\alpha) \to K(\beta) \subseteq \bar{K}$
$\alpha \mapsto \beta$
$K \to K$

$\tilde{\sigma}$: $L \to K'$, $K' \subseteq \bar{K}$
$\sigma : K(\alpha) \hookrightarrow \bar{K}$
$K \to K$

$\tilde{\sigma} : L \to \bar{K}$
$\tilde{\sigma}(\alpha) = \beta$ — ①
$\tilde{\sigma}|_K = id$ — ②
$L|_K$ is normal
$\Rightarrow L|_{K(\alpha)}$ is normal
so we can use the theorem

$\tilde{\sigma} : \alpha \in L \to$ any root $\in L$ of some minimal polynomial

$\Rightarrow \tilde{\sigma}(L) = L$
$\Rightarrow \tilde{\sigma} \in Aut(L|_K)$
so, $\exists\ \sigma \in Gal(L|_K)$ s.t $\sigma(\alpha) = \beta$

4. L / K finite, normal

$\tilde{\tau} : L \to \bar{K}$ $\Rightarrow \tilde{\tau} \in Gal(L|_K)$ extending τ

normal(|)
$\tau : M \to M' \subseteq \bar{K}$
$M \cong M$
K

5. L / M / K) Normal $\quad \sigma \in Gal(L|_K)$

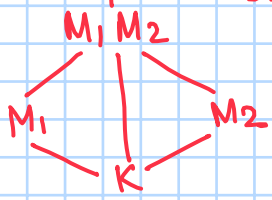
$\sigma : L \to L$
$\sigma|_K = id_K$
$\sigma_* : f \to f$
$\{\alpha_1, \alpha_2, \ldots \alpha_n\} \subseteq M \quad \alpha_1 = \alpha$
$f = \min_K \alpha \to$ root of f goes to M in σ
$\Rightarrow \sigma(M) = M$
$\Rightarrow \sigma|_M \in Gal(M|_K)$

7. L / K; M_1, M_2 normal; normal

$\alpha \in M_1 \cap M_2$
$\Rightarrow \alpha \in M_1, \ \alpha \in M_2$
$\Rightarrow \min_K \alpha$ splits in M_1 and M_2
$\Rightarrow \min_K \alpha$ splits in $M_1 \cap M_2$



$\tilde{N}$ → smallest normal containing N_1N_2

now, 

$\tilde{N}|_K$ normal

$\alpha \in M_1M_2 \Rightarrow \alpha \in \tilde{N}$

$\Rightarrow f = \min_K \alpha$

roots of f $\{\alpha_1, \alpha_2, \ldots \alpha_n\} \subseteq \tilde{N}$ $(\because \tilde{N}|_K$ normal$)$

wlog $\alpha_1 = \alpha$

by (3), $\tilde{N}$ / K normal, $\exists \sigma_i^\circ \in Gal(\tilde{N}|_K)$ s.t $\sigma_i^\circ(\alpha) = \alpha_i^\circ$

$\sigma_i^\circ : \tilde{N} \to \tilde{N}$
$\alpha \mapsto \alpha_i^\circ$

as $\alpha \in M_1M_2 \Rightarrow \alpha = \sum a_i^\circ b_i^\circ$

$a_i^\circ \in M_1, \ b_i^\circ \in M_2$

$\sigma_i^\circ|_{M_1M_2} : M_1M_2 \to \tilde{N}$

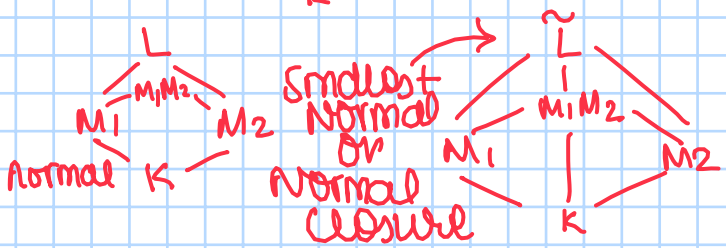
$\sigma(\alpha) = \sum \sigma(a_i^\circ)\sigma(b_i^\circ)$
$\quad \in M_1 \quad \in M_2 \quad (\because$ (5) problem$)$

$\sigma|_{M_1} \in gal(M_1|_K) \quad \sigma|_{M_2} \in gal(M_2|_K)$

$\Rightarrow \sigma(\alpha) \in M_1M_2$

$\Rightarrow \alpha_i^\circ \in M_1M_2 \ \forall i$

$\Rightarrow M_1M_2|_K$ is normal

8. 

$M_1|_K$ normal if $\sigma M_1 = M_1 \ \forall \sigma \in Gal(\tilde{L}|_K)$ $(\because$ (6) problem$)$

$\sigma \in Gal(\tilde{L}|M_2) \Rightarrow \sigma \in Gal(\tilde{L}|K)$

as $K \subset M_2 \subset \tilde{L}$

$\sigma|_{M_2} = id \Rightarrow \sigma|_K = id$ so $\sigma \in Gal(\tilde{L}|K)$

then, $\alpha \in M_1M_2$ i.e $\alpha = \sum a_i b_i$, $a_i \in M_1$, $b_i \in M_2$

$$\sigma(\alpha) = \sum \sigma(a_i)\sigma(b_i) = \sum \sigma(a_i) b_i$$

($\sigma(a_i) b_i \in M_2$)

$M_1|K$ is normal

$\Leftrightarrow \sigma(M_1) = M_1 \ \forall \sigma \in Gal(\tilde{L}|K)$

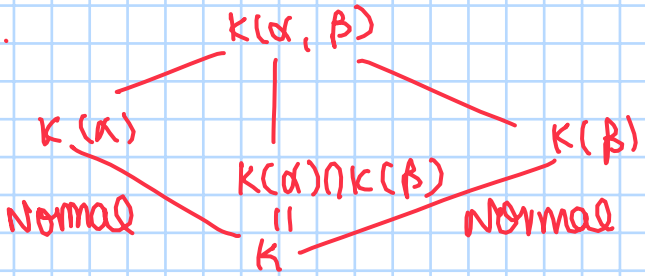
$\Rightarrow \sigma(M_1M_2) = M_1M_2$

so, $\forall \sigma \in Gal(\tilde{L}|M_2)$ $\sigma(M_1M_2) = M_1M_2$

$\Rightarrow M_1M_2|M_2$ is normal

(∵ (6) problem)

9.



$[K(\alpha,\beta):K] = [K(\alpha,\beta):K(\alpha)][K(\alpha):K]$

$[K(\beta):K]$

if $\min_K \beta = \min_{K(\alpha)} \beta$ then we are done

as $[K(\beta):K] = [K(\alpha,\beta):K(\alpha)]$

$f = \min_K \beta \in K[t]$

as $K(\beta)$ is normal, let $\{\beta_1, \beta_2, \dots \beta_n\} \subseteq K(\beta)$ roots of f

K

if $f(x) = g(x)h(x) \in K(\alpha)[x]$

$g = \min_{K(\alpha)} \beta$ then $g|f$

but $g = (x-\beta_1)\cdots(x-\beta_r)$ $\{\beta_1 \dots \beta_r\} \subseteq K(\beta)$

coeff of g $\Sigma\pi\beta_i^\circ \Rightarrow g \in K(\beta)[t]$

as $K(\alpha) \cap K(\beta) = K$

and $g \in K(\alpha)[t] \Rightarrow g \in K[t]$

$\Rightarrow \min_{K(\alpha)} \beta \in K[t]$

$\Rightarrow \min_{K(\alpha)} \beta = \min_{K} \beta$

10. L normal $f \in K[t]$ monic, reducible

L / K

$f(x) = g_1 g_2$ → monic, irreducible

$f = g_1 g_2$ — K — $f = (x-\alpha_1)\cdots(x-\alpha_n)$

L — N — $L \cap N$ — K

$g_1 \in L[x]$, $g_2 \in L[x]$

$\Rightarrow g_1 \in N[x]$, $g_2 \in N[x]$ is trivial

$\Rightarrow g_1 \in L \cap N[x]$, $g_2 \in L \cap N[x]$ now from above question get $\sigma \in \mathrm{Gal}(L|K)$ s.t $\sigma(g_1) = g_2$

1.(a) $\mathbb{Q}(2^{1/4})$ / $\mathbb{Q}$ $\quad \alpha = 2^{1/4}$

$f = \min_{\mathbb{Q}} \alpha = t^4 - 2$

then $(t^2-\sqrt{2})(t^2+\sqrt{2}) \Rightarrow (t-2^{\frac{1}{4}})(t+2^{\frac{1}{4}})$

$(t-i2^{\frac{1}{4}})(t+i2^{\frac{1}{4}})$

$\mathrm{spl}_{\mathbb{Q}} f = \mathbb{Q}(2^{\frac{1}{4}}, i)$

$\&$, $N = \mathbb{Q}(2^{\frac{1}{4}}, i)$

(b) $\min_{\mathbb{Q}(2^{1/2})} (2^{\frac{1}{4}}) = t^2 - 2^{\frac{1}{2}} = f = (t-2^{\frac{1}{4}})(t+2^{\frac{1}{4}})$

now, $\mathrm{spl}_{\mathbb{Q}(2^{1/2})} f_{1/2} = \mathbb{Q}(2^{\frac{1}{2}})(2^{\frac{1}{4}}) = \mathbb{Q}(2^{\frac{1}{4}})$

$\&$, $N = \mathbb{Q}(2^{\frac{1}{4}})$

or normal

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

$\min_{\mathbb{Q}} 2^{\frac{1}{3}} = t^3 - 2 = (t - 2^{\frac{1}{3}})(t - \omega 2^{\frac{1}{3}})(t - \omega^2 2^{\frac{1}{3}})$

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

(d) $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ from (a) $N = \mathbb{Q}(2^{\frac{1}{4}}, i)$

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

now $\min_{\mathbb{Q}} \sqrt{2} = t^2 - 2 = f_1 = (t-\sqrt{2})(t+\sqrt{2})$

$\min_{\mathbb{Q}} \sqrt{3} = t^2 - 3 = f_2 = (t-\sqrt{3})(t+\sqrt{3})$

then, $\operatorname{spl}_{\mathbb{Q}}(f_1, f_2) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = N$

so, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal over $\mathbb{Q}$

(f) $\mathbb{Q}(t)$ over $\mathbb{Q}(t^3)$ now $\min_{\mathbb{Q}(t^3)} t = x^3 - t^3 = f(x) \in \mathbb{Q}(t^3)[x]$

then $f(x) = (x-t)(x-\omega t)(x-\omega^2 t)$

$\Rightarrow \operatorname{spl}_{\mathbb{Q}(t^3)} f_3 = \mathbb{Q}(t, \omega)$

$\Rightarrow N = \mathbb{Q}(t, \omega)$

(g) $\mathbb{F}_3(t)$ over $\mathbb{F}_3(t^4)$ $\min_{\mathbb{F}_3(t^4)} t = x^4 - t^4 = f(x) \in \mathbb{F}_3(t^4)[x]$

now, $x^4 - t^4 = (x^2 - t^2)(x^2 + t^2)$

$= (x-t)(x+t)(x+it)(x-it)$

$\Rightarrow \operatorname{spl}_{\mathbb{F}_3(t^4)} f = \mathbb{F}_3(t, i) = N$

(h) $\mathbb{Q}(a)$ over $\mathbb{Q}$ as $a^5 = 1$, $a \neq 1$ now $\zeta_5 = e^{2\pi i/5}$

$\phi(5) = 4 \Rightarrow \min_{\mathbb{Q}} \zeta_5 = t^4 + t^3 + t^2 + t + 1$

now, as $\zeta_5 = e^{2\pi i/5} = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$

$= \frac{-1+\sqrt{5}}{2} + i\left(\frac{1+\sqrt{5}}{2}\right) = a$

so, $\operatorname{spl}_{\mathbb{Q}} f = \mathbb{Q}(i, \sqrt{5}) = N$

2. LINK

(a) normal $L = \mathbb{Q}(2^{\frac{1}{4}})$ / normal $M = \mathbb{Q}(2^{\frac{1}{2}})$ / $K = \mathbb{Q}$

but L/K not normal from above

(b) L/M normal, $\forall \alpha \in L$, $\min_K \alpha$ splits in L

$\Rightarrow \min_M \alpha$ splits in L

as $\min_M \alpha \mid \min_K \alpha$

so, L/M normal

M/K not normal as

$\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ / normal $\mathbb{Q}(2^{\frac{1}{3}})$ / not normal $\mathbb{Q}$

from above

3. L/K normal

$\alpha, \beta \in L$

s.t $\min_K \alpha = f$

$\min_K \beta = f$

$\exists \tilde{\sigma} : L \to \bar{K}$ s.t $\tilde{\sigma} : L \to \bar{K}$, $\tilde{\sigma}|_K = id$ $\tilde{\sigma}|_M = \sigma$

now, normal L/K, $\sigma : M \hookrightarrow \bar{K}$ embedding

$\sigma : M \hookrightarrow \bar{K}$ / K

now $\sigma : K(\alpha) \to K(\beta) \subseteq \bar{K}$

$\alpha \mapsto \beta$

K

normal by (2) $\Rightarrow \exists \tilde{\sigma} : L \to \bar{K}$

$L \to \bar{K}$ / $K(\alpha) \hookrightarrow \bar{K}$ / $K \to K$

$\tilde{\sigma}|_{K(\alpha)} = \sigma$ —①

$\tilde{\sigma}|_K = id$ —②

now as $\ell \in L$, ℓ is s.t $\min \ell$ splits in L

then in $\min_K \ell = g$ then $\tilde{\sigma}'(g(\ell))$

$= g(\tilde{\sigma}(\ell)) = 0$

so, $\sigma^2(\ell)$ is a root of some minimal polynomial

$\Rightarrow \sigma^2(\ell) \in L$

$\Rightarrow \sigma^2(L) = L$ — ③

$\Rightarrow \sigma^2 \in Aut(L|_K)$ ($\because$ ①, ②, ③)

4.

finite normal $\begin{pmatrix} L \\ | \\ K \end{pmatrix}$

$\tilde{\varphi} : L \to \bar{K}$ $\Rightarrow \varphi \in Gal(L|_K)$ extending τ from (3)

$\varphi : M \xrightarrow{\cong} M' \leq \bar{K}$ ($\cong$ over K)

normal ($\because$ (2))

5. $\begin{pmatrix} L \\ | \\ M \\ | \\ K \end{pmatrix}$ normal

$\sigma \in Gal(L|_K)$

$\sigma|_K = id_K$

$\sigma_* : f \to f$ $\{\alpha_1, \alpha_2, \ldots \alpha_n\} \subseteq M$ $\alpha_1 = \alpha$

$f = \min_K \alpha \to$ roots of f goes to M in σ

$\Rightarrow \sigma(M) = M$ ($\because \sigma_* : S \to S$)

$\Rightarrow \sigma|_M \in Gal(M|_K)$

6. normal $\begin{pmatrix} L \\ | \\ M \\ | \\ K \end{pmatrix}$ normal

M/K normal iff $\sigma M = M$ $\forall \sigma \in Gal(L|_M)$

($\Rightarrow$) $\begin{matrix} M \\ | \\ K \end{matrix}$ normal then we saw in (5) $\sigma M = M$ $\forall \sigma \in Gal(L|_M)$

($\Leftarrow$) if $\sigma M = M$ $\forall \sigma \in Gal(L|_M)$

$\alpha \in M$, $g = \min_K \alpha$ if g splits in M then we are done

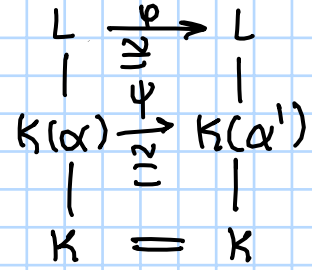
g splits in L

let α' be root of g then $\alpha' \in L$

$\Rightarrow \min_K \alpha = \min_K \alpha' = g$

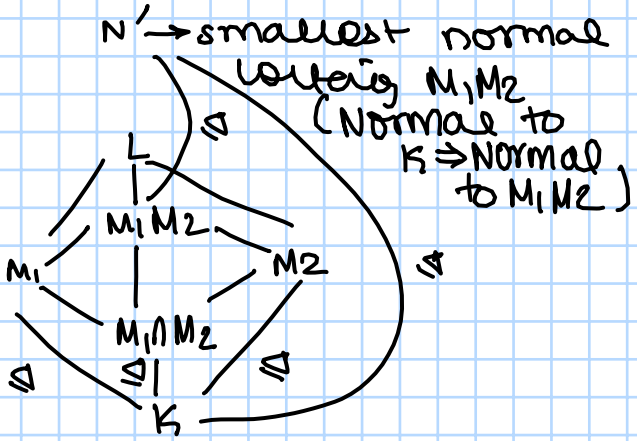
by below diagram $\varphi \in Gal(L|_K)$

$\Rightarrow \varphi(\alpha) = \alpha' \in M$ as $\alpha \in M$ & $\varphi(M) = M$



$\therefore$, M / K normal

7.



$\alpha \in M_1 \cap M_2$
$\Rightarrow \alpha \in M_1,\ \alpha \in M_2$
$\Rightarrow \min_K \alpha$ splits in M_1 & M_2
$\Rightarrow M_1 \cap M_2$ normal K

now $\alpha \in M_1M_2 \Rightarrow \alpha \in N'$

then $f = \min_K \alpha$ splits in N'
$(\because N'|_K$ normal$)$

then roots of f be $\{\alpha_1, \alpha_2 \dots \alpha_n\}$
α

then $\exists \sigma_i \in$ Gal$(N'|_K)$ s.t
$\sigma_i(\alpha) = \alpha_i$

as $\alpha \in M_1M_2$, $\alpha = \sum a_i b_i$
$a_i \in M_1,\ b_i \in M_2$

$\sigma_i(\alpha) = \sum \sigma(a_i)\sigma(b_i)$
$\in M_1 \quad \in M_2$
$(\because M_1, M_2$ normal over K, by (5))

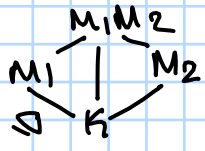
$\Rightarrow \sigma_i(\alpha) \in M_1M_2$

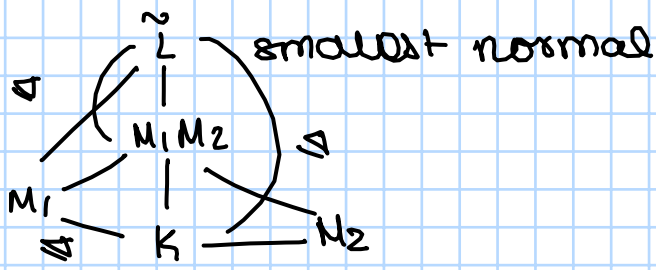
$\Rightarrow \alpha_i \in M_1M_2 \ \forall i$

$\Rightarrow M_1M_2$ splits $\min_K \alpha$

$\therefore$, M_1M_2 / K normal

8.



now 

then, $M_1|_K$ normal iff $\sigma M_1 = M_1 \ \forall \ \sigma \in Gal(\tilde{L}|_K)$ $(\because (6))$
(①)

$\sigma' \in Gal(\tilde{L}|M_2) \Rightarrow \sigma' \in Gal(\tilde{L}|K)$ ——②

as trivial

then $\alpha \in M_1M_2 \quad \alpha = \sum \alpha_i \beta_i$

$\sigma'(\alpha) = \sum \sigma'(\alpha_i)\sigma'(\beta_i)$

$\in M_1 \quad \in M_2$

$(\because ①, ②)$

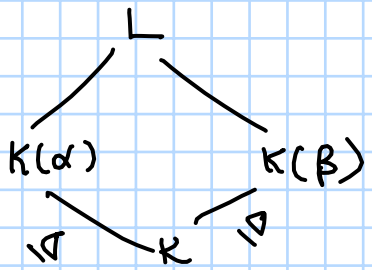
$\Rightarrow \sigma'(\alpha) \in M_1M_2$

so, $\sigma'(M_1M_2) = M_1M_2 \ \forall \ \sigma' \in Gal(\tilde{L}|M_2)$

$\Rightarrow M_1M_2$ normal $(\because (6))$

M_2

9.



$K(\alpha) \cap K(\beta) = K$

$[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K]$

$\leq [K(\beta) : K]$

$\min_K \beta = \min_{K(\alpha)} \beta$ then we are

$f = \min_K \beta \in K[L]$

$K(\beta)$ normal $\quad \{\beta_1 \dots \beta_n\} \subseteq K(\beta)$

K $\quad$ ↓ roots of f

if $f(x) = g(x)\,h(x) \in K(\alpha)[x]$

then

$g = \min_{K(\alpha)} \beta = (x-\beta_1)\dots(x-\beta_r)$

but $K(\alpha) \cap K(\beta) = K \Rightarrow g \in K[L]$

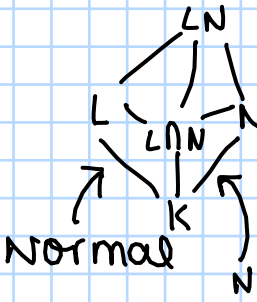
so, $g = f$

10.

L
|
K normal

$f(t) \in K[t]$ monic irreducible

$f \to$ Reducible over $L[t]$



f roots $\alpha_1 \ldots \alpha_n$

LN, LNN also normal ($\because$ 7)

let $\alpha_1 \to g_1$ $\alpha_2 \to g_2$ then

$\tilde{\sigma}: LN \longrightarrow LN$ ($\because$ 3)
$\alpha_1 \longrightarrow \alpha_2$ as roots of f over LN are $\alpha_1 \ldots \alpha_n$

$\tilde{\sigma}|_L = \sigma$

$f = (x-\alpha_1)\cdots(x-\alpha_n)$

$\exists\ \tilde{\sigma} \in Gal_K(LN)$

now

LN
|
L
|
K

$\tilde{\sigma}|_L \in Gal(L|_K)$ ($\because$ 5)

say $\tilde{\sigma}|_L = \sigma$

now, $\tilde{\sigma}: LN \to LN$ s.t $\alpha_1 \to \alpha_2$ $\quad \tilde{\sigma} \in Gal(LN|_K)$

$\tilde{\sigma}|_L = \sigma \in Gal(L|_K)$

now $g_1(\alpha_1) = 0$

$g_2(\alpha_2) = 0$

$\tilde{\sigma}(g_1(\alpha_1)) = 0$

$\tilde{\sigma}(g_1)(\tilde{\sigma}(\alpha_1)) = 0$

$\Rightarrow \tilde{\sigma}(g_1)(\alpha_2) = 0$

but $\tilde{\sigma}|_L = \sigma$ and as g_1, g_2 over L

$\Rightarrow \tilde{\sigma}(g_1)(\alpha_2) = 0$

$\Rightarrow \sigma(g_1)(\alpha_2) = 0$ but $g_2(\alpha_2) = 0$ and inducible monic

$\Rightarrow \sigma(g_1) = g_2$ $\quad \min_L \alpha_2 = \sigma(g_1)$ as g_1 irreducible monic
$\Rightarrow \sigma(g_1)$ also irreducible monic

11. $f \in K[t]$ irreducible is normal if $spl_K f = K(\alpha)$ α as a zero of f

($\Rightarrow$) If f is normal i.e $spl_K f = K(\alpha)$, $f(\alpha)=0$ f is irreducible (wlog monic)

$\min_K \alpha = f$

$[spl_K(f) : K] = [K(\alpha) : K] = \deg(f)$

$(\because \min_K \alpha = f)$

($\Leftarrow$) If deg of $spl_K(f) = \deg(f)$ then f is irreducible (wlog monic)

$spl_K(f) = K(\alpha_1, \alpha_2, .. \alpha_n)$

|

K

let $\alpha_1, \alpha_2, .. \alpha_n$ be roots of f

as f is irreducible, $\min_K \alpha_i = f \ \forall i \in \{1, 2, .. n\}$

if $n \geq 2$ then

$K(\alpha_1, \alpha_2) \subseteq K(\alpha_1 .. \alpha_n)$

and $f(\alpha_1) = 0$

$\Rightarrow \alpha_1^{\deg f} = \sum_{i=0}^{\deg f - 1} a_i^0 \alpha_1^i$

s.t $\{\alpha_1, \alpha_2\}$ independent

$\Rightarrow [K(\alpha_1, \alpha_2) : K] \geq \deg f + 1$

but $[K(\alpha_1, \alpha_2 .. \alpha_n) : K] = \deg f$

$\Rightarrow n < 2 \Rightarrow n = 1$

so, f is normal

now, $t^n - 2 \in \mathbb{Q}[t]$ is s.t,

$spl_{\mathbb{Q}}(t^n - 2) = \mathbb{Q}(2^{\frac{1}{n}}, \zeta_n)$

$\neq \mathbb{Q}(\alpha)$

so, not normal

Tutorial-1:

1. $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}$

now, $f(x)=x^4-2$ roots of f are $2^{\frac{1}{4}}, i2^{\frac{1}{4}}, -2^{\frac{1}{4}}, -i2^{\frac{1}{4}}$

$\sigma \in Gal(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q})$ then
$\sigma(2^{\frac{1}{4}})$ is root of f

as $\sigma(2^{\frac{1}{4}}) \in \mathbb{Q}(2^{\frac{1}{4}}) \subseteq \mathbb{R}$
$\Rightarrow \sigma(2^{\frac{1}{4}}) = \{2^{\frac{1}{4}}, -2^{\frac{1}{4}}\}$

so, $\rho: 2^{\frac{1}{4}} \to -2^{\frac{1}{4}}$
$id: 2^{\frac{1}{4}} \to 2^{\frac{1}{4}}$

then, $Gal(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}) = \{id, \rho\}$

$\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}})$

then roots of $t^2-2^{\frac{1}{2}} = (t-2^{\frac{1}{4}})(t+2^{\frac{1}{4}})$

now $f=t^2-\sqrt{2}$ is irreducible over $\mathbb{Q}(2^{\frac{1}{2}})$

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

$\mathbb{Q}(2^{\frac{1}{4}})$ and $\mathbb{Q}(2^{\frac{1}{2}})$ — Normal, separable (trivial; no common roots)

$\Rightarrow |Gal(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}}))| = 2$
$\Rightarrow Gal(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}})) \cong \mathbb{Z}/2\mathbb{Z}$
$\Rightarrow Gal(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}(2^{\frac{1}{2}})) = \{id, \tau\}$

$\mathbb{Q}(2^{\frac{1}{4}}, i)$

Normal, separable over $\mathbb{Q}$:
$(t^4-2) = (t \pm \sqrt[4]{2})(t \pm i\sqrt[4]{2})$
$(t^2+1) = (t \pm i)$

$\sigma: \mathbb{Q}(2^{\frac{1}{4}}, i) \longrightarrow \mathbb{Q}(2^{\frac{1}{4}}, i)$

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

$\sqrt[4]{2} \to \pm\sqrt[4]{2}$, $i \to \pm i$

$\rho: \sqrt[4]{2} \to \sqrt[4]{2}$, $i \to -i$ $\quad \rho = \rho^{-1} \Rightarrow \rho^2 = 1$

$\tau: \sqrt[4]{2} \to i\sqrt[4]{2}$, $i \to i$ $\Rightarrow \tau^4 = 1$

and $\tau\rho\tau = \rho \Rightarrow Gal(\mathbb{Q}(2^{\frac{1}{4}}, i)/\mathbb{Q}) \cong D_4$

$\mathbb{Q}(2^{\frac{1}{4}}, i)$ ← Normal as $\forall a \in \mathbb{Q}(2^{\frac{1}{4}}, i)$ $\min_{\mathbb{Q}(2^{\frac{1}{4}})} \alpha$ splits in $\mathbb{Q}(2^{\frac{1}{4}}, i)$

4 | 2

$\mathbb{Q}(2^{\frac{1}{4}})$ — 2 — $\mathbb{Q}(2^{\frac{1}{2}})$ separable as char is 0 so all imed separable

$$\sigma : 2^{\frac{1}{4}} \to i\,2^{\frac{1}{4}} \qquad \sigma^2 = 1$$

$$\tau : 2^{\frac{1}{4}} \to -2^{\frac{1}{4}} \qquad \tau^2 = 1$$

$$\langle \sigma, \tau \rangle = \{ id, \sigma, \tau, \sigma\tau \}$$

$\mathbb{F}_2(t)$

|

$\mathbb{F}_2(t^2)$

$x^2 - t^2 = (x-t)(x+t)$

$= (x-t)^2$

as $t = -t$ as $-1 = 1$ for $\mathbb{F}_2$

&, minimal polynomial: $(x-t)^2$

$\sigma : t \to t$ id

$\mathrm{Gal}(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)) = \{id\}$

$\mathbb{F}_5(t)$

|

$\mathbb{F}_5(t^4)$

↑ galois

$x^4 - t^4 = f$

$x^4 - t^4 = (x^2 - t^2)(x^2 + t^2)$

$= (x-t)(x+t)(x^2 - 4t^2)$

$= (x-t)(x+t)(x-2t)(x+2t)$

$= (x-t)(x-4t)(x-2t)(x-3t)$

also, minimal polynomial deg 4 and all $i \to j$ for $i, j \in \mathbb{Z}/4\mathbb{Z}$ possible

$\Rightarrow \mathrm{Gal}(\mathbb{F}_5(t)/\mathbb{F}_5(t^4)) \cong \mathbb{Z}/4\mathbb{Z}$

$= \langle \sigma \rangle$

$\sigma : t \to 2t$

$\sigma^2 : t \to 4t$

$\sigma^3 : t \to 3t$

$\sigma^4 : t \to t$

2. K char $p > 0$ perfect if $K = K^p := \{ a^p : a \in K \}$

(a) any finite field has char $p > 0$

$\phi : x \to x^p$ $\qquad \phi : K \to K$

$\phi(x+y) = x^p + y^p$

$= \phi(x) + \phi(y)$

$\phi(xy) = \phi(x)\phi(y)$

also $\ker(\phi) = \{x \in K \mid x^p = 0\}$
$= \{0\}$

$\Rightarrow \phi$ is automorphism

$\Rightarrow K^p = K$

(b) $\forall a \in K$, $a^p \in K$ is trivial

$\Rightarrow \forall a^p \in K^p$, $a^p \in K$

$\Rightarrow K^p \subset K$

as not perfect

$K \ni a$ s.t $a \notin K^p \Rightarrow a^p \in K^p$

$\Rightarrow t^p - a^p \in K^p[t]$

K^p

then $(t^p - a^p) = (t-a)^p$

$(t^p - a^p)$: irreducible as $(t-a) \notin K^p[t]$ and only factor

$(t-a)^p$: inseparable

(c) M / $K = K^p$ $\Big) < \infty$ finite extension

now, $\forall \alpha \in M$, if $\min_K \alpha$ is separable, then we are done

let $f_\alpha = \min_K \alpha \in K[t] = K^p[t]$

(over $p > 0$)

f_α is separable iff $f_\alpha \notin K[t^p]$

(∵ theorem done in class)

now, $K[t^p] = K^p[t^p]$

so, if $f_\alpha \in K[t^p]$ i.e $K^p[t^p]$

then, $f_\alpha = \sum_{i=0}^{n} q_i^p (t^p)^p$

$= \left(\sum_{i=0}^{n} q_i t^p\right)^p$

$\sum_{i=0}^{n} q_i t^p \in K[t]$

but $f_\alpha = \min_K \alpha$ is irreducible $\Rightarrow f_\alpha \notin K^p[t^p]$

3. $d \mid n$ iff $t^d - 1 \mid t^n - 1$

($\Leftarrow$) let $n = dq + r$ then

$t^n - 1 = (t^{dq+r} - t^r) + (t^r - 1)$

now $t^d-1 \mid t^n-1 \Rightarrow \exists f(t)$ s.t

$$(t^d-1)f(t) = t^n-1$$
$$= t^{qd+r} - t^r + t^r - 1$$

t^d-1 common

$r<d$

$$t^d-1 \;\Big)\; t^{r+(q-1)d} + \cdots + t^{r+d} + t^r$$
$$t^{qd+r} - t^r + t^r - 1$$
$$t^{qd+r} - t^{(q-1)d+r}$$
$$\vdots$$
$$t^{r+d} - t^r$$
$$t^r - 1$$

as $t^d-1 \mid t^n-1$

$t^r = 1 \Rightarrow r = 0$

$\Rightarrow d \mid n$

($\Leftarrow$) If $d \mid n$ then $dq = n$ then from above trivial to see

$t^d-1 \mid t^n-1$

4. $a > 1 \in \mathbb{N}$ $d \mid n$ iff $a^d-1 \mid a^n-1$

this follows from above putting $f(t) = t^d-1$, $g(t) = t^n-1$

then $f(a) \mid g(a)$ iff $d \mid n$

now, $x^{p^d-1} - 1 \mid x^{p^n-1}$

iff $p^d-1 \mid p^n-1$

iff $d \mid n$

so, $x^{p^d-1} - 1 \mid x^{p^n-1}$ iff $d \mid n$

$\mathbb{F}_{p^d}$ = field as roots of $x^{p^d-1} - 1$ other than 0

$\mathbb{F}_{p^n}$ = field as roots of $x^{p^n-1} - 1$ other than 0

for all roots of $x^{p^d-1} - 1$ in $\mathbb{F}_{p^n}$ trivial to see

$$x^{p^d-1} - 1 \mid x^{p^n-1} - 1$$

5. $a \in \mathbb{F}_p^*$ $t^p - t + a \in \mathbb{F}_p[t]$ is irreducible and separable

$f(t) = t^p - t + a \in \mathbb{F}_p[t]$

now $df(t) = pt^{p-1} - 1 + 0$
$= -1 \neq 0$
$\Rightarrow f$ is seperable

if α is a root of $f(t)$
then

$\alpha^p - \alpha + a = 0$

also, $(\alpha+1)^p - (\alpha+1) + a = \alpha^p + 1 - \alpha - 1 + a$
$= \alpha^p - \alpha + a$

so, $\alpha, \alpha+1, \alpha+2, \ldots$ all are roots

if $\alpha \in \mathbb{F}_p$ then

$\alpha^{p-1} = \alpha \Rightarrow \alpha^p = \alpha \Rightarrow a = 0$ as $f(\alpha) = 0$
but $a \neq 0$

so, $\alpha \notin \mathbb{F}_p$, now if reducible then

$f(t) = g(t)h(t)$

$\alpha + i$ roots $i \in \mathbb{F}_p$

now, if g has roots $\alpha + i_1, \alpha + i_2, \ldots \alpha + i_k$

then sum of all roots

$k\alpha + \sum_{j=1}^{k} i_j \in \mathbb{F}_p$

$\Rightarrow k\alpha \in \mathbb{F}_p$

$k \in \mathbb{F}_p \Rightarrow \alpha \in \mathbb{F}_p$ but $\alpha \notin \mathbb{F}_p$
Irreducible

6. $t^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (t - \alpha)$

as $|\mathbb{F}_{p^n}| = p^n$ then

$\mathbb{F}_{p^n} \cong \operatorname{Spec}_{\mathbb{F}_p} f \quad f = t^{p^n - 1} - 1$

upto $\mathbb{F}_p$ isomorphism

then trivial to see $t^{p^n - 1} = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (t - \alpha)$

then $t = 0$: $1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (-\alpha)$

$1 = (-1)^{p^n - 1} \prod_{\alpha \in \mathbb{F}_{p^n}^*} (\alpha)$

$(-1)^{p^n} \bmod p = \prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha$

also, now $n = 1$: $(-1)^p \bmod p = \prod_{\alpha \in \mathbb{F}_p^*} \alpha = (1)(2)\cdots(p-1)$

now, $p \to$ odd $\quad (-1) \bmod p = (p-1)!$

$p=2$ then $1 \bmod 2 = 1 = 1$ trivial

so, in both cases

$$(p-1)! = -1 \bmod p$$

7. $f(t_1, t_2, \dots t_n) \in \mathbb{Z}[t_1, t_2, \dots t_n]$ n variable polynomial $t_1, t_2, \dots t_n$

let $f(t) = a(t) + b(t)$

then $f^p = a^p(t) + b^p(t) \bmod p$

Similarly $f = \sum q_k t_1^{k(1)} \dots t_n^{k(n)}$

$$f^p = \sum q_k^p t_1^{pk(1)} \dots t_n^{pk(n)} \bmod p$$

now, $\sum q_k^p t_1^{pk(1)} \dots t_n^{pk(n)}$

$q_k^p = q_k \bmod p$

$$\Rightarrow \sum q_k^p t_1^{pk(1)} \dots t_n^{pk(n)} = \sum q_k t_1^{pk(1)} \dots t_n^{pk(n)} \bmod p$$

$$\Rightarrow f^p = f(t_1^p, \dots t_n^p) \bmod p$$

8. $\phi : K[t] \to K[t]$ K-homomorphism

$t \longmapsto at+b$

$a, b \in K \quad a \neq 0$

$\phi|_K = id$

then ① $\phi(f(t) + g(t)) = f(at+b) + g(at+b)$

$= \phi(f(t)) + \phi(g(t)) \quad \forall t$

② $\phi(f(t)g(t)) = f(at+b) \cdot g(at+b)$

$= \phi(f(t)) \cdot \phi(g(t)) \quad \forall t$

③ $\forall f(t) \in K[t], \exists g(t) = f(a^{-1}(t-b))$ s.t

$\phi(g(t)) = g(at+b) = f(t) \quad \forall t$

④ $\phi(f) = \phi(g)$

$\Rightarrow f(at+b) = g(at+b) \quad \forall t$

$\Rightarrow f(a(a^{-1}(t-b))+b) = g(a(a^{-1}(t-b))+b)$

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

$\Rightarrow f \equiv g$

so, from ①, ②, ③, ④ $\phi \in Aut_K(K[t])$

$\phi : K[t] \longrightarrow K[t]$ is k-isomorphism

then $t \longrightarrow f(t)$
s.t $\forall\ g \in K[t]$
$\exists\ r \in K[t]$ s.t
$\phi(r) = g$

but if $\deg f \geq 2$

then $g = r(f(t))$
$\deg \geq 2$

so not true for g deg < 2

$\Rightarrow \deg f = 1$

so, $f = at + b$ $a \neq 0$ for deg 1
as deg 0 not possible
as one-one

9. $\alpha = \frac{f(t)}{g(t)} \in K(t)$, $f(t), g(t) \in K[t]$ comaximal
$g(t) \neq 0$

$K(t)$
|
$K(\alpha)$ $\quad \alpha = \frac{f(t)}{g(t)}$ $\quad \deg\left(\min_{K(\alpha)} t\right) = [K(t) : K(\alpha)]$
|
K

(a) $f(X) - \alpha g(X) \in K[\alpha][X]$

irred in $K[\alpha][X]$ iff irred in $K[X][\alpha]$ ($\because$ gauss)

then trivial $f(X) - \alpha g(X)$ irred

(b) now as $f(X) - \alpha g(X) \in K[\alpha][X]$

then $\deg(f(X) - \alpha g(X)) \geq \deg(f)$ & $\deg(g)$

$\Rightarrow \deg(f(X) - \alpha g(X)) = \max\{\deg f, \deg g\}$

(c)

$K(t)$
|
$K(\alpha)$ $\quad \Big)\ \min_{K(\alpha)} t = f(X) - \alpha g(X)$
($\because$ irred & root of t)

Now, $\deg \min_{K(\alpha)} t = \max\{\deg f, \deg g\}$

so, $[K(t) : K(\alpha)] = \max\{\deg f, \deg g\}$

(d) let $\sigma \in Aut(K(t)/K)$

then $\sigma : K(t) \longrightarrow K(t)$
$\sigma|_K = id_K$

$\sigma : t \mapsto f(t)/g(t)$

$\sigma(t) = \frac{f(t)}{g(t)}$

now $K(t) = K\left(\underbrace{\frac{f(t)}{g(t)}}_{\alpha}\right)$

$= K(\alpha)$

$\Rightarrow [K(t) : K(\alpha)] = 1$

$\Rightarrow \max\{\deg f, \deg g\} = 1$

$\Rightarrow t \mapsto \frac{at+b}{ct+d}$

were one-one and onto

so, $t \leftarrow \frac{at+b}{ct+d}$

i.e $\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0 \Rightarrow ad - bc \neq 0$

10. $G = Aut(\mathbb{F}_2(t)/\mathbb{F}_2)$ $Fix(G)$ is basic ($\because$ theorm done in tutorial)

$\mathbb{F}_2(t)$ then $\sigma : t \longrightarrow \frac{at+b}{ct+d}$

$|$

$\mathbb{F}_2$ $a, b, c, d \in \mathbb{F}_2$ $ad - bc \neq 0$

i.e $t, t+1, \frac{t}{t+1}, \frac{1}{t}, \frac{1}{t+1}, \frac{t+1}{t}$

so, $|G| = 6$ $G = \{\sigma : t \to r(t)\}$

now $Fix(G) = \{f \in \mathbb{F}_2(t) \mid f(\sigma(t)) = f(t) \ \forall \sigma \in G\}$

$\frac{(t^2+t+1)^3}{(t^2+t)^2} = \frac{t\left(t+\frac{1}{t}+1\right)^3}{(t+1)^2}$

then $t^2+t+1 \longrightarrow t^2+1+t+1+1$

$t^2+t \longrightarrow t^2+1+t+1$

$\frac{1}{t} \to \frac{\frac{1}{t}\left(\frac{t+1}{t}+1\right)^3}{\frac{(t+1)^2}{t^2}}$ same

$\frac{1}{t+1}$ same as well, same for $\frac{t}{t+1}, \frac{t+1}{t}$

so, $\mathbb{F}_2\left(\frac{(t^2+t+1)^3}{(t^2+t)^2}\right)$ is the $\mathrm{Fix}(G)$

11. $\mathbb{F}_p(t)$ $\sigma(t)=at+b$ $a\in\mathbb{F}_p^*$ $b\in\mathbb{F}_p$

$G=\{\sigma(t)=at+b \mid a\in\mathbb{F}_p^*, b\in\mathbb{F}_p\}$

$|G|=p(p-1)$

also $\alpha\in\mathbb{F}_p$ $\alpha^{p-1}=1$

$\alpha^p=\alpha$

$(t^p-t)\longrightarrow (at+b)^p-(at+b)$

$= a^p t^p + b^p - at - b$

$= a^p(t^p-t)$

so, $(t^p-t)^{p-1}$ is s.t

$f(t)=(t^p-t)^{p-1}\in\mathbb{F}_p(t)$

then

$f(\sigma(t))=f(t)\ \forall\ \sigma\in G$

also G is basic $\Rightarrow$ $G=\mathbb{F}_p\left((t^p-t)^{p-1}\right)$

12. $G=\langle\sigma\rangle\leq \mathrm{Aut}(\mathbb{R}(X,Y)/\mathbb{R})$

$\sigma: \begin{matrix} X\longrightarrow -X \\ Y\longrightarrow Y \end{matrix}$

$\mathrm{Fix}(G)=\{f\in\mathbb{R}(X,Y) \mid f(\sigma(X,Y))=f(X,Y)\}$

now, $\sigma^2=\mathrm{id}$ $-X, X$ same

then $f\in\mathbb{R}(X^2,Y)$

then $f(\sigma(X,Y))=f(X,Y)$ trivial as X^2

so, $\mathrm{Fix}(G)=\mathbb{R}(X^2,Y)$

$\begin{matrix} X\longrightarrow -X \\ Y\longrightarrow -Y \end{matrix}$ then $\mathbb{R}(X^2,Y^2)$

$\begin{matrix} X\longrightarrow Y \\ Y\longrightarrow X \end{matrix}$ form of f

then $t^2-(X+Y)t+XY$ i.e roots X,Y

$\Rightarrow \mathbb{R}(X+Y, XY)$

so, $\mathbb{R}(\sigma(X+Y),\sigma(XY))=\mathbb{R}(X+Y,XY)$

13. $L = K(t_1, \dots t_n)$

$S_n \leq Aut(L|K)$ $\quad \sigma \in S_n$

$\sigma(t_i) = t_{\sigma(i)}$

$Fix(S_n) = K(S_1 \dots S_n)$

$S_1 = \sum t_i \quad S_2 = \sum_{i<j} t_i t_j \quad S_3 = \sum_{i<j<k} t_i t_j t_k \dots \quad S_n = t_1 t_2 \dots t_n$

now, $Fix(S_n) = \{ f \in K(t_1, t_2, \dots t_n) \mid f(\sigma(\underset{\sim}{t})) = f(\underset{\sim}{t}) \}$

$\forall \sigma \in S_n$

i.e $f(t_1, t_2 \dots t_n) = f(t_{\sigma(1)}, t_{\sigma(2)}, \dots t_{\sigma(n)})$

we know $\sigma\left(\prod_{i=1}^{n}(X - t_i)\right) = \prod_{i=1}^{n}(X - t_i)$

now $\prod_{i=1}^{n}(X - t_i) = X^n - (\sum_{i=1}^{n} t_i) X^{n-1} + (\sum_{i<j} t_i t_j) X^{n-2} + \dots + (-1)^n t_1 t_2 \dots t_n$

so, $fix(S_n)$ of form

$K[S_1, S_2, \dots S_n]$

as all $f \in K[S_1, S_2 \dots S_n]$

$\sigma(f) = f$ as $\sigma(S_i) = S_i \ \forall \ i$

<u>Theorm</u> : $K[S_1, S_2, \dots S_n]$ is a polynomial ring st

$f(X_1, X_2 \dots X_n) \in K[X_1, X_2, \dots X_n]$

$f(S_1, S_2, \dots S_n) = 0$ then $f \equiv 0$

14. $\sigma \in Aut(\mathbb{Q}(t)/\mathbb{Q})$

$\sigma(t) = t+1 \quad Fix(\sigma) = \{ f \in \mathbb{Q}(t) \mid f(\sigma(t)) = f(t) \}$

$\sigma(t) = t+1$
i.e $\quad t \to t+1$

$\sigma\left(\frac{f(t)}{g(t)}\right) = \frac{f(t)}{g(t)}$

$\frac{f(t+1)}{g(t+1)} = \frac{f(t)}{g(t)}$

$f(t+1)\, g(t) = f(t)\, g(t+1)$

$p(t) = g(t) f(t+1) - f(t) g(t+1)$

now, $P(t)$ is a polynomial

if α root of f

then $P(\alpha) = g(\alpha) f(\alpha+1) \quad g(\alpha) \neq 0$

$$\frac{f(\alpha+1)}{g(\alpha+1)} = \frac{f(\alpha)}{g(\alpha)} = 0$$

$$f(\alpha+1) = 0$$

$$\Rightarrow P(\alpha) = 0$$

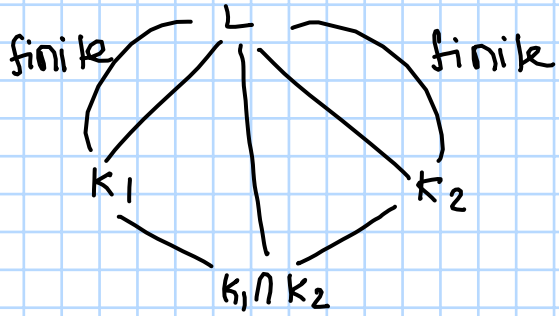
then, $\frac{f(\alpha+2)}{g(\alpha+2)} = \frac{f(\alpha+1)}{g(\alpha+1)} = 0$

$$\Rightarrow f(\alpha+2) = 0$$

$$\Rightarrow f \equiv 0 \ (\because \alpha+i \text{ is a root})$$

$\therefore$ $Fix(\sigma) = \mathbb{Q}$ ($\because$ no such polynomial)

15.



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

$K_1 = \mathbb{Q}(t^2)$

$K_2 = \mathbb{Q}(t^2+t)$

then as $X^2 - t^2 \in \mathbb{Q}(t^2)[X]$

$$f(X) \overset{s.t}{=} X^2 - t^2$$

$$f(t) = 0$$

$$\Rightarrow [\mathbb{Q}(t) : \mathbb{Q}(t^2)] < \infty$$

also, $g(X) = X^2 + X - (t^2+t) \in \mathbb{Q}(t^2+t)[X]$

s.t $g(t) = 0 \Rightarrow [\mathbb{Q}(t) : \mathbb{Q}(t^2+t)] < \infty$

but $\mathbb{Q}(t^2) \cap \mathbb{Q}(t^2+t) = \mathbb{Q}$

as $t^2 \notin \mathbb{Q}(t^2+t)$ & $t^2+t \notin \mathbb{Q}(t^2)$

but $[\mathbb{Q}(t) : \mathbb{Q}]$ not finite

16. cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$

primitive n roots: ζ_n^m $1 \leq m < n$ m, n coprime

$\langle \zeta_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$

ζ_n^m corresponds to generator $\bar{m}$ in $\mathbb{Z}/n\mathbb{Z}$

$\Phi_n(t) = \prod (t - \zeta_n^m)$ n^{th} cyclotomic polynomial

(a) $t^n - 1 = \prod_{d|n} \Phi_d(t)$

now $t^n - 1 = \prod_{i=0}^{n-1} (t - \zeta_n^i)$



order d for $d|n$

if $(\zeta_n^m)^d = 1$

then $d = \frac{n}{\gcd(m,n)}$

as $(\zeta_n^m)^d = 1$

so, ζ_n^k is primite d^{th} root of unity

$M_n = \bigsqcup_{d|n} \{\alpha \in M_n \mid \text{ord}(\alpha) = d\}$

$t^n - 1 = \prod_{d|n} \left(\prod_{\text{ord}(\alpha)=d} (t - \alpha) \right)$

$= \prod_{d|n} \Phi_d(t)$

(b) $\Phi_n(t) = \prod_{\text{ord}(\alpha)=n} (t - \alpha)$

↑

order n for $d = \frac{n}{\gcd(m,n)} = n$

$\Rightarrow \gcd(n,m) = 1$

i.e coprimes

$\Phi_n(t) = \prod_{\substack{\gcd(m,n)=1 \\ m \in \{1,2,\ldots n-1\}}} (t - \zeta_n^m)$

$n=1$ trivial, for $n>1$ $t^n - 1 = \prod_{d|n} \Phi_d(t)$ $\Phi_d(t) \in \mathbb{Z}[t]$ monic for $d<n$ by inductive

then $t^n - 1 = f(t)\Phi_n(t)$ $f(t) \mid t^n - 1$ in $\mathbb{Q}(\zeta_n)[t]$ and both monic in $\mathbb{Z}[t]$

$\Rightarrow f(t) \mid t^n - 1$ in $\mathbb{Q}[t]$ ($\because \zeta_n$ does not as both in $\mathbb{Z}[t]$)

$\Rightarrow f(t) \mid t^n - 1$ in $\mathbb{Z}[t]$

So, $\Phi_n(t)$ is monic in $\mathbb{Z}[t]$

(c) $\Phi_n(t)$ is deg $\phi(n)$

$\phi(n)$ = no of $m<n$ s.t $\gcd(m,n)=1$

$\phi(p)$ = no of $m<p$ s.t $\gcd(m,p)=1$

as p is prime

$m \in \{1,2,\dots p-1\}$

$\Rightarrow \phi(p) = p-1$

$$\phi(\underbrace{n_1,n_2}_{\text{coprimes}}) = \left|\{m<n_1n_2 \mid \gcd(m,n_1n_2)=1\}\right|$$

$$= \left|\{m<n_1n_2 \mid \gcd(m,n_1)=1 \text{ and } \gcd(m,n_2)=1\}\right|$$

$$n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$$

$$\phi(n) = n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$$

now $\gcd(m,n_1n_2)=1$ iff $\gcd(m,n_1)=1$ and $\gcd(m,n_2)=1$

($\because$ Chinese remainder theorem)

so, $\phi(n_1n_2) = \phi(n_1)\phi(n_2)$

$\phi(p^r) = p^{r-1}(p-1)$

as, $\{m<p^r \mid \gcd(m,p^r)=1\}$

$1,2,\dots p-1$ ($p-1$), $p+1,\dots 2p-1$, $2p+1,\dots 3p-1$, $3p+1,\dots p^{r-1}(p)-1$

(p : no p form; $p-1$; $p-1$; ....)

$$(p^{r-1})(p-1) = \phi(p^r)$$

(d) Theorem: $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible

Tutorial-8:

1. $\mathbb{Q}(2^{\frac{1}{4}}, i)$ ← spl of t^4-2
   |
   $\mathbb{Q}(i)$
   $\mathbb{Q}(\sqrt[n]{2}, \zeta_n)$ is galois
   |
   $\mathbb{Q}(\zeta_n)$

$\mathbb{Q}(t)$ → spl of $X^2-t^2=(X-t)(X+t)$ quadratic
|
$\mathbb{Q}(t^2)$

$\mathbb{F}_p(t)$
|
$\mathbb{F}_p(t^2)$ not separable for $p=2$

$\mathbb{F}_2(t)$ $\quad X^2-t^2=(X-t)^2$
|
$\mathbb{F}_2(t^2)$

$\mathbb{F}_p(t^2)$ $\quad X^2-t^2=(X-t)(X+t)$
$df=2X\neq 0$
so, $\mathbb{F}_p(t)$ separable

well $\quad K(\alpha)$ if α separable
|) then all $K(\alpha)$ separable
K

$\mathbb{R}(t)$ $\quad X^3-t^3=(X-t)(X-\omega t)(X-\omega^2 t)$
|
$\mathbb{R}(t^3)$ Not normal

2. $\mathrm{Gal}_{\mathbb{Q}}(f)=\mathrm{Gal}_{\mathbb{Q}}(t^4-2)$
$=D_4$ (we have seen it)
$\rho^4=\tau^2=1 \quad \tau\rho\tau=\rho^{-1}$
$\rho(\sqrt[4]{2})=i\sqrt[4]{2} \quad \rho(i)=i$
$\tau(i)=-i \quad \tau(\sqrt[4]{2})=\sqrt[4]{2}$

$|\mathrm{Aut}(K/\mathbb{Q})|=[K:\mathbb{Q}]$
$\mathrm{Gal}(K/\mathbb{Q})$ find all subgroup

4. deg$n$ $\mathrm{Gal}_K(f)\leq S_n$
order roots, and similar to before

5. f no rep roots

$\{\alpha_1 \dots \alpha_n\}$ our f has r orbits

r may ind polynomials

$a_0 + a_1 x + \cdots + a_k x^k = f(x)$ irred

$\alpha_i \xrightarrow{\sigma} \alpha_j$ exist

$\sigma \in \mathrm{Gal}(K/F)$

$f(\alpha) = 0$

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

$\sigma(\alpha)$ minimal

in one orbit $\alpha_1, \alpha_2 \dots \alpha_n$ acts $\mathrm{Gal}(K/\mathbb{Q})$ ↑ K | $\mathbb{Q}$

$\alpha_i \to \alpha_n$ orbits r: $O_1 \dots O_r$

↑ all roots mapped inside

$\sigma(O_i) = O_i$

$\underbrace{\alpha_1, \alpha_2 \dots \alpha_k}_{O_1} \quad \underbrace{\alpha_{k+1}, \dots \alpha_n}_{O_2} \dots$

$f = g_1 g_2 \dots g_r$

↑ all ind roots are O_i for g_i

$g(x) = \prod_{i=1}^{k} (x - \alpha_i) \in \mathbb{Q}[x]$ is irred and inside $\mathbb{Q}[x]$ then we are done

K | $\mathbb{Q}$) $\mathrm{fix}(\mathrm{Gal}(K/\mathbb{Q})) = \mathbb{Q}$

$\sigma(g) = g \ \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$

$\Rightarrow g$ is fixed

$\Rightarrow g \in \mathbb{Q}[t]$

$g(x) = h_1(x) \cdots h_j(x)$

$S_1 \cup S_2 = O_i$

all roots in O_i → No other orbit

so, g is irreducible

7. M | gal | K ; K' | fin | K

MK' | K' $\quad \mathrm{Gal}(MK'|K') \cong \mathrm{Gal}(M|M \cap K') \subset \mathrm{Gal}(M|K)$



$M = spl_K(f)$ MK' K'/K finite

$f(x) \in K[x] \subset K'[x]$

$\Rightarrow MK' = spl_{K'}(f)$

$\downarrow$

MK' is galois as f is seperable

$MK'/K' = spl_{K'}(f)$

then $Gal(MK'/K') \cong Gal(M/M \cap K')$

$\delta : Gal(MK'/K') \longrightarrow Gal(M/K)$

$\sigma \longrightarrow \sigma|_M$

$\sigma \in Gal(MK'/K')$ M/K Normal $\rightarrow \sigma(M) \subseteq M$ (∵ done previously)

MK
$\cup$
M
$\cup$
K

$\ker \delta = \{\sigma \in Gal(MK'/K') \mid \sigma|_M = id\}$

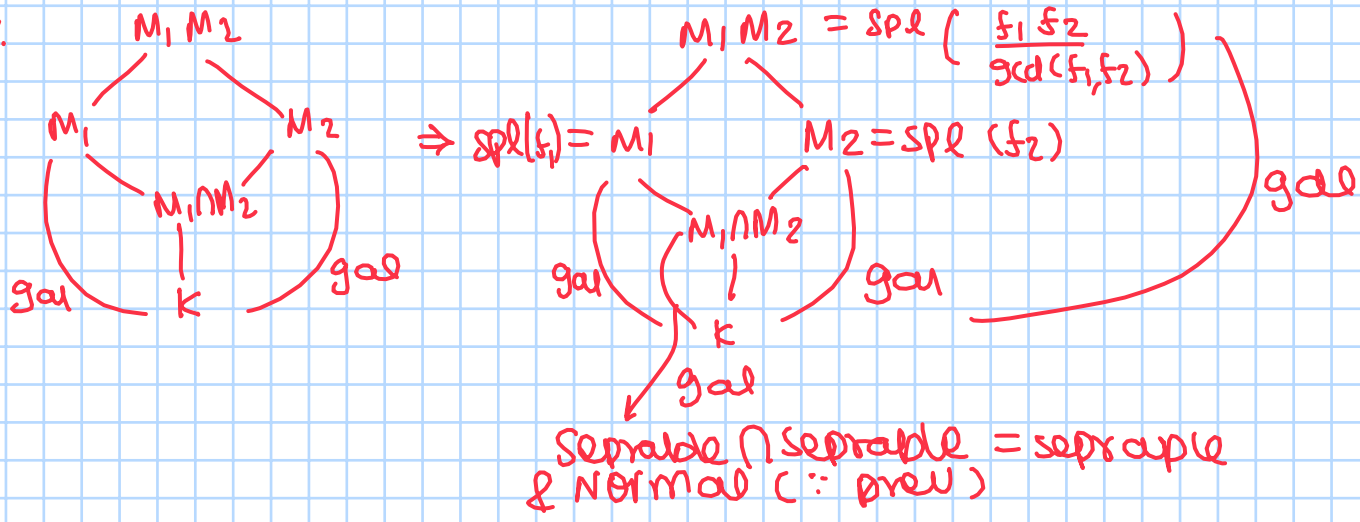
$= id$ as $\sigma(m) = m \ \forall m \in M$

δ is injective $H = Img(\delta)$

$Fix(H) = M \cap K'$ by defn of σ

$Gal\left(\frac{M}{Fix H}\right) = H = Img(\delta)$

8.



Seprable ∩ seprable = seprable
& Normal (∵ prev)

$\phi : Gal(M_1M_2/K) \longrightarrow Gal(M_1/K) \times Gal(M_2/K)$

$\sigma \longmapsto (\sigma|_{M_1}, \sigma|_{M_2})$

$\sigma : M_1 \to M_1 \qquad \sigma : M_2 \to M_2$

$\Sigma M_{i_1}, M_{i_2}$ $\begin{cases} \sigma|_{M_1} = id_{M_1} \\ \sigma|_{M_2} = id_{M_2} \end{cases}$

$\ker$ = trivial

$\Rightarrow$ injetive map

$H = \{(\sigma, \tau) \mid \sigma = \tau \text{ on } M_1 \cap M_2\}$

$M_1 \cap M_2 = K$ $\quad M_1 M_2 \; MK'$



from 7. $Gal(M_1K'/K') \cong Gal(M_1/K)$

$[M_1M_2 : M_2] = [M_1 : K]$

$|Gal(M_1M_2/K)| = [M_1M_2 : K]$

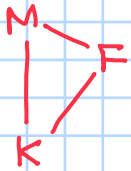
then ϕ and on both side equal
+ one-one
$\Rightarrow \phi$ is subjetive
$\Rightarrow$ isomorphism

9. $F_p(x,y)/F_p(x^p, y^p)$

inf many subfields

$M = K(\alpha)$ basic extension
$|$ $\uparrow$ primite element
K

primite element theorm: normal



$\Leftrightarrow$ basic

if only finitely many intermed extions

M/K iff basic

$\mathbb{Q}(\sqrt[3]{2}, \omega)$ normal finite + separable

$|$ $\quad \tilde{M} \to$ smallest galois cont K
$\mathbb{Q}$ $\quad M \to K$

so if finite separable $M = k(\alpha)$ form

$\mathbb{F}_p(x,y) \neq k(\alpha)$ $\forall \alpha$ then done

$\mathbb{F}_p(x^p, y^p)$ deg p

p2 degree $\frac{f(x,y)}{g(x,y)} = u$ $u^p = \frac{(f(x,y))^p}{(g(x,y))^p} = \frac{f(x^p,y^p)}{g(x^p,y^p)} \in \mathbb{F}_p(x^p, y^p)$

so not basic

$\mathbb{F}_p(x,y)$

$\mathbb{F}_p(x^p, y^p, x+y\lambda^{p^n})$

$\mathbb{F}_p(x^p, y^p)$

1. $\mathbb{Q}(\sqrt{2})$ / $\mathbb{Q}$ char $=0 \Rightarrow$ separable
also $\min_{\mathbb{Q}} \sqrt{2} = t^2 - 2$ splits in $\mathbb{Q}$
$\Rightarrow$ all $\alpha \in \mathbb{Q}(\sqrt{2})$ splits in $\mathbb{Q}$
so, $\mathbb{Q}(\sqrt{2})$ / $\mathbb{Q}$ is galois extension

$\mathbb{Q}(\sqrt[4]{2})$ / $\mathbb{Q}$ char $=0 \Rightarrow$ separable
also, $\min_{\mathbb{Q}} \sqrt[4]{2} = t^4 - 2$
but $i \notin \mathbb{Q}(\sqrt[4]{2})$, so $\sqrt[4]{2}$ does not split in $\mathbb{Q}(\sqrt[4]{2})$
i.e extension not galois

$\mathbb{Q}(\sqrt[4]{2})$ / $\mathbb{Q}(\sqrt{2})$ char 0 $\Rightarrow$ separable
also $\min_{\mathbb{Q}(\sqrt{2})} \sqrt[4]{2} = t^2 - \sqrt{2} = (t - \sqrt[4]{2})(t + \sqrt[4]{2})$ splits in $\mathbb{Q}(\sqrt[4]{2})$
so, extension is galois

$\mathbb{Q}(\sqrt[4]{2}, i)$ / $\mathbb{Q}(i)$ separable as char $=0$
also $\min_{\mathbb{Q}(i)} \sqrt[4]{2} = t^4 - 2^4$ splits in $\mathbb{Q}(\sqrt[4]{2}, i)$
so, galois

$\mathbb{Q}(t)$ char $=0 \Rightarrow$ seperable
$|$
$\mathbb{Q}(t^2)$ $\min_{\mathbb{Q}(t^2)} t = (X-t)(X+t)$ splits in $\mathbb{Q}(t)$

$\Rightarrow$ Normal

so, galois extension

$\mathbb{F}_p(t)$ ① Normal is from before
$|$
$\mathbb{F}_p(t^2)$ ② $\min_{\mathbb{F}_p(t^2)} t = (X-t)(X+t)$
if $-1=1$ then not seprable

so $p=2$ Not seprable
$p \neq 2$ seprable

so, galois if $p \neq 2$, if $p=2$ not galios

$\mathbb{R}(t)$ $\min_{\mathbb{R}(t^3)} t = X^3 - t^3 = (X-t)(X-\omega t)(X-\omega^2 t)$ does not split in $\mathbb{R}(t)$
$|$
$\mathbb{R}(t^3)$

so, not galios

2. $\mathrm{Gal}_{\mathbb{Q}}(f)$ $\mathrm{spl}_K(f)/\mathbb{Q}$

$(t^2-t)(t^2-3) = f(t)$

now $f(t) = (t)(t-1)(t-\sqrt{3})(t+\sqrt{3})$

$0 \to 0$
$1 \to 1$
$\sqrt{3} \to \pm\sqrt{3}$

so, $\mathrm{gal}(f) = \{id, K\}$
$K(\sqrt{3}) = -\sqrt{3}$ else all same

i.e $\mathrm{gal}_{\mathbb{Q}}(f) = \{id, K\} \cong \mathbb{Z}/2\mathbb{Z}$ so, $\{e\}$ only subgroup corresponds to $\mathbb{Q}$

now, $\mathrm{spl}_K(f)/\mathbb{Q} = \mathbb{Q}(\sqrt{3})$
$|$
$\mathbb{Q}$

$(t^4-1)(t^2-5) = f(t)$

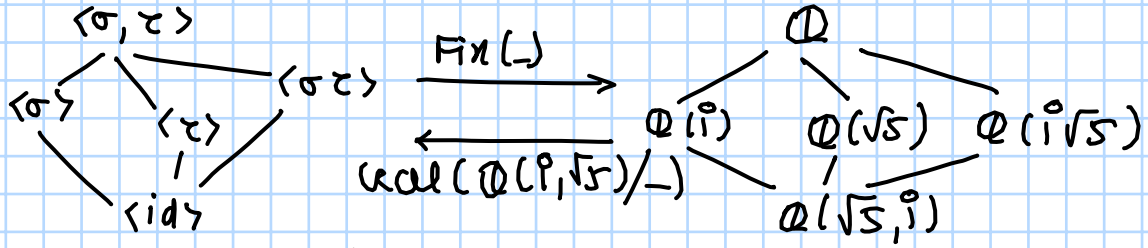
$f(t) = (t-i)(t-1)(t+1)(t+i)(t-\sqrt{5})(t+\sqrt{5})$

$\mathrm{Gal}_{\mathbb{Q}} f = \langle \sigma, \nu \rangle$ $\sigma: \sqrt{5} \to -\sqrt{5}$, $i \to i$ $\nu: \sqrt{5} \to \sqrt{5}$, $i \to -i$

$\mathrm{spl}_{\mathbb{Q}} f = \mathbb{Q}(i, \sqrt{5})$

now $\langle \sigma, \tau \rangle$ σ order 2 ν order 2
total order 4

$\langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle$ subgroups of order 2



$$\mathrm{Fix}(\sigma) = \{\alpha \mid \sigma(\alpha)=\alpha,\ \alpha \in \mathbb{Q}(i,\sqrt{5})\}$$

$\sigma : \sqrt{5} \to -\sqrt{5}$, $i \to i$ $\quad \mathrm{Fix}(\sigma) = \mathbb{Q}(i)$

$\mathrm{Fix}(\tau) = \mathbb{Q}(\sqrt{5})$

$\sigma\tau : \sqrt{5} \to -\sqrt{5}$, $i \to -i$

$\mathrm{Fix}(\sigma\tau) = \mathbb{Q}(i\sqrt{5})$

$t^5 - 1 = f(t)$

$\mathrm{spl}_{\mathbb{Q}} f = \mathbb{Q}(\zeta_5)$

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4 = \left|\mathrm{Gal}_{\mathbb{Q}}(f)\right|$$

also $\min_{\mathbb{Q}} \zeta_5 = 1 + t + t^2 + t^3 + t^4$

$\mathbb{Q}(\zeta_5)$ / $\mathbb{Q}$) galois extension

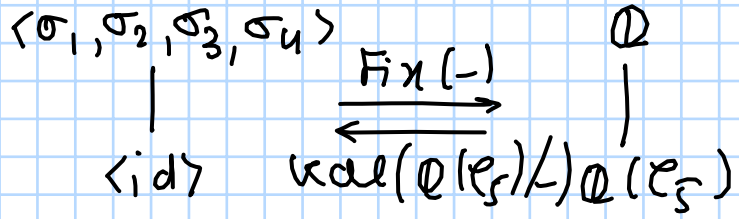
now as $\sigma_i : \zeta_5 \to \zeta_5^i$

$i = 1,2,3,4$ part of $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\zeta_5)$

$$\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\zeta_5) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

or $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\zeta_5) \cong (\mathbb{Z}/5\mathbb{Z})^\times$ or C_4

C_4 has $\{1\}, C_4$ as subgroups, so



$$(t^4+1) = (t^2+1)(t^2-i)$$
$$= (t+i)(t-i)(t+\sqrt{i})(t-\sqrt{i})$$

$\underset{\mathbb{Q}}{spl}(t^4+1) = \mathbb{Q}(\sqrt{i})$

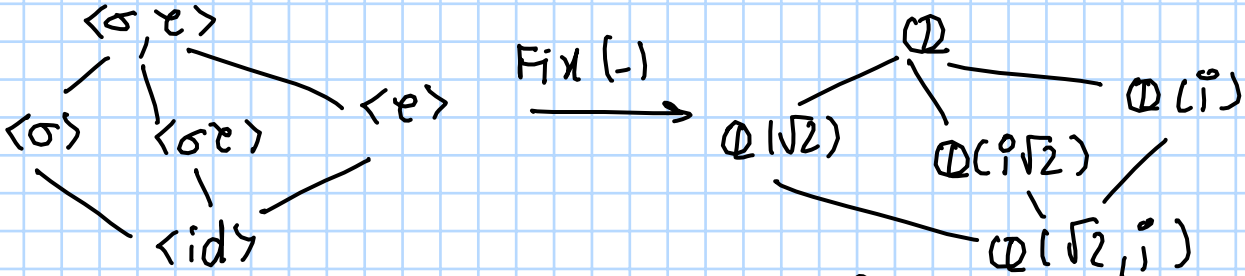
now, $\underset{\mathbb{Q}}{Gal}(\mathbb{Q}(\sqrt{i}))$

$\sqrt{i}$ as $i = e^{i\pi/2}$ $\quad \sqrt{i} = e^{i\pi/4} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)$

$= \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

now, $\sigma : \sqrt{2} \to \sqrt{2}$, $i \to -i$ $\quad \tau : \sqrt{2} \to -\sqrt{2}$, $i \to i$

so, $\underset{\mathbb{Q}}{Gal}(\mathbb{Q}\sqrt{i}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle \tau, \sigma \rangle$



as, $\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ is s.t $\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)^2 = \frac{1}{2} + \frac{(-1)}{2} + \frac{2i}{2}$

$\Rightarrow i \in \mathbb{Q}\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)$

also, $\frac{i}{\sqrt{2}} - \frac{1}{\sqrt{2}} = i\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)$

$\Rightarrow \left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) - \left(\frac{i}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right) \in \mathbb{Q}(\sqrt{i})$

$\Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{i})$

so, $\mathbb{Q}(\sqrt{i}) = \mathbb{Q}(\sqrt{2}, i)$

$\underset{\mathbb{Q}}{spl}(t^3-5) = \mathbb{Q}(\sqrt[3]{5}, \omega)$ galois extension

$\mathbb{Q}$

$\mathbb{Q}(\sqrt[3]{5}, \omega)$ — 3 — $\mathbb{Q}(\omega)$ — 2 — $\mathbb{Q}$

$[\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}] = 6$

$\Rightarrow \left|\underset{\mathbb{Q}}{Gal}(t^3-5)\right| = 6$

but $\underset{\mathbb{Q}}{Gal}(t^3-5) \leq S_3$

$\Rightarrow \underset{\mathbb{Q}}{Gal}(t^3-5) \cong S_3$

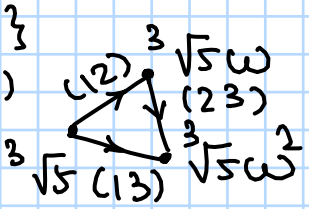
now, $S_3 = \{e, (12), (13), (23), (123), (132)\}$

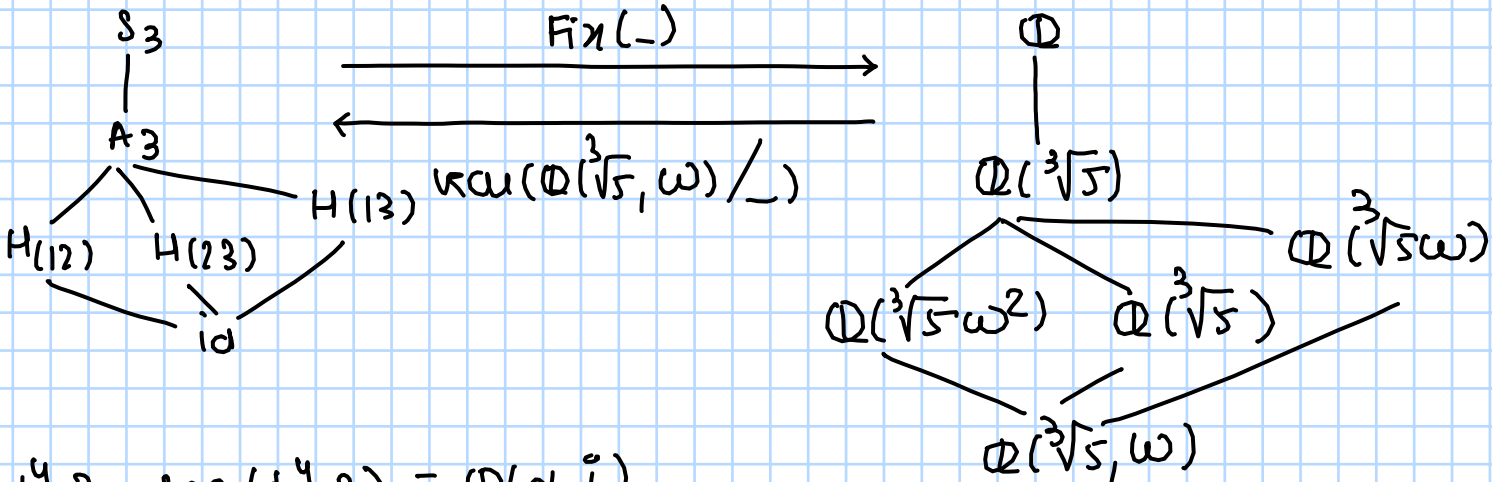
order 1: $\{e\}$

order 2: $\{e, (12)\}$, $\{e, (13)\}$, $\{e, (23)\}$ ($H(12)$, $H(13)$, $H(23)$)

order 3: $\{e, (123), (132)\} = A_3$

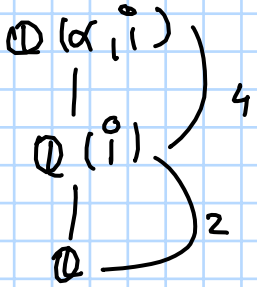
order 6: S_3





$t^4 - 2$ $\quad \mathrm{Spe}_{\mathbb{Q}}(t^4-2) = \mathbb{Q}(\alpha, i)$

$\alpha = 2^{1/4}$

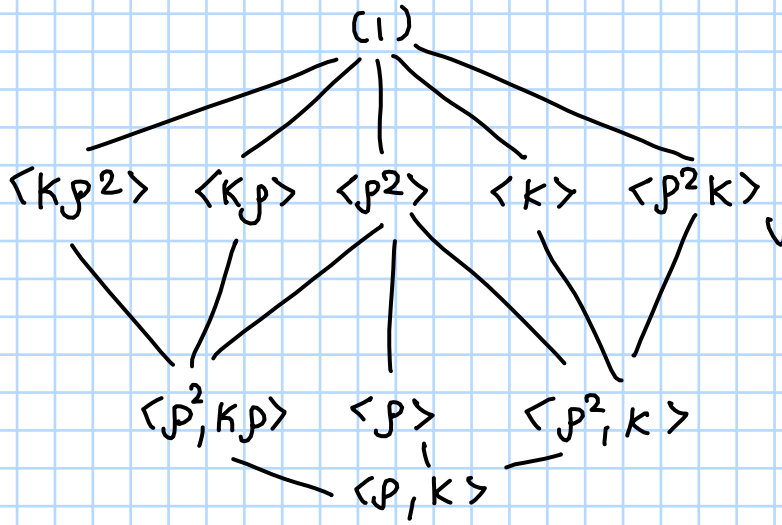


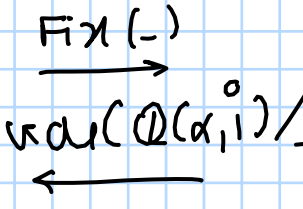
$|\mathrm{Gal}_{\mathbb{Q}} f| = 8$

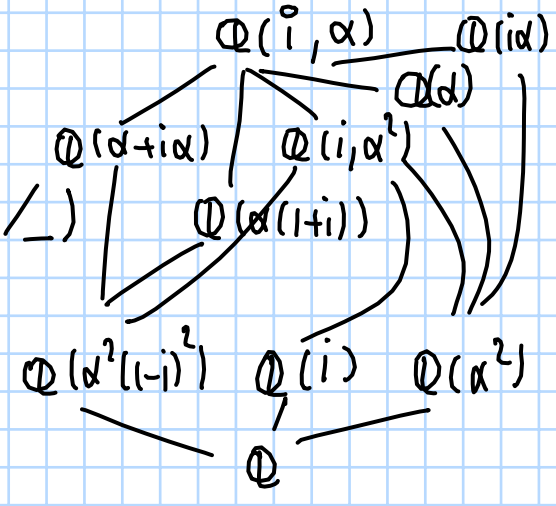
$\rho : \alpha \to i\alpha$, $i \to i$ $\qquad \rho^4 = 1$

$\kappa : \alpha \to \alpha$, $i \to -i$ $\qquad \kappa^2 = 1$

So, $D_4 \cong \mathrm{Gal}_{\mathbb{Q}} f$







$\underset{\mathbb{Q}}{spe}(t^3-1) = \mathbb{Q}(\omega)$

$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$

so, $\left| \underset{\mathbb{Q}}{Gal}(t^3-1) \right| = 2$

now $\Rightarrow \underset{\mathbb{Q}}{Gal}(t^3-1) \cong C_2$ or $\left(\mathbb{Z}/3\mathbb{Z}\right)^\times$

also $\sigma : \omega \to \omega^2$
s.t $\sigma : \omega^2 \to \omega$

so, $\underset{\mathbb{Q}}{Gal}(t^3-1) = \langle \sigma \rangle$

$$(1) \quad \xrightarrow{\text{Fix}(-)} \quad \mathbb{Q}(\omega)$$
$$\langle \sigma \rangle \quad \xleftarrow{Gal(\mathbb{Q}(\omega)/-)} \quad \mathbb{Q}$$

3. $\underset{\mathbb{Q}}{Gal}(f) \leq S_4$

as $f = t^4 - 2$ generated by $(1\,3\,2\,4)$, $(3\,4)$

as roots are $\{\alpha, -\alpha, \alpha i, -\alpha i\}$

$(1\,3\,2\,4)$ same as ρ

$(3\,4)$ same as κ

4. deg of $f = n$ then tion after ordering roots trivially

$(t^2-t)(t^2-3)$ S_4 roots $= (0, 1, \sqrt{3}, -\sqrt{3})$

generated by $(3\,4)$

$(t^4-1)(t^2-5)$ roots $= (1, -1, i, -i, \sqrt{5}, -\sqrt{5})$

$\pm 1, \pm i$ $\quad \pm\sqrt{5}$

so generated by $(3\,4), (5\,6)$

(t^5-1), generated by $(2\,3), (2\,4), (2\,5)$ roots $= (1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4)$

t^4+1 generated by $(1\,2), (3\,4)$ roots $= (i, -i, \sqrt{i}, -\sqrt{i})$

t^3-5 is S_3 so generated by $(1\,2\,3)$ and $(1\,2)$ roots all of order

t^4-2 is generated by $(1\,3\,2\,4), (3\,4)$ roots $= (\alpha, -\alpha, i\alpha, -i\alpha)$

t^3-1 is generated by $(2\,3)$ roots $= (1, \omega, \omega^2)$

5. $f \in \mathbb{Q}[t]$ has no rep roots

$\mathrm{Gal}_{\mathbb{Q}}(f)$ on set of roots $\{\alpha_1, \alpha_2, \dots \alpha_n\}$ of f has r orbits

$f(x) = a_0 + a_1 x + \cdots a_k x^k$

$\alpha_i \xrightarrow{\sigma_j} \alpha_j$ exist if $\exists\, \sigma_j \in \mathrm{Gal}(K/F)$

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

$\sigma(\alpha)$ minimal

now r orbits: $O_1 \dots O_r$
↑ all roots mapped inside

$\sigma(O_i) = O_i$

$f = g_1 \cdots g_r$
↑ g_i all roots are O_i

$g_i(x) = \prod_{j=1}^{k_i} (x - \alpha_j) \quad \alpha_j \in O_i$
$\in \mathbb{Q}[x]$

K | $\mathbb{Q}$ $\quad \mathrm{Fix}(\mathrm{Gal}(K/\mathbb{Q})) = \mathbb{Q}$

$\sigma(g_i) = g_i \; \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$

$\Rightarrow g_i$ is fixed
$\Rightarrow g_i \in \mathbb{Q}[t]$

now, $g_i(x) = h_1(x) \cdots h_n(x)$
then $S_1 \cup S_2 = O_i$ or some other orbit

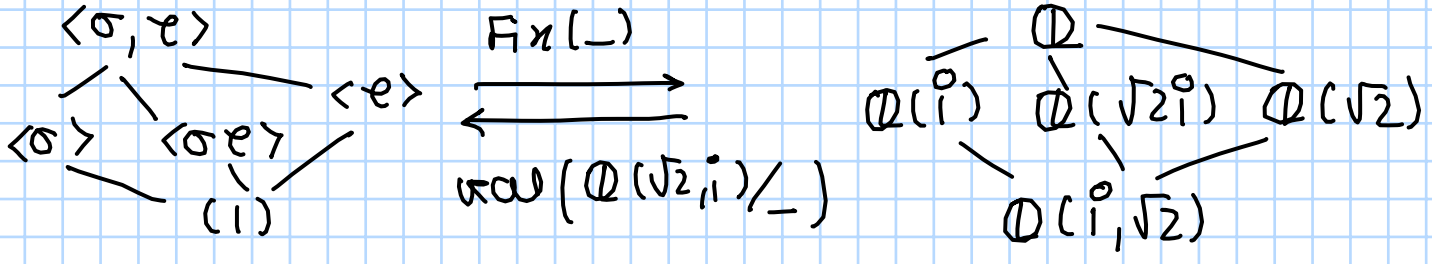
but as no other orbit, g_i is irreducible and in $\mathbb{Q}[t]$

6. $\mathbb{Q}(\sqrt{2}, i)$
|
$\mathbb{Q}$ galois as $\min_{\mathbb{Q}} \sqrt{2} = t^2 - 2$, $\min_{\mathbb{Q}} i = t^2 + 1$ $\Rightarrow$ Normal + finite

and $\mathrm{char} = 0 \Rightarrow$ separable

now, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$ $\quad \mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, i) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\sigma : \sqrt{2} \to -\sqrt{2}$, $i \to i$ $\qquad \tau : \sqrt{2} \to \sqrt{2}$, $i \to -i$



$\mathbb{Q}(\sqrt[3]{2},\omega)$ $\quad \alpha=\sqrt[3]{2}$

| $\mathbb{Q}$

$\mathbb{Q}$

① Normal as trivial $\min_{\mathbb{Q}} \alpha = t^3-2$ } Galois

② separable as char $=0$ }

$[\mathbb{Q}(\alpha,i):\mathbb{Q}]=6$

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

$\mathbb{Q}(\omega)$

|) 2

$\mathbb{Q}$

also $\mathrm{spl}_{\mathbb{Q}}(t^3-2) = \mathbb{Q}(\alpha,i)$

$\Rightarrow \mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\alpha,i) \cong S_3$

full lattice structure similar to $\mathbb{Q}(\sqrt[3]{5},\omega)$ question

$\mathbb{Q}$

$\mathbb{R}(t)$

|

$\mathbb{R}(t^2+\frac{1}{t^2})$

$\min_{\mathbb{R}(t^2+\frac{1}{t^2})} t = x^4 - x^2\left(t^2+\frac{1}{t^2}\right)+1 = f(x)$

$x^2=y \quad y^2 - y\left(t^2+\frac{1}{t^2}\right)+1 = 0$

$$\alpha,\beta = \frac{+\left(t^2+\frac{1}{t^2}\right) \pm \sqrt{\left(t^2-\frac{1}{t^2}\right)^2}}{2}$$

$$= \frac{+t^2+\frac{1}{t^2} \pm t^2 \mp \frac{1}{t^2}}{2}$$

$$= t^2, \frac{1}{t^2}$$

so, roots are $t, \frac{1}{t}, -t, -\frac{1}{t}$

i.e splits in $\mathbb{R}(t)$

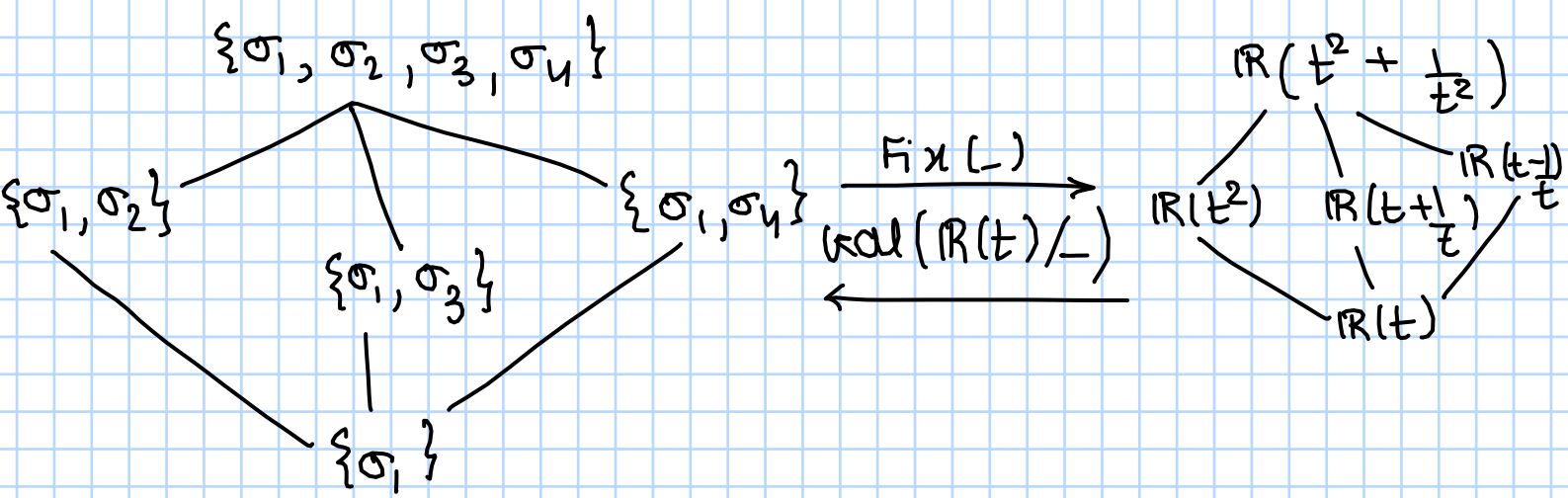
also char $=0$ so separable

now $[\mathbb{R}(t):\mathbb{R}(t^2+\frac{1}{t^2})] = 4$

$\mathrm{spl}_{\mathbb{R}(t^2+\frac{1}{t^2})} f(x) = \mathbb{R}(t) \quad z = t^2+\frac{1}{t^2}$

so, $\mathrm{Gal}_{\mathbb{R}(z)} \mathbb{R}(t) \subseteq S_4$

i.e $\mathrm{Gal}_{\mathbb{R}(z)} \mathbb{R}(t) = \{\sigma_1: t\to t, \sigma_2: t\to -t, \sigma_3: t\to \frac{1}{t}, \sigma_4: t\to -1/t\}$



$\mathbb{R}(X,Y)$ char $=0$ $\Rightarrow$ separable

$\mathbb{R}(X^2,Y^2)$

also $\min_{\mathbb{R}(X^2,Y^2)} X = t^2 - X^2$ splits in $\mathbb{R}(X,Y)$

$\min_{\mathbb{R}(X^2,Y^2)} Y = t^2 - Y^2$ splits in $\mathbb{R}(X,Y)$

} galois

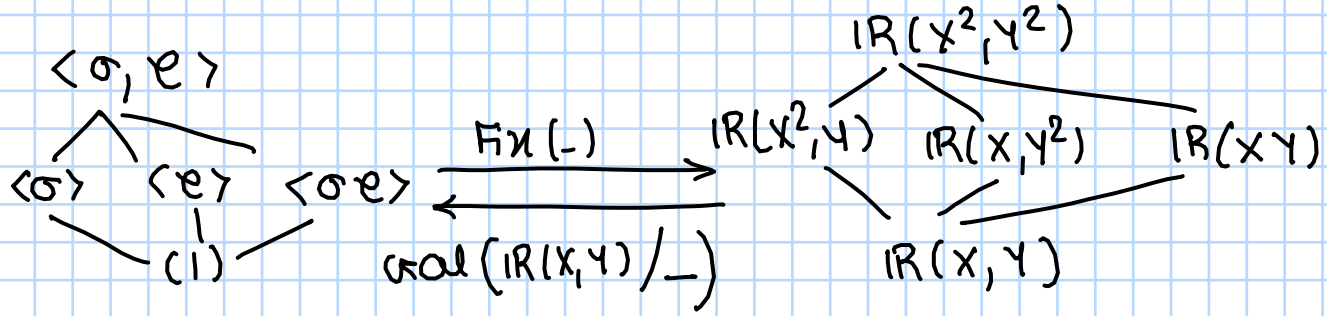
$\mathbb{R}(X,Y)$ — 2 — $\mathbb{R}(X^2,Y)$ — 2 — $\mathbb{R}(X^2,Y^2)$

$[\mathbb{R}(X,Y) : \mathbb{R}(X^2,Y^2)] = 4$

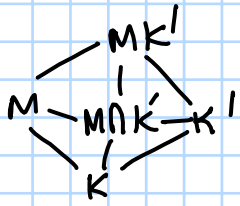
$|\mathrm{Gal}_{\mathbb{R}(X^2,Y^2)} \mathbb{R}(X,Y)| = 4$

$\sigma : \begin{matrix} X \to -X \\ Y \to Y \end{matrix}$ $\quad \tau : \begin{matrix} X \to X \\ Y \to -Y \end{matrix}$

$\mathrm{Gal}_{\mathbb{R}(X^2,Y^2)} \mathbb{R}(X,Y) = \langle \sigma, \tau \rangle$



7.



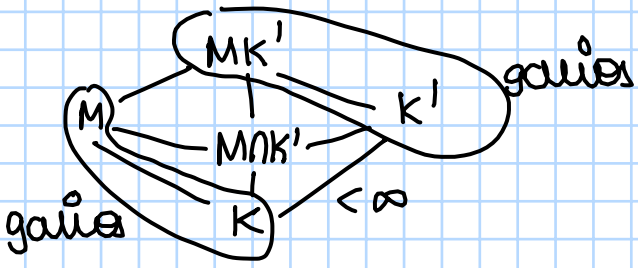
M/K galois $\Rightarrow M = \mathrm{spl}_K f$ f is separable

also $MK' = \mathrm{spl}_{K'} f$

since f is separable

$\Rightarrow MK'/K'$ is galois

now,



$\delta : Gal(MK'/K') \longrightarrow Gal(M/K)$

$\sigma \longmapsto \sigma|_M$

as $\sigma \in Gal(MK'/K')$

$\Rightarrow \sigma \in Gal(MK'/K)$

$\Rightarrow \sigma|_M \in Gal(M/K)$ as $\begin{matrix} M \\ | \\ K \end{matrix}$ is galois extension

so, $\sigma(M) \subseteq M$

now, δ is one-one as

$$\ker(\delta) = \{\sigma \in Gal(MK'/K') \mid \sigma|_M = id\}$$

now $\alpha \in MK'$

$\alpha = \sum a_i b_i \Rightarrow \sigma(\alpha) = \sigma(a_i b_i)$
$= a_i b_i$
$= \alpha$

i.e $\sigma = id$

so, $\ker(\delta) = \{id\}$

$H = img(\delta)$ then

$img(\delta) \cong Gal(MK'/K')$

now, $Fix(H) = \{\alpha \in M \mid \sigma(\alpha) = \alpha \ \forall \alpha \in H\}$

$img(\delta) \subseteq Gal(M/K)$ $= \{\alpha \in M \mid \sigma|_M(\alpha) = \alpha, \ \sigma|_M \in Gal(M/K)$ s.t $\exists \sigma \in Gal(MK'/K')\}$

↑ K' is fixed

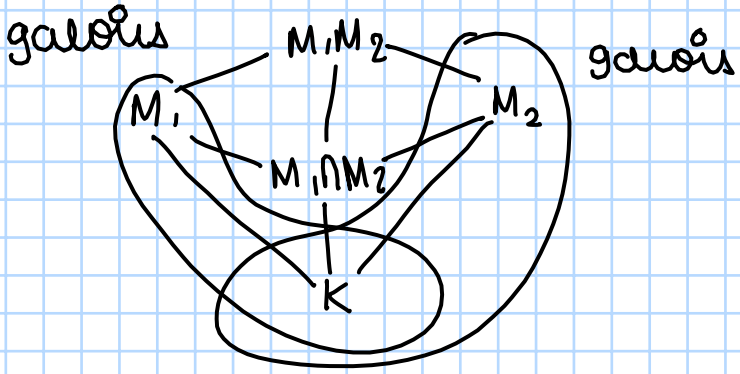
$= MnK'$

so, $Fix(H) = MnK'$, as $\begin{matrix} M \\ | \\ K \end{matrix}$ is galois $Gal\left(\frac{M}{Fix(H)}\right) = H = Im(\delta)$

$\Rightarrow Gal(M/MnK') = img(\delta)$

Φ, $\mathrm{Gal}(M/M\cap K') \cong \mathrm{Gal}(MK'/K')$

8.



seprable $\cap$ seprable $\Rightarrow$ $M_1\cap M_2$ seprable —①

$|$
K

also, $\forall \alpha \in M_1\cap M_2$, $\alpha \in M_1$, $\alpha \in M_2$

$\Rightarrow \min_K \alpha$ splits in M_1, M_2

$\Rightarrow \min_K \alpha$ splits in $M_1\cap M_2$ —②

by ①, ② $M_1\cap M_2$ is galois

$|$
K

also, $M_1 = \mathrm{spl}_K(f_1)$

$M_2 = \mathrm{spl}_K(f_2)$

then $M_1M_2 = \mathrm{spl}_K\left(\frac{f_1 f_2}{\gcd(f_1,f_2)}\right)$

seprable

$|$
K

$\Rightarrow M_1M_2$ is finite normal + seprable

$|$
K

$\Rightarrow M_1M_2$ is galois

$|$
K

$\phi: \mathrm{Gal}(M_1M_2/K) \longrightarrow \mathrm{Gal}(M_1/K)\times\mathrm{Gal}(M_2/K)$

$\sigma \longmapsto (\sigma|_{M_1}, \sigma|_{M_2})$

$$\ker(\phi) = \{\sigma \in \mathrm{Gal}(M_1M_2/k) \mid \sigma|_{M_1} = id,\ \sigma|_{M_2} = id\}$$
$$= \{id\}$$

so, ϕ is one-one

also, $\mathrm{img}(\phi) = \{(\sigma, e) \mid \sigma = e \text{ on } M_1 \cap M_2\}$

if $M_1 \cap M_2 = k$ then

$\mathrm{img}(\phi) = \{(\sigma, e) \mid \sigma = e \text{ on } k\}$

$= \mathrm{Gal}(M_1/k) \times \mathrm{Gal}(M_2/k)$

i.e $\mathrm{Gal}(M_1M_2/k) \cong \mathrm{Gal}(M_1/k) \times \mathrm{Gal}(M_2/k)$

9. $F_p(x, y)$

$F_p(x^p, y^p, x + yx^{p^n})$

$F_p(x^p, y^p)$

$(x + yx^{p^n})^p \in F_p(x^p, y^p)$

also, $x + yx^{p^n} \in F_p(x^p, y^p, x + yx^{p^n})$

so, $F_p(x^p, y^p) \subseteq F_p(x^p, y^p, x + yx^{p^n}) \subseteq F_p(x, y)$

also, if $M_n = M_m$ $m \neq n$ M_n $n < m$

then $x + yx^{p^n} - (x + yx^{p^m}) \in M_m$

$\Rightarrow y(x^{p^n} - x^{p^m}) \in M_n, M_m$

$\Rightarrow y \in M_n, M_m$

$\Rightarrow x \in M_n, M_m$ contradiction

so, infinite many subfields

Tutorial-9:

1. $G_n = 1 \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G = G_0$

G_i/G_{i+1} abelian

(a) $|G|$ trivial

(b) S_3, S_4

$1 \trianglelefteq A_3 \trianglelefteq S_3$ (A_3: cyclic)

$1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ (V_4: 4, A_4: 12)

$(e), (1,2), (3,4), (1,3), (2,4), (1,4), (2,3)$

$|A_4/V_4| = 3 \to$ cyclic

(c) $|D_n| = 2n$

$r^n = 1 = s^2$ $C_n \trianglelefteq D_n$

C_n: Abelian so done

$1 \trianglelefteq C_n \trianglelefteq D_n$

(d) Q_8 $(\pm 1, \pm i) \trianglelefteq Q_8$

$(\pm 1, \pm i)$: abelian

$1 \trianglelefteq \{(\pm 1, \pm i)\} \trianglelefteq Q_8$

(e) $|G| < 60 \Rightarrow G$ not basic abelian

$d < n \Rightarrow |G| = d$ solvable

$N \trianglelefteq G$ G/N, N both solvable $\Leftrightarrow G$ solvable

By induction

2. G A abelian $A \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n$

$d_1 | d_2 | \cdots | d_n$

by CRT: $A \cong \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_K^{r_K}$

$G_1 \trianglelefteq G$ $G/G_1 = \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_K^{r_K}$

largest normal subgroup → Quotient prime

$n = pm$ then there subgroup of order m

$H/G_1 \trianglelefteq G/G_1$ H: index p

$G_1 \trianglelefteq H \trianglelefteq G$

we can have index p

do same work till we end our claim

4. $\mathbb{Q}$
|
$\mathbb{Q}(\sqrt{3})$
|
$\mathbb{Q}(\sqrt{3}, \sqrt[5]{2})$
|
$\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}, \sqrt[5]{2})$
|
$\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}, \sqrt[3]{2+\sqrt[5]{2}})$

5. $x^4 - 4x^2 - 21 = (x-7)(x+7)(x+3i)(x-3i)$ all roots in $\mathbb{Q}(i)$

$\mathrm{Gal}_{\mathbb{Q}}(f) = \{id, \kappa\}$
$= \mathbb{Z}/2\mathbb{Z}$

abelian
$\Rightarrow$, solvable

$x^4 + ax^2 + b \quad x^2 = u$
$u^2 + au + b$

$\mathbb{Q}(\alpha)$
|
$\mathbb{Q}(u)$ } Radical
|
$\mathbb{Q}$ } Radical

$x^3 = u$ and $x^6 + ax^3 + b$ done

$t = 1 \pm \sqrt{3}$

$\mathbb{Q}(\sqrt{3}) \leftarrow \mathbb{Q}(\sqrt{3}, \omega)$ $\quad \omega^3 = 1$ $\quad x^{2n} + ax^n + b$ always solvable
|
$\mathbb{Q}$

7. $x^n + \cdots = 0$
$n-2$ roots real
2 roots complex

$\mathrm{Gal}(K/\mathbb{Q})$ (K / $\mathbb{Q}$)

$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ $\quad \sigma(\alpha_1) = \alpha_2$ everything else find

$\mathrm{Gal}(K/\mathbb{Q}) \subseteq S_n$

σ is like (i, κ) transposition

now, $S_n = \langle (1,2), n\text{-cycle} \rangle$

S_p not solvable $\quad$ prop $S_p \geq 4$ $\sigma \in 4$ transitive
$4 \curvearrowright$ roots and having 1 exit,

$|G| = |\text{orbit}| \cdot |\text{stab}|$

$|G| = p \times |\text{stab}|$

$p \mid |G| \Rightarrow \exists$ a p-cycle as cycles of order p in $G \leq S_p$ and p degree, criterion was deg p

so, $G = S_p$

S_p not solvable

$A_5 \leq S_n$

↑

Not solvable so, S_p not solvable

by lemma irreducible, use derivative argument for only $p-2$ real roots



9. $f(x) \in \mathbb{Q}[x]$ irred
one root radical

normal closure of radical extension is radical

$\mathbb{Q}(\alpha) \xrightarrow{\sigma} \mathbb{Q}(\beta)$
root to other root

$\mathbb{Q}$

$\sigma(F_2) = \sigma(F_1)\sigma(\gamma_1)$

radicals map to radicals as roots map to roots

1.(a) Abelian group G

then $(1) \trianglelefteq G$ is trivial

and $G/(1)$ is abelian as G is abelian

(b) S_3 has 6 elements

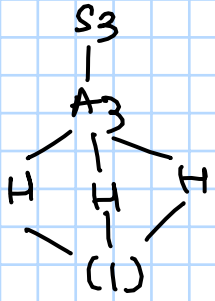
subgroups of S_3 are $\langle (123), (132) \rangle = A_3$

$\langle (12) \rangle = H_{(12)}$

$\langle (23) \rangle = H_{(23)}$

$\langle (13) \rangle = H_{(13)}$

$\langle id \rangle = (1)$



now $A_3 \trianglelefteq S_3$ we already know and

$|A_3| = 3 \Rightarrow A_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $|S_3/A_3| = 2$

$\Rightarrow$ abelian

i.e A_3 is cyclic, so $1 \trianglelefteq A_3 \trianglelefteq S_3$ $A_3/1$ and S_3/A_3 abelian

$|S_4| = 24$ as $A_4 \trianglelefteq S_4$

also $|S_4/A_4| = 2 \Rightarrow$ abelian

now $|A_4| = 12$ $\{e, a, b, c\}$ $a^2 = b^2 = c^2 = e$, $ab = c$ $bc = a$ $ca = b$

$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$

is s.t $|V_4| = 4$ and

$|A_4/V_4| = 3 \Rightarrow A_4/V_4$ is abelian

also $V_4 \trianglelefteq A_4$ as



$V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

now as conjugation in S_n does not change cycle structure, so conjugation in A_n also does not change cycle

$\Rightarrow V_4 \trianglelefteq A_4$

so, $(1) \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ abelian

abelian $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ abelian

(c) $D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$ group of symmetries of n-gon

$|D_n| = 2n$

$r^n = 1 = s^2$ $C_n = \langle r \mid r^n = 1 \rangle$

then $C_n \subseteq D_n$ and

$|C_n| = n$ $C_n \cong \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow (1) \trianglelefteq C_n \trianglelefteq D_n$

abelian $\mathbb{Z}/2\mathbb{Z}$ abelian

also $\frac{|D_n|}{|C_n|} = 2 \Rightarrow C_n \trianglelefteq D_n$

(d) $Q_8 = \langle i, j \mid i^2 = j^2 = -1, ij = -ji \rangle$

$H = \{\pm 1, \pm i\}$ then H is abelian

and $|Q_8| = 8$ $|H| = 4$

$\Rightarrow \frac{|Q_8|}{|H|} = 2 \Rightarrow H \trianglelefteq Q_8$

H abelian

$\{e\}, (1) \trianglelefteq H \trianglelefteq Q_8$

H abelian

(c) $|G| < 60 \Rightarrow G$ is not basic $\quad n < 60$

$d < n \Rightarrow |G| = d$ is solvable (induction step)
as trivial for $d = 1$

now $\exists N \neq (1), G$ s.t

$N \trianglelefteq G$ as G is not basic

$\Rightarrow |N| < |G| = n$

$\Rightarrow |N| < n \Rightarrow N$ is solvable

$\&$, now, N solvable and G/N solvable by induction
$(\because |G/N| < n)$

$\Rightarrow G$ solvable $(\because N, G/N$ solvable iff G solvable$)$

2. G is solvable, $\&$, $\exists \underset{(1)}{H_n} \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_0 = G$

H_i/H_{i+1} is abelian

now, H_i/H_{i+1} is abelian

$\Rightarrow H_i/H_{i+1} \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n$
$d_1 | d_2 | \cdots | d_n$

$(\because$ fundamental theorem of finite generated abelian groups$)$

$\Rightarrow H_i/H_{i+1} \cong \mathbb{Z}/p_1^{\sigma_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\sigma_2}\mathbb{Z} \times \cdots \mathbb{Z}/p_k^{\sigma_k}\mathbb{Z}$

$(\because$ CRT$)$

i.e the largest normal subgroup will be quotient to some prime

$(\because n = pm$, we have subgroup of order m $)$ $\quad |H/H_{i+1}| = m$

$\Rightarrow H/H_{i+1} \trianglelefteq H_i/H_{i+1}$

$\hookrightarrow |H/H_{i+1}| = m$ then $|H_i/H_{i+1}| = pm$

$\Rightarrow H_{i+1}^{\circ} \trianglelefteq H \trianglelefteq H_i^{\circ}$

$|H_i^{\circ}/H| = \frac{mp}{m} = p$

$\Rightarrow H_i^{\circ}/H \cong \mathbb{Z}/p\mathbb{Z}$ and $H \trianglelefteq H_i^{\circ}$

then putting $i=0$, $\exists H$ s.t $H \trianglelefteq G = G_n$

s.t $G/H \cong \mathbb{Z}/p\mathbb{Z}$

then by induction let $H = G_{n-1}$ (∵above for any finite H_i°)

$\exists G_{n-2} \trianglelefteq G_{n-1}$

$\vdots$

$(1) \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$

3. $|G| = p^n$

centre of $G = Z(G)$ is non-trivial as it is a p-group

$\Rightarrow (1) \trianglelefteq Z(G)$ $Z(G) \neq (1)$

also, $G/Z(G)$ is a p-group, and $Z(G)$ abelian

then by induction

$G/Z(G)$ and $Z(G)$ are solvable

$\Rightarrow G$ is solvable

4. $\mathbb{Q}$

$|$

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

$|$

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

$|$

$\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}, \sqrt[5]{2})$

$|$

$\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}, \sqrt[3]{2+\sqrt[5]{2}})$

5. $x^4 - 4x^2 - 21$ / $x^6 - 2x^3 - 2$ $\rightarrow$ solvable by radicals

as $x^2 = u \Rightarrow u^2 - 2u - 21 = 0$

$u = \frac{2 \pm \sqrt{4+84}}{2} = 1 \pm \sqrt{1+21}$

$= 1 \pm \sqrt{22}$

so final roots are $\pm\sqrt{1\pm\sqrt{22}}$ radicals

$\mathbb{Q}(\sqrt{1+\sqrt{22}}, \sqrt{1-\sqrt{22}})$

$\mathbb{Q}(\sqrt{22})$

$\mathbb{Q}$

$x^6-2x^3-2=0$

$x^3=u \quad u^2-2u-2=0$

$u^2-2u+1-3=0$

$\Rightarrow (u-1)^2=3$

$\Rightarrow u-1=\pm\sqrt{3}$

$\Rightarrow u=1\pm\sqrt{3}$

$\Rightarrow x^3=1\pm\sqrt{3}$

$\Rightarrow x=(1\pm\sqrt{3})^{\frac{1}{3}}, (1\pm\sqrt{3})^{\frac{1}{3}}\omega, (1\pm\sqrt{3})^{\frac{1}{3}}\omega^2$

all radicals

6. $x^5-25x-5=f(x)$

$f'(x)=5x^4-25=5(x^4-5)$

$=5(x^2-\sqrt{5})(x^2+\sqrt{5})$

↑ 2 real roots

$x=\pm(5)^{\frac{1}{4}}$

$f'(x)=0$

also, $f''(x)=20x^3$

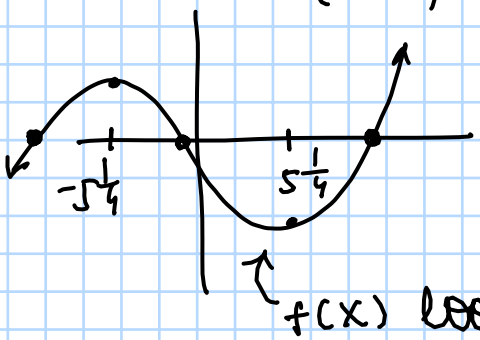
$f''(5^{\frac{1}{4}})>0, \quad f''(-5^{\frac{1}{4}})<0$

$f(5^{\frac{1}{4}})=5^{\frac{5}{4}}-5^2\cdot 5^{\frac{1}{4}}-5$

$=5^{\frac{1}{4}}-5^{\frac{9}{4}}-5$

$=5[5^{\frac{1}{4}}-5^{\frac{5}{4}}-1]<0$

$f(-5^{\frac{1}{4}})>0$



↑ $f(x)$ looks like this

3 real roots, 2 imaginary roots $\Rightarrow$ Gal $\underset{\mathbb{Q}}{f(x)} = S_5$

$A_5 \trianglelefteq S_5$ as A_5 is basic, so (1) ∇A_5 but A_5 NOT abelian

$\Rightarrow$ A_5 not solvable $\Rightarrow$ S_5 not solvable

$\Rightarrow f(x)$ is not solvable by radicals

$x^5 - 6x^2 + 3 = g(x)$

$g'(x) = 5x^4 - 12x$

$g'(x) = x(5x^3 - 12)$

$x = 0, \quad x^3 = \frac{12}{5}$

$\Rightarrow x = 0, \left(\frac{12}{5}\right)^{\frac{1}{3}}$ only real solution of $g'(x)$

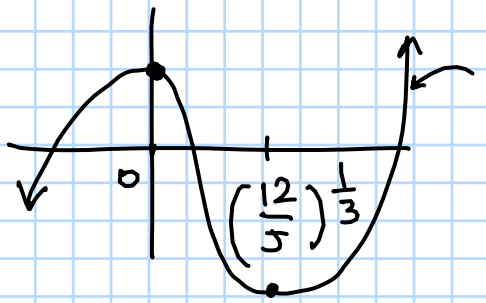
also $g''(x) = 20x^3 - 12$

$g''(0) = -12 < 0$

$g''\left(\left(\frac{12}{5}\right)^{\frac{1}{3}}\right) = 20 \times \frac{12}{5} - 12 > 0$

$g(0) = 3 > 0$

$g\left(\left(\frac{12}{5}\right)^{\frac{1}{3}}\right) = \left(\frac{12}{5}\right)^{\frac{2}{3}} \left[\frac{12}{5} - 6\right] + 3 < 0$



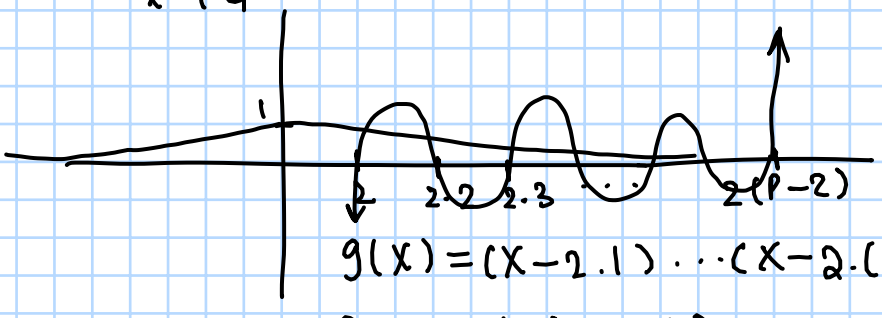
$g(x)$ has 3 roots real
2 roots imaginary

$\Rightarrow gal_{\mathbb{Q}} g(x) = S_5$

$\Rightarrow$ g not solvable by radical over $\mathbb{Q}$

7. $f(x) = (x^2+4)(x-2)(x-2(2))(x-2(3))\cdots(x-2(p-2)) - 2 = 0$

$\frac{2}{x^2+4} = (x-2)(x-2(2))\cdots(x-2(p-2))$



$g(x) = (x-2.1)\cdots(x-2.(p-2))$

$p \to$ odd $\Rightarrow$ $\underbrace{2(1), \ldots 2(p-2)}_{\text{odd}}$

$g(3) = (3-2)(2.2-3)(2.3-3)\cdots(2(p-1)-3) \geq 1$

similarly $g(5) \leq -1$, $g(7) \geq 1$

$\vdots$



$\therefore$ entany $(p-2)$ roots real

$\therefore$ 2 imaginary roots

it is trivial to see $2 \mid a_i \; \forall i$ but $4 \nmid -2$ (last an

$\therefore f(X)$ is irreducible by eisenstein criterion

$\therefore \alpha$ root of f then

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = p \Rightarrow p \mid [\text{spl}_{\mathbb{Q}} f : \mathbb{Q}] = |G|$

$G = \text{Gal}_{\mathbb{Q}} f(X)$

$\text{spl}_{\mathbb{Q}} f$ galois extension of $\mathbb{Q}$

$\therefore \exists$ p-cycle as $G \subseteq S_p$ and $p \mid |G|$

also $K : \mathbb{C} \to \mathbb{C}$, $z \to \bar{z}$ $\quad o(K) = 2 \quad K \in G$

as 2 imaginary roots

$\Rightarrow (i\ j) \in G \subseteq S_p$

then as $S_p = \langle (i\ j), p\text{-cycle} \rangle \Rightarrow G \geq \langle (i\ j), p\text{-cycle} \rangle$

$\Rightarrow S_p \geq G \geq S_p$

$\Rightarrow S_p = G$

Now for $p \geq 5$ f is not solvable by radicals

as $A_5 \subset S_p$ and A_5 Not solvable

also $p < 5 \Rightarrow p \leq 4$ solvable by radicals

8. $f(X) = 0$ f polynomial of degree ≤ 4 is solvable by radical our $\mathbb{Q}$

as $\text{gal}_{\mathbb{Q}} f \subset S_4$ were from 1 (b) S_4 is solvable

$\Rightarrow \text{gal}_{\mathbb{Q}} f$ is solvable

$\Rightarrow f$ is solvable by radicals on $\mathbb{Q}$

9. $f(x) \in \mathbb{Q}[x]$ is irreducible and one root is radical then all roots are radical

Let α be the radical root

$\mathbb{Q}(\alpha)$ — $\mathrm{spl}_{\mathbb{Q}}(\min \alpha)$ normal closure of radical extension is radical extension ($\because$ done in class)

$|$

$\mathbb{Q}$

Now, $\sigma : \alpha \to \beta \quad \exists \sigma \in \mathrm{Gal}_{\mathbb{Q}} f$

β: any root of f ($\because f$ is irreducible)

$\Rightarrow \mathbb{Q}(\beta) \subset \mathrm{spl}_{\mathbb{Q}}(\min \alpha)$

$\Rightarrow \mathbb{Q}(\beta)$ is radical extension

$\Rightarrow$ all roots radical

now let $f = (x+1)(x^5 - 25x - 5)$

↳ Not irreducible

and from (6) we saw $x^5 - 25x - 5$ does not have radical roots

but $f(1) = 0$, 1 is a radical root