MA 414
Algebra 1



Attendance - 80%.
grading - min 35
35-40 DD, every 10 marks 1 grade increase
Ref - 1. Ron Weinstein - Galois theory
2. J.S Milne - Field theory and galois theory
3. Ian Stewart - Galois theory (only introduction)
Quiz - 4 Quizes - 35-40%.
midsem, Endsem

6th Jan:

motivation of Galois theory comes from

$$ax^2+bx+c=0 \quad \text{(Radical)}$$

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \quad (8^{th}\ CE)$$

Ex: does ∃ similar solution for roots of a cubic, quartic...?

Ans:

Cubic: yes (Tartaglia, 1500
Cardano, 1540)

Quadratic: yes (Ferrai, 1540)
↖ student of Cardano's student

Quintic: NO (Ruffini - 1800, Abel - 1823)

(NO general formula exist which works for all degree 5 equations)

Galois: (1830) precise condition when a given degree ≥5 polynomial can be solved by radicals

Eg: $x=\sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}}+\sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}}$

$$x^3=\left(1+\frac{2}{3}\sqrt{\frac{7}{3}}\right)+\left(1-\frac{2}{3}\sqrt{\frac{7}{3}}\right)+3(x)\left(\sqrt[3]{1-\frac{4}{9}\cdot\frac{7}{3}}\right)$$

$$\Rightarrow x^3=2+3(x)\sqrt[3]{\frac{-1}{33}}$$

$$\Rightarrow x^3=2-x$$

so, x is a root of $x^3+x-2=0$

as $x=1$ is also a root

$$x^3-x^2+x^2-x+2x-2=0$$
$$\Rightarrow x^2(x-1)+x(x-1)+2(x-1)=0$$
$$\Rightarrow (x-1)(x^2+x+2)=0$$

(x^2+x+2: complex roots)

but $x\in\mathbb{R}\Rightarrow x=1$ as only 3 roots possible

so, $\sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}}+\sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}}=1$

Solve general cubic by radicals:

$$a_0x^3+a_1x^2+a_2x+a_3=0$$
$$a_0\neq 0$$

divide by a_0, $x^3+ax^2+bx+c=0$

$$\Rightarrow \left(x+\frac{a}{3}\right)^3+b'x+c'=0$$

$$y=x+\frac{a}{3}$$

$$\Rightarrow y^3+py+q=0$$

assume $y = T + U$

$\Rightarrow y^3 = T^3 + U^3 + 3(TU)(T+U)$

$\Rightarrow y^3 = T^3 + U^3 + 3TUy$

and $y^3 + py + q = 0$

$\Rightarrow (T^3 + U^3 + 3TUy) + py + q = 0$

$\Rightarrow (T^3 + U^3 + q) + y(3TU + p) = 0$

($T^3 + U^3 + q = 0$, $3TU + p = 0$)

$\Rightarrow T^3 + U^3 = -q$ ——— (1)

$TU = -p/3 \Rightarrow T^3U^3 = \left(-\frac{p}{3}\right)^3$ ——— (2)

$z^2 + qz + \left(-\frac{p}{3}\right)^3 = 0$ quadratic equation roots T^3, U^3

as sum $= -\frac{b}{a}$ $a = 1$

product $= \frac{c}{a}$

$\Rightarrow z = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = T^3, U^3$

so, $T = \omega^m \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$, $U = \omega^n \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}}$ $\quad 0 \le m, n \le 2$

so, $y = T + U$ where total 9 choices but as T, U should satisfy (2)

we need $m+n$ as multiple of 3

$\Rightarrow (m, n) = (0,0), (1,2), (2,1)$ so,

let $t = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$ $\quad u = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$

then $y = \sqrt[3]{t} + \sqrt[3]{u}$, $\omega\sqrt[3]{t} + \omega^2\sqrt[3]{u}$, $\omega^2\sqrt[3]{t} + \omega\sqrt[3]{u}$

$1, \omega, \omega^2$ are cube roots of unity

eg: $x^3 + x - 2 = 0$ $\quad p = 1, q = -2$ $\quad \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = \sqrt{1 + \frac{1}{27}} = \frac{2}{3}\sqrt{\frac{7}{3}}$ $\quad x = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}$

overview of Galois theory:

view of $\mathbb{C}$ over $\mathbb{R}$: i - symbol s.t $i^2 = -1$

$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$

↑ closed under + and multiplication

$(-i)^2 = -1$, $(i)^2 = -1$ so we cannot distinguish i from $-i$ over $\mathbb{R}$

Def: Two complex numbers z, z' are conjugate / indistinguishable over $\mathbb{R}$ if any $P(t) \in \mathbb{R}[t]$, $P(z) = 0$ iff $P(z') = 0$

Theorem: $z, z' \in \mathbb{C}$ are conjugate over $\mathbb{R}$ iff $z = z'$ or $\bar{z} = z'$ ($\bar{z}$ = complex conjugate of z)

proof: ($\Rightarrow$) if $z, z' \in \mathbb{C}$ are conjugate over $\mathbb{R}$

if $z = z'$ then

for any $P(t) \in \mathbb{R}[t]$ $P(z) = 0$ iff $P(z') = 0$

is trivial

now if $z \in \mathbb{C}$ (z is any complex number)
$z = x + iy$ ($y \neq 0$)

case I: $y = 0$:
if $y = 0$ then
$P(t) = t - x \in \mathbb{R}[t]$
then $P(z) = 0$
by our defn
$P(z') = 0$
$\Rightarrow z' - x = 0$
$\Rightarrow z' = x = z$

case II: $y \neq 0$:
$z = x + iy$ with $y \neq 0$
let $P(t) = (t-x)^2 + y^2 \in \mathbb{R}[t]$
so, $P(z) = (iy)^2 + y^2 = 0$
as z, z' are conjugate from definition
$P(z') = 0 \Rightarrow P(z') = (z'-x)^2 + y^2 = 0$
$z' - x = \pm iy$
$\Rightarrow z' = z$ or $z = \bar{z}$

($\Leftarrow$) Assume $z' = \bar{z}$, as if $z = z'$ then trivial
case I: $y = 0$: $z = x \in \mathbb{R}$, $z' = x$ trivially z, z' are conjugate

case II: $y \neq 0$: $z = x + iy$, $y \neq 0$
let $p(t) \in \mathbb{R}[t]$
$p(z) = 0$, to show $p(\bar{z}) = 0$
$w_1, w_2 \in \mathbb{C}$
$\overline{w_1 + w_2} = \bar{w}_1 + \bar{w}_2$
$\overline{w_1 \cdot w_2} = \bar{w}_1 \cdot \bar{w}_2$
by induction
$\overline{w_1 \cdots w_n} = \bar{w}_1 \cdots \bar{w}_n$ ——— ①
and $\overline{w_1 + \cdots w_n} = \bar{w}_1 + \bar{w}_2 + \cdots + \bar{w}_n$ ——— ②
as $w \in \mathbb{C}$, and $\bar{a} = a$ if $a \in \mathbb{R}$ ——— ③
$\Rightarrow P(w) = P(\bar{w})$ ($\because$ ①, ②, ③)

$\Rightarrow P(z) = 0$
$\Rightarrow \overline{P(z)} = \bar{0} = 0$
$\Rightarrow P(\bar{z}) = 0$

one more way to show this is
if $P(t) \in \mathbb{R}[t]$, $P(z) = 0 \Rightarrow P(\bar{z}) = 0$ then we are done
let $w(t) = (t-x)^2 + y^2 \in \mathbb{R}[t]$
$w(z) = 0$
$w(\bar{z}) = 0$ (trivial to see)

$P(t) = q(t) w(t) + r(t)$ in $\mathbb{R}[t]$
$\deg(r(t)) \leq 1$

$\Rightarrow P(z) = 0, w(z) = 0 \Rightarrow r(z) = 0$ but as $y \neq 0$, $r(t) \in \mathbb{R}[t]$ and $\deg \leq 1$, $r(t)$ has to be zero as z cannot be root of one degree
$\Rightarrow r(z) \equiv 0$

so, $P(t) = q(t) w(t)$, as $w(z) = w(\bar{z}) = 0$
$\Rightarrow P(\bar{z}) = 0$

Defn: $z, z' \in \mathbb{C}$ are conjugate over $\mathbb{Q}$ if $\forall P(t) \in \mathbb{Q}[t]$, $P(z) = 0$ iff $P(z') = 0$

Note: z, z' conjugate over $\mathbb{R} \Rightarrow z, z'$ are conjugate over $\mathbb{Q}$ as $\mathbb{Q}[t]$ is smaller than $\mathbb{R}[t]$

Note: converse does not hold true as if z, z' are s.t $z \neq \bar{z}$, $z' \neq \bar{z}$ and z, z' conjugate over $\mathbb{Q}$ we find such example

Eg: $\sqrt{2}, -\sqrt{2}$ are conjugate over $\mathbb{Q}$

let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

any $w \in \mathbb{Q}[\sqrt{2}]$ has a unique representation

$w = a + b\sqrt{2}$

as if not then $w = a_1 + \sqrt{2} b_1$

$w = a_2 + \sqrt{2} b_2$

$\Rightarrow a_2 - a_1 = \sqrt{2}(b_1 - b_2)$

contradiction

let $\tilde{w} = a - b\sqrt{2}$

now $\widetilde{w_1 + w_2} = \tilde{w}_1 + \tilde{w}_2$

$\widetilde{w_1 \cdot w_2} = \tilde{w}_1 \cdot \tilde{w}_2$

similar to before by induction $\widetilde{\alpha} = \alpha$ $\forall \alpha \in \mathbb{Q}$, $\widetilde{w_1 + \dots + w_n} = \tilde{w}_1 + \dots + \tilde{w}_n$, $\widetilde{w_1 \dots w_n} = \tilde{w}_1 \dots \tilde{w}_n$

let $w \in \mathbb{Q}[\sqrt{2}]$ $P(t) \in \mathbb{Q}[t]$

$\Rightarrow \widetilde{P(w)} = P(\tilde{w})$ ($\because$ similar to before)

so, $P(z) = 0 \Rightarrow P(\bar{z}) = 0$

$P(\sqrt{2}) = 0 \Rightarrow P(\tilde{\sqrt{2}})$

$\Rightarrow P(-\sqrt{2}) = 0$

so, $\sqrt{2}, -\sqrt{2}$ are conjugate over $\mathbb{Q}$

we have one more way to see this

If $w = a + \sqrt{2} b$, $b \neq 0$ ($b = 0$ case is trivial)

$P(t) \in \mathbb{Q}[t]$

and $P(w) = 0$, then let $A(t) = (t-a)^2 - 2b^2$

$A(w) = 0$

$A(\tilde{w}) = 0$

as $w = a + \sqrt{2} b$

so, $P(t) = q(t) A(t) + r(t)$

again $\deg r \leq 1$

$\Rightarrow r \equiv 0$ as $\sqrt{2}$ is not rational so w cannot be root of rational one degree polynomial

$\Rightarrow P(\tilde{w}) = 0$

so, $\sqrt{2}, -\sqrt{2}$ are conjugates

Defn: Two k tuples of complex numbers (ordered) $(z_1, z_2, \dots z_k)$ and $(z_1', z_2', \dots z_k')$ are conjugate / $\mathbb{Q}$ if $\forall P(t_1, \dots t_k) \in \mathbb{Q}[t_1, \dots t_k]$

$P(z_1, \dots z_k) = 0$ iff $P(z_1', \dots z_k') = 0$

Corr: If $(z_1 \dots z_k)$ & $(z_1', \dots z_k')$ are conjugate / $\mathbb{Q}$

$\Rightarrow z_i$ & z_i' are conjugate / $\mathbb{Q}$ $\forall i = 1, 2 \dots k$

proof: It will follow from defn

given $P(t_i) \in \mathbb{Q}[t_i]$

$\in \mathbb{Q}[t_1, \dots t_k]$

where

$P(t_i) = P(t_1 \dots t_k)$

$P(z_1, \dots z_k) = P(z_i) = 0$

$\Leftrightarrow P(z_1', \dots z_i', \dots z_k') = 0$

$\Leftrightarrow P(z_i') = 0$

Note: converse is not true

Eg: $\omega = e^{2\pi i/5}$, ω is root of $t^5 - 1 = 0$

$1, \omega, \dots \omega^4$ are roots of $t^5 - 1 = 0$

1 is not conjugate to any ω^i for $i = 1, 2 \dots 4$ as we can find any $P(t) \in \mathbb{Q}[t]$ s.t $P(1) = 0$ but $P(\omega^i) \neq 0$

Infact $\omega, \omega^2, \dots \omega^4$ are conjugate\$\mathbb{Q}$ to each other

i.e ω^i, ω^j are conjugate\$\mathbb{Q}$

we can show this by using prev corr and appropriate tuples

$(\omega, \omega^2, \omega^3, \omega^4)$ & $(\omega^4, \omega^3, \omega^2, \omega)$ are conjugate / $\mathbb{Q}$ as they are complex conjugate



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

so conjugate/$\mathbb{R}$ $\Rightarrow$ conjugate/$\mathbb{Q}$ (similar proof for tuple)

$(\omega, \omega^2, \omega^3, \omega^4)$, $(\omega^2, \omega, \omega^3, \omega^4)$ are not conjugate over $\mathbb{Q}$

$P(t_1, t_2, t_3, t_4) = P(t_1, t_2) = t_1^2 - t_2$

$P(\omega, \omega^2) = 0$ but $P(\omega^2, \omega) \neq 0$

Eg: $(\omega, \omega^2, \omega^3, \omega^4)$, $(\omega^2, \omega^4, \omega, \omega^3)$ are conjugate/$\mathbb{Q}$ as they are square of it

using field automorphism (will come later)

Exe: show that $\overline{\omega_1 + \dots \omega_n} = \bar{\omega}_1 + \dots + \bar{\omega}_n$

and $\overline{\omega_1 \dots \omega_n} = \bar{\omega}_1 \dots \bar{\omega}_n$

Ans: $\omega_1 = \alpha_1 + i\beta_1$

$\omega_2 = \alpha_2 + i\beta_2$

$n = 2$:

$\overline{\omega_1 + \omega_2} = \alpha_1 + \alpha_2 - i(\beta_1 + \beta_2) = \bar{\omega}_1 + \bar{\omega}_2$

$\overline{\omega_1 \cdot \omega_2} = (\alpha_1\alpha_2 - \beta_1\beta_2 + i(\alpha_1\beta_2 + \alpha_2\beta_1)) = \alpha_1\alpha_2 - \beta_1\beta_2 - i(\alpha_1\beta_2 + \beta_1\alpha_2)$

$= (\alpha_1 - i\beta_1)\cdot(\alpha_2 - i\beta_2)$

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

true for $n=2$

$n=k$:

If true for $n=k-1$ then, for $n=k$: (hypothesis)

$\overline{\omega_1+\cdots+\omega_k} = \overline{(\omega_1+\cdots\omega_{k-1})+\omega_k}$ from $n=2$ case

$= \overline{\omega}_1+\cdots\overline{\omega}_{k-1}+\overline{\omega}_k$ from $n=k-1$ case

similarly, $\overline{\omega_1\cdots\omega_k} = \overline{(\omega_1\cdots\omega_{k-1})\cdot\omega_k}$ from $n=2$ case

$= \overline{\omega_1}\cdots\overline{\omega_{k-1}}\cdot\overline{\omega_k}$ from $n=k-1$ case

so by induction, true for $n=k$, so true for all n

Exe: show that $\widetilde{\omega_1+\cdots+\omega_n} = \widetilde{\omega}_1+\cdots+\widetilde{\omega}_n$

$\widetilde{\omega_1\cdots\omega_n} = \widetilde{\omega}_1\cdot\widetilde{\omega}_2\cdots\widetilde{\omega}_n$

Ans: $n=2$:

$\omega_1 = \alpha_1+\sqrt{2}\beta_1$ $\quad \alpha_i, \beta_i \in \mathbb{Q}$

$\omega_2 = \alpha_2+\sqrt{2}\beta_2$

then $\widetilde{\omega_1+\omega_2} = \widetilde{(\alpha_1+\alpha_2+\sqrt{2}(\beta_1+\beta_2))} = \alpha_1+\alpha_2-\sqrt{2}(\beta_1+\beta_2)$

$= \widetilde{\omega}_1+\widetilde{\omega}_2$

$\widetilde{\omega_1\cdot\omega_2} = \widetilde{(\alpha_1\alpha_2+\sqrt{2}(\alpha_1\beta_2+\alpha_2\beta_1)+2\beta_1\beta_2)}$

$= \alpha_1\alpha_2+2\beta_1\beta_2-\sqrt{2}(\alpha_1\beta_2+\alpha_2\beta_1)$

$= (\alpha_1-\sqrt{2}\beta_1)\cdot(\alpha_2-\sqrt{2}\beta_2)$

$= \widetilde{\omega}_1\cdot\widetilde{\omega}_2$

so for $n=2$ true

$n=k$: let's assume true for $n=k-1$ then

$\widetilde{\omega_1+\cdots+\omega_k} = \widetilde{(\omega_1+\cdots\omega_{k-1})+\omega_k}$ from $n=2$ case

$= \widetilde{\omega}_1+\cdots\widetilde{\omega}_{k-1}+\widetilde{\omega}_k$ from $n=k-1$ case

similarly, $\widetilde{\omega_1\cdots\omega_k} = \widetilde{(\omega_1\cdots\omega_{k-1})\cdot\omega_k}$ from $n=2$ case

$= \widetilde{\omega}_1\cdots\widetilde{\omega}_{k-1}\cdot\widetilde{\omega}_k$ from $n=k-1$ case

so by induction, true for $n=k$, so true for all n

7th Jan:

Recall, z, z' conjugate/$\mathbb{R}$ meaning any $p(t) \in \mathbb{R}[t]$, $p(z)=0$ iff $p(z')=0$

Theorem: z, z' are conjugate/$\mathbb{R}$ iff $z' \in \{z, \bar{z}\}$, $\bar{z}$ = complex conjugate

we also saw, $z, z' \in \mathbb{C}$ conjugate/$\mathbb{Q}$ then any $p(t) \in \mathbb{Q}[t]$, $p(z)=0$ iff $p(z')=0$

Theorem: $\sqrt{2}, -\sqrt{2}$ conjugate/$\mathbb{Q}$

$z, \bar{z}$ conjugate/$\mathbb{Q}$

now, $(z_1, \dots z_k), (z_1', \dots z_k') \in \mathbb{C}^k$ are conjugate/$\mathbb{Q}$ if for any $p(t_1 \dots t_k)$ in $\mathbb{Q}[t_1 \dots t_k]$, $p(z_1 \dots z_k)=0$ iff $p(z_1', \dots z_k')=0$

we also saw, $\omega = e^{2\pi i/5} \in \mathbb{C}$ then $\omega, \omega^2, \dots \omega^4$ are pairwise conjugate/$\mathbb{Q}$

↑ we have to do similar GCD construction to show this

$\varphi: \mathbb{Q}[t] \longrightarrow \mathbb{C}$ ring homomorphism

$q(t) \longmapsto q(\omega)$

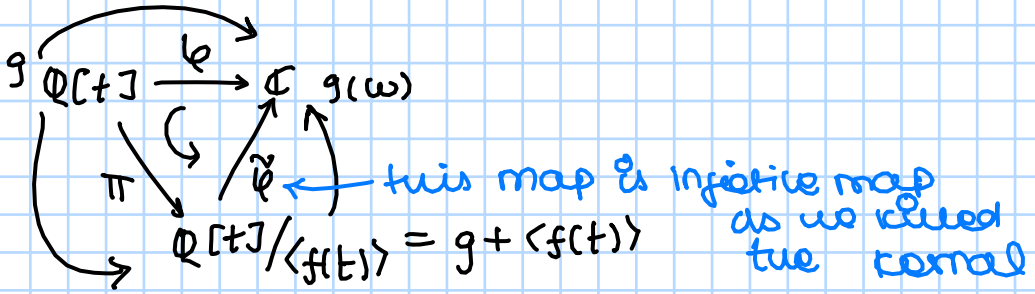
$\varphi/\mathbb{Q} = id : t \longmapsto \omega$

$\ker(\varphi) = \langle f(t) \rangle$ ← as PID so kernel generated by one element

$\varphi(q(t)) = q(\omega)$

$\omega^5 = 1$, $t^5 - 1 \xmapsto{\varphi} 0 \Rightarrow t^5 - 1 \in \ker \varphi$

$\Rightarrow t^5 - 1 = g(t) f(t)$



$\tilde{\varphi}$ is injective ring homomorphism

$\tilde{\varphi}\left(\frac{\mathbb{Q}[t]}{\langle f(t) \rangle}\right) \cong \frac{\mathbb{Q}[t]}{\langle f(t) \rangle}$ ← isomorphic to image

$\tilde{\varphi}: \frac{\mathbb{Q}[t]}{\langle f(t) \rangle} \longrightarrow \mathbb{C}$ ← codomain

as $\frac{\mathbb{Q}[t]}{\langle f(t) \rangle}$ now becomes integral domain as $\mathbb{C}$ is ID so $\tilde{\varphi}\left(\frac{\mathbb{Q}[t]}{\langle f(t) \rangle}\right)$ is ID

$\Rightarrow \frac{\mathbb{Q}(t)}{\langle f(t) \rangle}$ is a prime ideal

$\Rightarrow f(t)$ is irreducible polynomial

$(t-1)(\underbrace{t^4 + t^3 + \dots 1}_{\text{irreducible but } t-1 \text{ not in kernel as } \omega - 1 \neq 0}) = t^5 - 1$

so, $f(t) = t^4+t^3+t^2+t+1$

then we can use Divison algorithm using this idea

main ideas of galois:

① given $f \in \mathbb{Q}[t]$ symmetry group of f / Galio group of f $Gal(f/\mathbb{Q})$

let $\alpha_1 \dots \alpha_K$ be distinct roots of f in $\mathbb{C}$

Fundamental theorm of algebra:

$f(t) \in \mathbb{C}[t]$, then f has a unique factorisation as

$$f(t) = a\cdot(t-\alpha_1)^{\gamma_1}\cdots(t-\alpha_n)^{\gamma_n}$$
$$\alpha_1, \dots \alpha_n \in \mathbb{C}$$
$$\gamma_1, \dots, \gamma_n \geq 1$$

now, as $\alpha_1 \dots \alpha_K$ are roots of f in $\mathbb{C}$

$$Gal(f/\mathbb{Q}) = \{\sigma \in S_K \mid (\alpha_1 \dots \alpha_K) \& (\alpha_{\sigma(1)}, \dots \alpha_{\sigma(K)}) \text{ are conjugate}/\mathbb{Q}\}$$

$Gal(f/\mathbb{Q})$ is a subgroup of S_K

as $\sigma_1, \sigma_2 \in Gal(f/\mathbb{Q})$

$\Rightarrow \sigma_1 \circ \sigma_2, \sigma_1^{-1} \in Gal(f/\mathbb{Q})$

② f is soluable by radicals iff $Gal(f/\mathbb{Q})$ is a soluable group ← defn will come later

Eg: $f = (t-1)^5(t-2)^3$ $\alpha_1 = 1, \alpha_2 = 2$

(1, 2) and (2, 1) has to be conjugate / $\mathbb{Q}$

as $p(t) = t-1$
then 1 and 2 are not conjugate

$\Rightarrow$ (1,2) not conjugate over (2,1)

so, $Gal(f/\mathbb{Q}) = \{id\}$

Exe: $z \in \mathbb{Q}$, $z' \neq z$, $z' \in \mathbb{C}$, then z, z' are not conjugate / $\mathbb{Q}$ → done down

Eg: $f = (t-1)^5(t-2)^3(t^2-2)^6$

$\alpha_1 = 1, \alpha_2 = 2, \alpha_3 = \sqrt{2}, \alpha_4 = -\sqrt{2}$

$(1, 2, \sqrt{2}, -\sqrt{2})$ is conjugate/$\mathbb{Q}$ to $(1, 2, -\sqrt{2}, \sqrt{2})$

so, $Gal(f/\mathbb{Q}) = \{id, (3,4) \in S_4\}$

$1 \to 1$ $2 \to 2$ $3 \to 3$ $4 \to 4$ $\quad$ $1 \to 1$ $2 \to 2$ $3 \not\to 3$ $4 \not\to 4$

Note: we are starting with $f \in \mathbb{Q}[t]$ $f \longrightarrow Gal(f/\mathbb{Q})$

properties of this

tells us if f is solvable by radicals or not

There is one more problem of $\leftarrow$ first basic finite groups not necessary solvable

$f \dots \to G$: finite group inverse galois

$Gal(_/\mathbb{Q})$ $\leftarrow$ this can be done for finite basic group classification theorem

NOTE: PARI software takes $f \in \mathbb{Q}[t]$ deg ≤ 11 and tells if f is solvable by radicals or not

NOTE: If we change ordering of roots, $Gal(f/\mathbb{Q})$ will change but will be isomorphic

$1, \sqrt{2}, -\sqrt{2}, 2$ then:

$Gal(f/\mathbb{Q}) = \langle (2,3) \rangle \cong \langle (3,4) \rangle$

$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 3\ 4)$

$\uparrow$

this is function which makes $\langle (2,3) \rangle \cong \langle (3,4) \rangle$

Eg: deg $f = 2$

① one root $\alpha_1 \in \mathbb{Q}$ then $Gal(f/\mathbb{Q}) = \{id \in S_2\}$

② $\alpha_1 = x + iy$ $y \neq 0$, then $\alpha_2 = x - iy$ and so

$Gal(f/\mathbb{Q}) = S_2 = \{id, (1,2)\}$

③ $\alpha_1 \in \mathbb{R} \setminus \mathbb{Q}$ then also

$Gal(f/\mathbb{Q}) = S_2$

$\alpha_1 = 5 + 3\sqrt{2}$
then $\alpha_2 = 5 - 3\sqrt{2}$

Def: A radical is a number $z \in \mathbb{C}$ which can be obtained from $\mathbb{Q}$ by $\pm, \times, +, k^{th}$ root, $k \geq 2$

Eg: $\sqrt[3]{\sqrt{7}+2} + 11$

Sets:

It has a unique smallest element ϕ: empty set which is subset of every set

collection of all groups, it has a unique smallest element (e)

Exe: Gal(f/ℚ) is a subgroup of S_k

Ans:

let $\sigma_1, \sigma_2 \in gal(f/\mathbb{Q}) = \{\sigma \in S_k \mid (\alpha_1 \dots \alpha_k)$ and $(\alpha_{\sigma(1)}, \dots \alpha_{\sigma(k)})$ are conjugate $\}$

let $\tilde{P}(t_1, \dots t_k) = P(t_{\sigma_2(1)}, t_{\sigma_2(2)}, \dots t_{\sigma_2(k)})$

then $\tilde{P}(t_{\sigma_1(1)}, \dots t_{\sigma_1(k)}) = P(t_{\sigma_2 \circ \sigma_1(1)}, \dots t_{\sigma_2 \circ \sigma_1(k)})$

now, $\forall \tilde{P}(t_1 \dots t_k) \in \mathbb{Q}[t_1 \dots t_k]$

$\tilde{P}(t_1 \dots t_k) = 0 \Leftrightarrow P(t_{\sigma_2(1)}, \dots t_{\sigma_2(k)}) = 0 \Leftrightarrow P(t_1, t_2 \dots t_k) = 0$

$\Updownarrow$

$\tilde{P}(t_{\sigma_1(1)}, \dots t_{\sigma_1(k)}) = 0 \Leftrightarrow P(t_{\sigma_2 \circ \sigma_1(1)}, \dots t_{\sigma_2 \circ \sigma_1(k)}) = 0$

so, $\forall P(t_1 \dots t_k) \in \mathbb{Q}[t_1 \dots t_k]$

$\tilde{P}$ can be formed by σ_2^{-1} and so

$P(t_1 \dots t_k) = 0$ iff $P(t_{\sigma_2 \circ \sigma_1(1)}, \dots t_{\sigma_2 \circ \sigma_1(k)}) = 0$

so, $\sigma_2 \circ \sigma_1 \in gal(f/\mathbb{Q})$ ——— ①

now, let $\tilde{P}(t_1, \dots t_k) = P(t_{\sigma^{-1}(1)}, \dots t_{\sigma^{-1}(k)})$

then $\tilde{P}(t_1 \dots t_k) = 0 \Leftrightarrow P(t_{\sigma^{-1}(1)}, \dots t_{\sigma^{-1}(k)}) = 0$

$\Updownarrow$

$\tilde{P}(t_{\sigma_1(1)}, \dots t_{\sigma_1(k)}) = 0 \Leftrightarrow P(t_1, \dots t_k) = 0$

so, $\forall P(t_1 \dots t_k) \in \mathbb{Q}[t_1, \dots t_k]$

construct $\tilde{P}$ by σ we get

$P(t_1, \dots t_k) = 0$ iff $P(t_{\sigma^{-1}(1)}, \dots t_{\sigma^{-1}(k)}) = 0$

so, $\sigma^{-1} \in gal(f/\mathbb{Q})$ if $\sigma \in gal(f/\mathbb{Q})$ ——— ②

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

Exe: $z \in \mathbb{Q}$, $z' \neq z$, $z' \in \mathbb{C}$, then z, z' are not conjugate $/\mathbb{Q}$

Ans:

as $z' \neq z$, $z' \in \mathbb{C}$, $z \in \mathbb{Q}$

then let $z = x + iy$ with $y = 0$, $x \in \mathbb{Q}$

$\Rightarrow z = x$

now let $P(t) = t - x \in \mathbb{Q}(t)$

then $P(z) = x - x = 0$

but $P(z') = z' - x \neq 0$ as $z' \neq z$

$\Leftrightarrow$ z, z' not conjugate $\Leftrightarrow$
$\exists\, p(t) \in \mathbb{Q}[t]$ s.t. $p(z) = 0$ but $p(z') \neq 0$

9th Jan :

Defn : R: Ring (commutative with unity 1)

$(R,+,\cdot)$, $(R,+)$ is abelian group, $+,\cdot : R\times R \to R$

$\cdot$ is associative, $\cdot$ is distributive over $+$

Note: if $\cdot$ is commutative, it is commutative ring with unity

$1.a = a \quad \forall a \in R$

Defn: $\varphi : R \to S$ is ring homomorphism if $\varphi(a+b) = \varphi(a)+\varphi(b)$

$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$

$\varphi(1_R) = 1_S$

Eg: $R=(0)$ is a ring with unity

$\leftarrow 1_R = 0$ as $1_R \cdot a = a \quad \forall a \in R$

$1_R = 0 \quad a = 0$

$0 = 0$

Defn: (subring) R is a ring, S: subring of R if $S \subset R$, S is a ring with unity where $S\times S \xrightarrow{i} S$ are restrictions of $R\times R \to R$

Eg: (3) is a ring with identity $1_R = (3)$ but not a subring of $\mathbb{C}$

as $3\cdot 3 \to 3 \quad 3+3 \to 3$

$R=(0)$ is not a subring of $\mathbb{C}$

R : Ring, $\{S_i, i \in I\}$ subrings of R, then $\bigcap_{i\in I} S_i$, subring of R

Exe: union of subrings is not generally a subring → done down

$\{S_i, i \in I\}$ then $\bigcup_{i\in I} S_i$ not necessarily subring

Exe: Assume $\{S_i \mid i \in I\}$ satisfies → done down

$\forall S_i, S_j, \exists S_k$ s.t $S_i, S_j \subset S_k$ then $\bigcup_{i\in I} S_i$ is a subring

Defn: R Ring, $I \subset R$ ideal if $I + I \subset I$, $R\cdot I \subset I$, $0 \in I$

$I + I = \{a+b \mid a,b \in I\}$

Note: proper ideal when $I \neq R$

Eg: $R=(0)$, no proper ideal

$R \neq (0)$, has a proper ideal, (0)

for $R=\mathbb{Q}$ only proper ideal (0)

$\mathbb{Z}/p, \mathbb{R}$ only proper ideal (0), fields ← only proper ideal (0)

Exe : if R has only one proper ideal as (0) iff R is a field

ans:

($\Rightarrow$) If $a \neq 0 \in R$ then

$\langle a \rangle = R \Rightarrow ab = 1 \Rightarrow a$ is a unit $\forall a \in R, a \neq 0$

$\Rightarrow R$ is a field

($\langle a \rangle$: ideal generated by a (will be R as contains $a \neq 0$))

($\Leftarrow$) trivial as every ideal $\neq (0)$ contains $a \neq 0$ s.t $a.b = 1 \Rightarrow I = R$

Note: Any proper ideal of R is contained in a maximal proper ideal

Lemma: (Zorn) $(X, \leq)$ X: non empty set, $\leq$: partial order

$R \subset X \times X$ (= $\{(x,y) \mid x \leq y\}$), $\leq$ reflexive i.e $(x,x) \in R$

transitive i.e $(x,y) \in R, (y,z) \in R \Rightarrow (x,z) \in R$

antisymmetric i.e $x \leq y$, $y \leq x$ only when $x = y$

$\forall e$, if e is a chain in X (e: totally ordered subset of X, $\forall x, y \in e$ either $x \leq y$ or $y \leq x$)

then e has an upper bound in X

i.e $\exists \alpha \in X$ s.t $x \leq \alpha \ \forall x \in e$

then X will have a maximal element

Eg: $(\mathbb{N}, \leq)$ $e = \{1, 2\}$

$e = \mathbb{N} \rightarrow$ is a chain which has no upper bound

so, $(\mathbb{N}, \leq)$ has no maximal element

Eg: $X = \mathbb{N}_{\neq 0}$, $\prec$ i.e $n \prec m$ if $n \nmid m$ in natural order

totally ordered, X has an upper bound 0

so any chain will have an upper bound 0

hence any chain in X will have an upper bound 0

so, $(X, \prec)$ will have a maximal element namely 0

Note: $\mathbb{N}, \leq$

$R = \mathbb{N} \cup \{\infty\}$ $R = \{(n,m) \mid n \leq m\}$ then ∞ is maximal as it not related to anything but won't satisfy Zorn's lemma

$\mathbb{N}$ is a chain having no upper bound (so Zorn lemma is not iff)

Theorem: $R \neq (0)$, I: any proper ideal of R, then $\exists$ a maximal ideal m containing I (proper)

(m: maximal means $m \subset m' \Rightarrow m = m'$ or $m' = R$) ← ideal

proof: $\Sigma = \{$proper ideals containing $I\}$

we want maximal ideal now,

$J_1, J_2 \in \Sigma$, $J_1 \prec J_2$ if $J_1 \subset J_2$

as ①, ②, ③ are satisfied by this and so partially ordered

$\mathcal{C}$ is chain in Σ s.t $J_i \subseteq J$, $J_i \in \mathcal{C}$ $\quad \mathcal{C} = \{J_i \mid i \in I\}$

$\bigcup J_i = J$ is an ideal

if we show $\bigcup J_i = J$ is a proper ideal, we are done as if not then
$J = R$ and $1 \in J$ and so $\exists P$ s.t $1 \in J_P$
but each J_P is proper

So by Zorn's lemma, Σ has a maximal element

Defn: P is prime ideal of R if ① P is proper
② $a, b \in R$, $ab \in P \Rightarrow a \in P$ or $b \in P$

Exe: Every maximal ideal of R is prime ideal → done down

Exe: If R is PID then every non-zero prime ideal is maximal → done down

Note: $R \neq (0)$ ring without unit, then R may not have any prime ideal, so R has no maximal ideal

Eg: G: abelian gp wrt $*$, $|G| > 2$ then G has no unit
let $a * b = 0$ $\forall a, b \in G$ → this makes G a ring
subgroup of G is same as ideal (trivial as $a * b = 0$)
$0 \in$ subgroup

let P be prime ideal of G
$P = G \setminus (a)$ → maximal ideal ⇒ prime ideal
$b, a+b \in P \Rightarrow a = (a+b) - b \in P$ (contradiction)

So G does not have a proper prime ideal

Eg: ① for any ring R, ∃ a unique ring homomorphism $\varphi: \mathbb{Z} \to R$
$1 \to 1_R$
so $-1 \to -1_R$
$0 \to 0$

② $\varphi: R \to S$ ring homomorphism
$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$ ideal of R
If $1_S \neq 0$ then $\ker \varphi$ is a proper ideal of R
if $1_S = 0$ then $\varphi(r) = 1_S = 0 \Rightarrow \ker(\varphi) = R$

③ $\mathbb{Q} \to \mathbb{Z}$
$1 \to 1$
$\frac{1}{2} \to a$
$\frac{1}{2} + \frac{1}{2} = 1$ has no meaning in $\mathbb{Z}$

So $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}) = \phi$

Exe: $\varphi: \mathbb{Z} \to R$ $\quad 1 \to 1_R$ then $\ker \varphi = n\mathbb{Z}$ → done down
(i.e $n\mathbb{Z} = m\mathbb{Z} \Rightarrow n = m$ n is unique, $n \geq 0$)

Defn: n = characteristic of R

Exe: $\mathrm{char}(\mathbb{Z}) = 0$, $\mathrm{char}((0)) = 1$, $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$ $(n > 0)$

R : finite integral domain $1 \neq 0$, $ab = 0 \Rightarrow a = 0$ or $b = 0$

$\text{char}(R) = \text{prime}$ ← property if R is finite ID

$\varphi : \mathbb{Z} \to R$, $1 \to 1_R$ ← always as image finite but domain infinite

$\ker(\varphi) \neq (0) = n\mathbb{Z}$ as $\varphi : \mathbb{Z} \to R$, $1 \to 1_R$

$n \to n \cdot 1_R = 0$

then n is prime

as if $n \mid ab$ then $\varphi(ab) = 0 = \varphi(a)\varphi(b) \Rightarrow \varphi(a) = 0$ or $\varphi(b) = 0$

$\Rightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$

$\Rightarrow n \mid a$ or $n \mid$

as $|R| = p^m$, $p = \text{char}(R)$

$\varphi : \mathbb{Z} \to R$, $\ker \varphi = p\mathbb{Z}$

$\tilde{\varphi} : \mathbb{Z}/p\mathbb{Z} \to R$ injective

$\tilde{\varphi}(m + p\mathbb{Z}) = \varphi(m)$

Quotient map

$$\tilde{\varphi}\left(\mathbb{Z}/p\mathbb{Z}\right) \cong \mathbb{Z}/p\mathbb{Z}$$

$\cap$

subring of R

R is a ring which contains field $\cong \mathbb{Z}/p\mathbb{Z}$, so it's a vector space

$\Rightarrow$ R is a vector space over $\mathbb{Z}/p\mathbb{Z}$ but has finite many elements say m dimensions

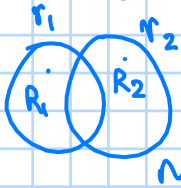
$\Rightarrow |R| = p^m$

Exe: Union of subrings is not generally a subring

$\{S_i, i \in I\}$ then $\bigcup_{i \in I} S_i$ not necessarily subring

Ans: $\{S_i, i \in I\}$ is the subring of R

let $R_1, R_2 \subset R$ subrings s.t $R_1 \cup R_2$ is a subring s.t R_1 or R_2 are not contained inside each other



let $r_1 \in R_1 \setminus R_2$

$r_2 \in R_2 \setminus R_1$

now if $r_1 + r_2 \in R_1$ then

as $r_1 \in R_1 \setminus R_2$

$\Rightarrow r_2 \in R_1$ (contradiction)

also if $r_1 + r_2 \in R_2$

then $r_1 \in R_2$ as $r_2 \in R_2 \setminus R_1$

$\Rightarrow r_1 \in R_2$ (contradiction)

so, $r_1 + r_2 \notin R_1$ or $R_2 \Rightarrow r_1 + r_2 \notin R_1 \cup R_2$

so, $R_1 \cup R_2$ not closed under addition

so we need R_1, R_2 s.t they are not inside one-another

$3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$

$5\mathbb{Z} = \{0, \pm 5, \pm 10, \dots\}$ both are subrings of $\mathbb{Z}$

then $5\mathbb{Z} \cup 3\mathbb{Z} = \{0, \pm 3, \pm 5, \pm 6, \pm 9, \pm 10, \dots\}$

now $5 \in 5\mathbb{Z} \cup 3\mathbb{Z}$
$6 \in 5\mathbb{Z} \cup 3\mathbb{Z}$
but $5 + 6 = 11 \notin 5\mathbb{Z} \cup 3\mathbb{Z}$

Exe: Assume $\{S_i \mid i \in I\}$ satisfies

$\forall S_i, S_j, \exists S_k$ s.t $S_i, S_j \subset S_k$ then $\bigcup_{i \in I} S_i$ is a subring

Ans: $\{S_i \mid i \in I\}$ $\forall S_i, S_j, \exists S_k$ s.t $S_i, S_j \subset S_k$

then for $x, y \in \bigcup_{i \in I} S_i$, $\exists\, i, j$ s.t $x \in S_i$, $y \in S_j$

$\Rightarrow \exists k$ s.t $S_i, S_j \subset S_k$

$\Rightarrow x + y \in S_k$

$\Rightarrow x + y \in \bigcup_{i \in I} S_i$

now, as $0 \in S_i$ $\forall\, i \in I \Rightarrow 0 \in \bigcup_{i \in I} S_i$

if $r \in \bigcup_{i \in I} S_i$, then $\exists\, i$ s.t $r \in S_i$
$\Rightarrow -r \in S_i$
$\Rightarrow -r \in \bigcup_{i \in I} S_i$

also, $1 \in S_i$ $\forall\, i \in I \Rightarrow 1 \in \bigcup_{i \in I} S_i$

$r, s \in \bigcup_{i \in I} S_i \Rightarrow \exists\, i, j$ s.t $r \in S_i$, $s \in S_j$

$\Rightarrow \exists k$ s.t $S_i, S_j \subset S_k$

$\Rightarrow r, s \in S_k$

$\Rightarrow r.s \in S_k$

$\Rightarrow r.s \in \bigcup_{i \in I} S_i$

and so $\bigcup_{i \in I} S_i$ is a subring

Exe: Every maximal ideal of R is prime ideal

Ans:

let M be the maximal ideal, then
R/M is a field
as $i + M \in R/M$
if $i + M \neq 0 + M$ then $i + M$ is a unit
so, we are done

$B = M + Ri$ then trivial to see
$M \subset M + Ri$ as $0 \in R$
also $M + Ri$ is an ideal (trivial)
as $i + M \neq 0 + M$ $i \notin M$ but $i \in B$ so, $M \subsetneq B = R$ as M is maximal ideal

$\Rightarrow 1 \in B$

$\Rightarrow \exists\, a, b$ s.t $a + bp = 1$

then $1 + M = (a + rp) + M = rp + M$

$= (r + M)(p + M)$

so, $p + M$ is a unit $\forall p \neq 0$

$\Rightarrow R/M$ is a field

now as M is a in ideal of R

R/M is field

let $a.b \in M$ if $a + M, b + M$ are two elements of R/M

s.t $(a + M)(b + M) = 0 + M = M$ ($\because a.b \in M$)

then $a + M = M$ or $b + M = M$ ($\because$ property of field)

so $a \in M$ or $b \in M$

so M is prime ideal

Exe: If R is PID then every non-zero prime ideal is maximal

Ans:

R is a PID then let P be a prime ideal s.t $P \neq (0)$

then $\exists\, p \in R$ s.t

$P = \langle p \rangle \quad p \neq 0$

now if $\exists$ ideal s.t

$\langle p \rangle \subsetneq m = \langle m \rangle \subseteq R$

then $m \mid p$ but p is prime

$\Rightarrow m = p$ or $p = 1$

in both cases $\langle m \rangle = \langle p \rangle$

so, $\langle p \rangle$ is maximal

Exe: $\varphi : \mathbb{Z} \to R$ then $\ker \varphi = n\mathbb{Z}$

$1 \to 1_R$

(i.e $n\mathbb{Z} = m\mathbb{Z} \Rightarrow n = m$ n is unique $n > 0$)

ans:

as $\varphi(1) = 1_R$

let n be smallest integer > 0 s.t

$\varphi(n) = 0$

then $n\mathbb{Z} \subseteq \ker(\varphi)$ ($\because$ trivial)

as $\forall\, p.n \quad \varphi(pn) = \varphi(p)\,\varphi(n)$

$= 0$

now, for $r \in \ker(\varphi)$

s.t $r \notin n\mathbb{Z}$

then $\tilde{r} = r + pn$ s.t $\tilde{r} > 0$ and is smallest of such kind

then $\varphi(\tilde{r}) = \varphi(r) + \varphi(-pn)$

$= 0$

but $\tilde{r} < n$ as $r \notin n\mathbb{Z}$

this is a contradiction

so, $\forall\, r \in \ker(\varphi)$, $r \in n\mathbb{Z}$

so, $\ker(\varphi) \subseteq n\mathbb{Z}$

so, $\ker(\varphi) = n\mathbb{Z}$

now, n is unique as if $n\mathbb{Z} = m\mathbb{Z}$
then

$n\mathbb{Z} = \{\ldots -n, 0, n, 2n \ldots\}$

$m\mathbb{Z} = \{\ldots -m, 0, m, 2m, \ldots\}$

if $n \neq m \neq 0$
and wlog $n < m$
then $\forall i \in \mathbb{Z}$ $i m \neq n$

so, this is a contradiction

$\Rightarrow n = m$

13th Jan:

$\varphi: R \to S$ ring homomorphism
$\ker\varphi$: ideal of R
$\mathrm{Im}\varphi$: subring of S

Exe: find examples s.t $\ker\varphi$ is not a subring of R and $\mathrm{Im}\varphi$ not an ideal of S → done down

R : ring, I is ideal of R ← Quotient ring

R/I = Equivalence class under relation
$a, b \in R$ $\quad a \sim b$ iff $a - b \in I$

Equivalence class containing $a \in R$ is written as

$$\bar{a} = a + I = \{a + x \mid x \in I\}$$

Defn: $\bar{a} + \bar{b} := \overline{a+b}$ $\quad a, b \in R$
$\bar{a} \cdot \bar{b} := \overline{ab}$

Exe: check well defined nes of above defn

i.e $\bar{a} = \bar{a_1}$, $\bar{b} = \bar{b_1}$ $\Rightarrow \overline{a+b} = \overline{a_1+b_1}$ → done down

and $\overline{ab} = \overline{a_1 b_1}$

R/I: Ring, $\bar{0}$ = zero element
$\bar{1}$ = multiplicative identity

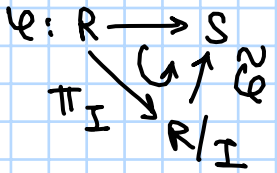
$\exists$ natural ring homomorphism

$$\pi_I : R \to R/I, \quad a \mapsto \bar{a}$$

$$\ker(\pi_I) = I$$

Universal property of π_I:

given any homo $\varphi: R \to S$ s.t $I \subseteq \ker\varphi$



$\tilde{\varphi}: R/I \to S$ s.t $\tilde{\varphi} \circ \pi_I = \varphi$

then $\exists$ unique ring homomorphism s.t diagram commutes

Defn: R is ring, X is subset of R. The smallest ideal of R containing X

$$= \bigcap_{\substack{I \text{ is ideal} \\ \text{containg } X}} I = \left\{ \sum_{\text{finite}} a_i x_i \mid a_i \in R, x_i \in X \right\}$$

The ideal of R generated by $X \subseteq R$ is the smallest ideal of R containg X

In particular $X = \{x_1 \dots x_n\}$ the ideal generated by X is

$$\left\{ \sum_{i=1}^{n} a_i x_i^{p} \;\middle|\; a_i \in R \right\}$$

Eg: smallest ideal of $R = (0)$

Def: R is ring, $X \subset R$ subset. The subring generated by X is the smallest subring of R containing X

$$= \bigcap_{S \supset X \text{ is a subring of } R} S = \left\{ \sum_{\substack{\text{finite} \\ x_i \in X \\ n \in \mathbb{Z}}} (n \cdot 1_R)\, x_1 \dots x_r + (m \cdot I_R) \right\}, \quad m \in \mathbb{Z}$$

now, if $X = \{x_1, \dots x_n\}$ the smallest subring of R containing X is

$$\left\{ \sum_{\substack{e = (e_1 \dots e_n) \in \mathbb{N}^n \\ n_e \in \mathbb{Z}}} n_e \cdot (x_1^{e_1} \dots x_n^{e_n}) \right\}$$

Eg: Ring: The smallest subring of $R = \mathbb{Z} \cdot 1_R$

$\chi : \mathbb{Z} \to R$, $1 \mapsto 1_R$ ring homomorphism

$\operatorname{img}(\chi) = \mathbb{Z} \cdot 1_R$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\chi} & R \\ & \searrow^{\chi_0} & \cup \\ & & \mathbb{Z} \cdot 1_R \end{array}$$

χ_0 is surjective ring homomorphism

$\ker(\chi_0) = n\mathbb{Z}$ (if χ is injective then $n = 0$; if not then take smallest $n > 0$ s.t. $\chi(n) = 0$)

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \cdot 1_R \\ \pi \downarrow & \nearrow \tilde{\chi}_0 & \\ \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

$\chi_0 : \mathbb{Z} \to \mathbb{Z} \cdot 1_R$ (surjective)

$\pi_{\ker(\chi_0)} : \mathbb{Z} \to \mathbb{Z}/\ker(\chi_0)$

$\tilde{\chi}_0 : \mathbb{Z}/\ker(\chi_0) \to \mathbb{Z} \cdot 1_R$ (isomorphism)

this becomes an isomorphism as χ_0 is surjective

so if $n = \operatorname{char}(R)$ then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z} \cdot 1_R$ is smallest subring of R (upto isomorphism)

smallest integral domain:

relation is containment (subring containing)

$\{ \mathbb{Z}/p\mathbb{Z}$ (p is prime), $\mathbb{Z} \}$

$\mathbb{Z}/p\mathbb{Z}$: finite fields (as finite ID $\Rightarrow$ field)

$\mathbb{Z}$: not a field but no subring smaller

now as $\mathbb{C}$ is a field, it has unique proper ideal (0)

Smallest subring of $\mathbb{C}$ containg X:

if $X = \phi$ then smallest subring is $\mathbb{Z}$

$X = \{\frac{1}{2}\}$ then smallest subring $= \left\{ \frac{m}{2^n} \;\middle|\; \begin{matrix} m \in \mathbb{Z} \\ n \geq 0 \end{matrix} \right\}$

$= \mathbb{Z}_2$ ← localisation of 2

$= \left\{ n\left(\frac{1}{2}\right)^m ; n \in \mathbb{Z}, m \geq 0 \right\}$

if $X = \left\{\frac{1}{2}, \frac{1}{3}\right\}$ by defn $= \left\{ n\left(\frac{1}{2}\right)^m + n'\left(\frac{1}{3}\right)^{m'} + n''\left(\frac{1}{6}\right)^{m''} \right\}$

$= \left\{ \frac{m}{6^n} \;\middle|\; m \in \mathbb{Z}, n \geq 0 \right\}$

if $X = \left\{ \frac{1}{p} \;\middle|\; p \text{ is prime} \right\}$ smallest is $\mathbb{Q}$ as $\mathbb{Q}$ has property

if $X = \{\sqrt{2}\}$ then smallest subring is (as $\mathbb{Q} = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{Z} \right\}$ $= \left\{ \frac{p_1^{a_1} \ldots p_m^{a_m}}{p_1'^{a_1'} \ldots p_n'^{a_n'}} \;\middle|\; p_i, p_i', a_i, a_i' \text{ are prime} \right\}$)

$\mathbb{Z}[X] = \mathbb{Z}[\{\sqrt{2}\}]$

↑ smallest subring

$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ as possible product of root $\sqrt{2}$ are $\sqrt{2}$

$= \mathbb{Z}[\sqrt{2}]$

$X = \{\sqrt[3]{2}\}$

$\mathbb{Z}[X] = \left\{ a + b(2)^{\frac{1}{3}} + c(2)^{\frac{2}{3}} \;\middle|\; a, b, c \in \mathbb{Z} \right\}$

Exe: $X = \{\pi\}$

Ans: $\mathbb{Z}[\pi] = \left\{ \sum_{\text{finite}} a_0 \pi^i : a_i \in \mathbb{Z} \right\}$

Smallest subring of $\mathbb{C}$ having property that for any element in the ring its n^{th} root is also in the ring $\forall n \geq 1$

lets start with $R_0 = \mathbb{Z}[\phi] = \mathbb{Z}$

$X_0 = \{m^{1/n} \mid m \in \mathbb{Z}, n \geq 1\}$

$R_1 = \mathbb{Z}[X_0] \ni \sqrt{2} + \sqrt[3]{5}$

but $((2)^{1/2} + (5)^{1/3})^{\frac{1}{4}}$ not in $\mathbb{Z}[X_0]$

$X_1 = \{a^{1/n} \mid a \in R_1, n \geq 1\}$

$R_2 = \mathbb{Z}[X_1]$ this will also not have closure property

$\vdots$

$R_0 \subset R_1 \subset R_2 \ldots$

so, $S = \bigcup_{i \geq 0} R_i$ is a subring of $\mathbb{C}$

let $\alpha \in S$

then $\exists R_i$ s.t $\alpha \in R_i \Rightarrow \alpha^{1/n} \in R_{i+1} \subset S$
$\Rightarrow \alpha^{1/n} \in S$

Defn: F is a field, $K \subseteq F$ is a subfield, if K is a subring of F
units of $K = U(K) = K \setminus 0$ i.e K is a field

Smallest subfield:

$\chi : \mathbb{Z} \longrightarrow F$ characteristic map

F: field, domain $\Rightarrow \ker(\chi) =$ prime ideal of $\mathbb{Z}$

as $\varphi : R \longrightarrow S$ $\quad I = \ker(\varphi)$

$\pi : R \to R/I$, $\tilde{\varphi} : R/I \to S$

φ is injective ring homomorphism

$\tilde{\varphi} : R/I \longrightarrow \text{im}(\tilde{\varphi})$ subring of S

so, $\mathbb{Z}/n\mathbb{Z} \cong$ subring of F (field $\Rightarrow$ ID)

$\Rightarrow \mathbb{Z}/n\mathbb{Z}$ is ID

$\Rightarrow n$ is prime or $n\mathbb{Z}$ is prime ideal

so, S: domain $\Rightarrow$ all its subrings are domains and so,
R/I is ID
$\Rightarrow I$ is Prime ideal

$\chi : \mathbb{Z} \longrightarrow F$ (F field)

$\ker \chi = \{ (0) ;\ p\mathbb{Z} \ ; p \text{ is prime} \}$

if $\ker \chi = p\mathbb{Z}$ then $\mathbb{Z}/p\mathbb{Z}$ is subring of F (Hill isomorphism)

Eg: $\varphi : K_1 \longrightarrow K_2$ field homomorphism

$\ker \varphi = \text{ideal} = (0)$ as $\varphi(1_{K_1}) = 1_{K_2}$ ($\because$ only ideal is (0) for fields)
$\Rightarrow \varphi$ is injective

$K_1 \cong \varphi(K_1)$ subfield of K_2

$\tilde{\chi} : \mathbb{Z}/p\mathbb{Z} \longrightarrow F$ is injective and so $\mathbb{Z}/p\mathbb{Z}$ is smallest subfield in F

↑ as smallest in case of ID too Fields $\subseteq$ ID

if $\text{char}(F) = 0$ then

$\chi : \mathbb{Z} \longrightarrow F$ injective so, $\mathbb{Z} \cdot 1 \subset F$

$\mathbb{Z}\left[\frac{1}{n} \mid n \geq 1\right]$ smallest ring s.t $\mathbb{Z}.1$ becomes field

$= \mathbb{Q}$ (by construction of $\text{char}(F)$)

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

defn: (prime subfields) $\{ \mathbb{Z}/p\mathbb{Z} \mid p \text{ is prime} \} \cup \{ \mathbb{Q} \}$

then are identified as $\mathbb{Z}.1_F$, $\mathbb{Q}.1_F$ and therefore 2 of them cannot be there (as char is unique and smallest by defn)

as $\begin{matrix} p.1 = 0 \\ q.1 = 0 \end{matrix} \Rightarrow 1 = 0$ if $p \neq q$

Eg: If $F = \mathbb{C}$ smallest containing $\{\sqrt{2}\}$ then $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

If this is a field it will be smallest one

$a + b\sqrt{2} \neq 0$

then $\frac{1}{a+b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} \in \mathbb{Q}[\sqrt{2}]$ so

$\mathbb{Q}[\sqrt{2}]$ is a field

Exe: Show that $\mathbb{Q}[\sqrt[3]{2}]$ is a field → done down

Exe: find examples s.t. ker φ is not a subring of R and Im φ not an ideal of S

Ans: $R = \mathbb{Z}$ $S = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\varphi : R \to S$ be a homomorphism

then

$\varphi(1) = (\bar{1}, \bar{1})$

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

So, $\varphi(2) = \varphi(1) + \varphi(1) = (\bar{1}, \bar{1}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0})$

similarly $\varphi(3) = (\bar{1}, \bar{1}) = \varphi(1)$

Extending this

$\varphi(2n+1) = (\bar{1}, \bar{1}) \ \forall \ n \in \mathbb{Z}$

$\varphi(2n) = (\bar{0}, \bar{0}) \ \forall \ n \in \mathbb{Z}$

$\Rightarrow \ker(\varphi) = 2\mathbb{Z}$ not a ring as $1 \notin 2\mathbb{Z}$

And $\text{img}(\varphi) = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$ not an ideal as

$(\bar{0}, \bar{1}) . (\bar{1}, \bar{1}) = (\bar{0}, \bar{1}) \notin \text{img}(\varphi)$

Exe: check well defined nes of above defn

i.e $\begin{matrix} \bar{a} = \bar{a_1} \\ \bar{b} = \bar{b_1} \end{matrix} \Rightarrow \overline{a+b} = \overline{a_1 + b_1}$

and $\overline{ab} = \overline{a_1 b_1}$

Ans: let $\bar{a} = \bar{a_1}$, $\bar{b} = \bar{b_1}$ i.e

$a - a_1 \in I$, $b - b_1 \in I$ for some ideal $I \subset R$

now, $\bar{a}+\bar{b}=\overline{a+b}$ ($\because$ defn)

then $\overline{a+b} = \{x+y \mid x-a\in I,\ y-b\in I\}$

$= \{x+y \mid x-a-a_1+a\in I,\ y-b-b_1+b\in I\}$

($\because a-a_1\in I, b-b_1\in I$ adding both sides)

$= \{x+y \mid x-a_1\in I,\ y-b_1\in I\}$

$= \bar{a}_1+\bar{b}_1$

$= \overline{a_1+b_1}$

similarly $\overline{a.b} = \bar{a}.\bar{b} = \{x.y \mid x-a\in I,\ y-b\in I\}$

$= \{x.y \mid x-a+a-a_1\in I,\ y-b+b-b_1 \in I\}$

($\because a-a_1\in I, b-b_1\in I$ adding both sides)

$= \{x.y \mid x-a_1\in I,\ y-b\in I\}$

$= \bar{a}_1.\bar{b}_1$

$= \overline{a_1b_1}$

Exe: R is finite ID then R is a field

Ans: $a\in R$ s.t $a\neq 0$

as R is finite $\{a^1, a^2, \ldots\}$ 2 of them must be equal

say i, j

$\Rightarrow a^i = a^j$ wlog $j>i$

$\Rightarrow a^i(a^{j-i}-1)=0$

as $a\neq 0$, R is ID

$\Rightarrow a^{j-i}=1$

Exe: show that $\mathbb{Q}[\sqrt[3]{2}]$ is a field

Ans:

$$\mathbb{Q}[\sqrt[3]{2}] = \left\{a+b(2)^{\frac{1}{3}} + c(2)^{\frac{2}{3}} \mid a,b,c\in\mathbb{Q}\right\}$$

$$x^3+y^3+z^3-3xyz = (x^2+y^2+z^2-xy-xz-yz)(x+y+z)$$

$$= x^3+x^2y+x^2z + y^3+y^2z+y^2x + z^3+z^2x+z^2y - x^2y-xy^2-xyz - x^2z-xz^2-xyz - xyz-y^2z-yz^2$$

if $x^2+y^2+z^2-xy-yz-zx=0$

then $2(x^2+y^2+z^2)=2(xy+yz+zx)$

$x^2+y^2+z^2-2(x^2+y^2+z^2) = (x+y+z)^2$ (contradiction)

as $x+y+z\neq 0$ assumption

So, $(x+y+z)(x^2+y^2+z^2-xy-yz-zx) \neq 0$

$\because \quad x+y+z \neq 0$

$\Rightarrow x^3+y^3+z^3-3xyz \neq 0$

$\Rightarrow \dfrac{x^2+y^2+z^2-xy-yz-zx}{x^3+y^3+z^3-3xyz} = \dfrac{1}{x+y+z} \quad \because \quad x+y+z \neq 0$

now if $x = a$

$y = b(2)^{1/3}$

$z = c(2)^{2/3}$ then we are done as

$* \; a+b(2)^{1/3}+c(2)^{2/3} \neq 0$

$\exists \; \dfrac{a^2+b(2)^{2/3}+2c(2)^{1/3}-(a)(b)(2)^{\frac{1}{3}}-(b)(c)(2)}{-(2)^{1/3}(a)(c)}$

$a^3+2b^3+4c^3-6abc$

16th Jan:

Quiz-1 : 27th Jan 7-8 PM Tuesday

Exe: Show that $\mathbb{Q}$ and $\mathbb{R}$ are isomorphic as abelian group but not as rings → dove down

Defn: R: ID the quotient field of R $qf(R) = \left\{ \frac{a}{b} ; a, b \in R, b \neq 0 \right\}$

$\frac{a}{b}$ is an equivalence class, relation $\frac{a}{b} = \frac{a'}{b'}$ iff $ab' - ba' = 0$ in R

addition: $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$

multiplication: $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$

Exe: check well definedness of $qf(R)$ i.e

if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then → dove down

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$$

Note: $\frac{a}{b} = \frac{0}{1}$ iff $a \cdot 1 - b \cdot 0 = 0 \Rightarrow a = 0$

so, $\frac{a}{b} = 0$ iff $a = 0$

and $\frac{a}{b} = \frac{1}{1}$ iff $a \cdot 1 - b \cdot 1 = 0 \Rightarrow a = b$

so, $\frac{a}{b} = 1$ iff $a = b$

$\frac{a}{b} \neq 0$ then $a \neq 0$, then $\frac{b}{a} \in qf(R)$ and $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

as $\frac{b}{a} \cdot \frac{a}{b} = 1 = \frac{a}{b} \cdot \frac{b}{a}$

Exe: check that $(qf(R), +, \cdot)$ is a field using above results → dove down

$\exists$ natural ring homomorphism $\varphi : R \to qf(R)$

$a \mapsto \frac{a}{1}$

φ is injective (trivial)

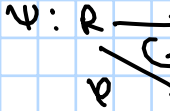
$\varphi(R) \cong R$

$\cap$

$qf(R)$

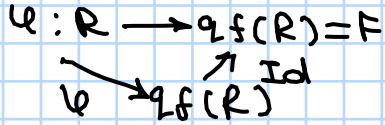
universal property:

If $\psi : R \to F$ any injective ring homomorphism, F: field



$\tilde{\psi}$ is unique isomorphism which makes diagram commute if $F = qf(R)$

$\tilde{\psi}\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)}$ so $qf(R) \cong F$



if R sitting inside F, then $qf(R) \cong F$

Eg: ① $R = \mathbb{Z}$ $qf(\mathbb{Z}) = \left\{ \frac{m}{n} ; n \neq 0 \right\} = \mathbb{Q}$

② $R = K[t]$ K is a field, t: indeterminate over K (symbol/place holder)

$qf(K[t]) = K(t)$

$= \left\{ \frac{f(t)}{g(t)} ; f, g \in K[t], g \neq 0 \right\}$

③ $\mathbb{F}_p[t]$, infinite ID having characteristic p

$qf(\mathbb{F}_p[t])$ is infinite ID having characteristic p

$= \left\{ \frac{f(t)}{g(t)} ; f, g \in \mathbb{F}_p[t], g \neq 0 \right\}$

$H(\mathbb{C})$ = ring of holomorphic functions on $\mathbb{C}$

↑ ID ↑ analytic / infinite series

$qf(H(\mathbb{C}))$ = field of meromorphic functions on $\mathbb{C}$ ← ratio of holomorphic

Eg: $R = K[[x]]$ (power series)

$\Rightarrow qf(R) = K((x)) = K[[x]]\left[\frac{1}{x}\right]$ as $\frac{1}{1+\sum \alpha_i x^i} = \sum \beta_i x^i$

Defn: R: domain $r \neq 0 \in R$, r not unit, r is irreducible if $r = a \cdot b \Rightarrow a$ or b is unit

THEOREM: R is PID, $r \neq 0$ then

r is irreducible iff $\langle r \rangle$: maximal ideal of R iff $R/\langle r \rangle$ is a field

proof: for PIDs

$(a) \supseteq (b) \Leftrightarrow a \mid b$

so having no proper containing ideal (maximal) same as having no proper divisor

(r) is maximal $\Leftrightarrow$ (r) has no proper container (d)

$\Leftrightarrow r$ has no proper divisor d

$\Leftrightarrow r$ is irreducible

now if R/I is a field

let $B \supseteq I$ B be a proper ideal

$B \neq I$ then

$\exists\, b \in B$, $b \notin I \Rightarrow b + I \neq 0 + I \in R/I$

so, $\exists\, c + I$ s.t

$(b+I)(c+I) = 1 + I$

as $b \in B$, $bc \in B$

$bc + I = 1 + I$

$\Rightarrow 1 - bc \in I \subseteq B$

$\Rightarrow 1 - bc \subset B$

so, $1 - bc + bc \subseteq B$ as $b \cdot c \in B$

$\Rightarrow 1 \in B \Rightarrow B = R$ (contradiction)

so, I is maximal

($\Leftarrow$) I is maximal $b \in R$ $b \notin I$ $B = \{ br + a \mid r \in R, a \in I \}$

B is an ideal properly containing I

$\Rightarrow B = R$ as I is maximal

so, $1 = bc + a'$ $a' \in I$, $1 + I = bc + a' + I = bc + I$

$\Rightarrow 1 + I = (b+I)(c+I) \Rightarrow R/I$ is a field

Exe: ① give examples of domain R, not PID

② find r: irreducible, but $\langle r\rangle$ not maximal → done down

③ show that $\langle r\rangle$: prime ideal $\Rightarrow \langle r\rangle$ is irreducible
$\nexists$ (find example)

④ R: UFD, then $r \neq 0 \in R$ is irreducible iff r is prime

Note: r is prime $\Leftrightarrow \langle r\rangle$ is prime ideal

Def: (Polynomial ring over R) $R^n = R\times R\times\cdots\times R$ (n times)

$R^n \subset R^{n+1}$
$a \mapsto (a,0)$

$\bigcup_{n\geq 0} R^n = R^\infty$: polynomial ring in one indeterminate

$a \in R^\infty$ $a=(a_0,a_1,\dots)$, $a_i=0$ for $i \geq n$ for some n

$b=(b_0,b_1,\dots)\in R^\infty$
$a+b=(a_0+b_0, a_1+b_1,\dots)$
$a\cdot b=(c_0,c_1,\dots)$ $c_i = a_0b_i+a_1b_{i-1}+\cdots+a_ib_0$

Exe: show that $(R^\infty,+,\cdot)$; ring → done down

Note: we write $a=(a_0,a_1,\dots) = a_0+a_1t+a_2t^2+\cdots$

$(1,0,\dots)=t^0$
$(0,1,0,\dots)=t^1$
$t^2=t\cdot t^1$

Note: $R[t][u] := R[t,u] = R[u][t]$

$R[t_i; i\in I]$: polynomial ring over R in arbitary no of variables $\{t_i; i\in I\}$

$$= \left\{ \sum_{\text{finite}} a_e t_{n_1}^{e_1} t_{n_2}^{e_2}\cdots t_{n_r}^{e_r} \;;\; n_i\in I, a_e\in R, e_i\geq 0 \right\}$$

Note: If $f(t)\in R[t]$, for any $r\in R$, it gives a function

$$f: R \longrightarrow R$$
$$r \mapsto f(r)$$

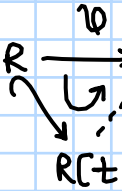
Even if $f\neq g\in R[t]$, it may give same fution from $R\to R$

Eg: $R=\mathbb{F}_2$ $f=t, t^2$ $t=t^2$ as futions: $\mathbb{F}_2\to\mathbb{F}_2$

Universal property of polynomial ring: (one variable)

R, S ring $\varphi: R\to S$ ring homomorphism, then $\exists$ unique extension of φ (fixing some s)

$\tilde\varphi(t)=s$, $\tilde\varphi|_R=\varphi$ → $\tilde\varphi$ is unique with this properties



if such a homomorphism

$a_0 + a_1 t + \cdots a_n t^n \xrightarrow{\tilde{\varphi}} \tilde{\varphi}(a_0) + \tilde{\varphi}(a_1)\tilde{\varphi}(t) + \cdots + \tilde{\varphi}(a_n)\tilde{\varphi}(t)^n$

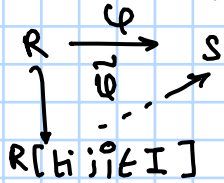
$= \varphi(a_0) + \varphi(a_1)s + \varphi(a_2)s^2 + \cdots \varphi(a_n)s^n$

as φ, s given to us, $a_0 + a_1 t + \cdots + a_n t^n$ has to go to above element, no other choice

so, $\tilde{\varphi}$ is unique

Exe: $\tilde{\varphi}(f(t) + g(t)) = \tilde{\varphi}(f(t)) + \tilde{\varphi}(g(t))$ → done down

Universal property of polynomial ring: (multiple variable)



homomorphism

given $\{s_i \in S ; i \in I\}$

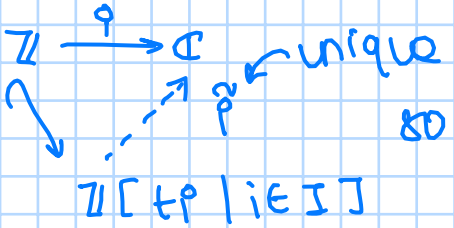
s.t $\tilde{\varphi}|_R = \varphi$ $\tilde{\varphi}(t_i) = s_i$

$\exists\, \tilde{\varphi}$ unique homomorphism (same as one variable case)

Eg: $\mathbb{C} \supset S$, we want smallest subring

subring of $\mathbb{C}$ generated by S

$S = \{s_i ; i \in I\}$



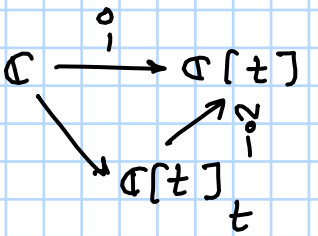
so, $\mathrm{img}(\tilde{\varphi})$ = smallest subring of $\mathbb{C}$ generated by S

now,

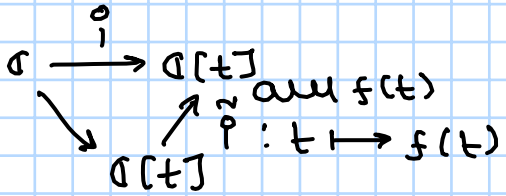
$\mathrm{Aut}_{\text{ring}}(\mathbb{C}[t]) = \{\varphi : \mathbb{C}[t] \to \mathbb{C}[t],\ \varphi|_{\mathbb{C}} = id,\ \varphi \text{ is automorphism}\}$

$\varphi_0 : t \to -t$

$\varphi_{a,b} : t \mapsto at + b \quad a \neq 0$



φ: ring homomorphism



we use universal property and now if $\tilde{f} : \mathbb{C}[t] \to \mathbb{C}[t]$ is bijective, it's an automorphism ($\tilde{f}$ is unique)

if $\tilde{f} : t \mapsto at + b \quad a \neq 0$, then $(\tilde{f})^{-1} : t \mapsto \frac{t-b}{a}$

Exe: $\mathbb{C}[t] \xrightarrow{\varphi} \mathbb{C}[t]$
$\varphi|_{\mathbb{C}} = id$ $\varphi(t) = f(t)$ $\deg f \geq 2$, then φ is not surjective and do not an automorphism
similarly $\deg f = 0$ not possible → done down
then from property only
$\varphi: t \longmapsto at+b$ $a \neq 0$ form

let φ: $\mathbb{C}$ automorphism of $\mathbb{C}[t_1, t_2]$

$\varphi_0 = id$

φ_1 : $t_1 \longrightarrow t_2$, $t_2 \longrightarrow t_1$

$\mathrm{Aut}(\mathbb{C}[t_1,t_2])$ ↙ $\mathbb{C}$ is a group wrt composition

φ_2 : $t_1 \longrightarrow at_1 + b$ $a \neq 0$
$t_2 \longrightarrow a't_2 + b'$ $a' \neq 0$

φ_3 : $t_1 \longrightarrow a_1t_1 + b_1t_2 + c_1$, $t_2 \longrightarrow a_1t_1 + b_2t_2 + c_2$ $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \in GL_2(\mathbb{C})$

φ_4 : $t_1 \longrightarrow t_1 + f(t_2)$, $t_2 \longrightarrow t_2$ ↖ any polynomial in $\mathbb{C}[t_2]$

Theorem: $\mathrm{Aut}_{\mathbb{C}}(\mathbb{C}[t_1,t_2])$ is generated by $GL_2(\mathbb{C})$ and $(t_1,t_2) \longmapsto (t_1 + f(t_2), t_2)$

Note: set of automorphism of an object will form a group wrt compositions

Exe: ① R: domain ⇒ R[t] is domain

② R[t] is PID ⇔ R is field → done down

③ K field, then units of K[t] = units of K

Exe: show that $\mathbb{C}$ and $\mathbb{R}$ are isomorphic as abelian group but not as rings

Ans:

$\mathbb{C}, \mathbb{R}$ are fields of char 0

$(F,+)$ of char 0 is uniquely divisible group i.e
$\forall n \in \mathbb{Z}$,
$[n]: F \longrightarrow F$
$x \longmapsto nx$ is isomorphism + homomorphism (group $(+)$) (for commutative)
moreover
$[n]^{-1}: F \longrightarrow F$ $n \neq 0$, F is commutative
$x \longmapsto \frac{1}{n}x$

for any $\frac{p}{q} \in \mathbb{Q}$ s.t $p \neq 0$, and any $x \in M$ (uniquely divisible commutative group)
$\frac{p}{q}x = y$ ↙ unique $\in M$ s.t $qy = px$
↘ $[p]: M \longrightarrow M$ is isomorphic
$q \neq 0 \Rightarrow [q]^{-1}: M \longrightarrow M$

now, when V is a vectorspace over field K
cardinality of V is more than that of K
then dimV is equal to card V

$V = \mathbb{R}$ or $\mathbb{C}$
$K = \mathbb{Q}$ so, both have continuum cardinality
$(|\mathbb{C}| = |\mathbb{R}|^2)$

now, from above $\mathbb{R}, \mathbb{C}$ have same dimension (continuum)
and so are isomorphic as vector spaces

$\Rightarrow \mathbb{R}, \mathbb{C}$ isomorphic as groups wrt $+$ (∵ we mapped basis)

as $T(\vec{v}) = T(a_1\vec{v}_1 + \cdots + a_k\vec{v}_k)$
$= a_1 T(\vec{v}_1) + \cdots + a_k T(\vec{v}_k)$

$T(\vec{v} + \vec{u}) = (\quad) + (\quad) \in \mathbb{C}$

$(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ is not isomorphic as
if so then
$\exists \varphi: \mathbb{R} \to \mathbb{C}$ be an isomorphism

$\varphi(1) = 1$
$\exists \alpha \in \mathbb{R}$ s.t $\varphi(\alpha) = i$
and so $\varphi(-\alpha) = -i$
then $\varphi(\alpha)\varphi(-\alpha) = -(-1) = 1$
$\Rightarrow \varphi(-\alpha^2) = 1$
$\Rightarrow -\alpha^2 = 1$
this is a contradiction as $-\alpha^2 \leq 0$

Exe: check well definedness of $qf(R)$ i.e
if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$$

Ans: $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$

then $\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{adb'd' + cbd'b'}{bdb'd'}$

$ab' - a'b = 0$
$cd' - c'd = 0$

$= \frac{a'b\cancel{d}d' + c'\cancel{d}\cancel{b}b'}{\cancel{b}\cancel{d}b'd'}$

$= \frac{a'd' + c'b'}{b'd'}$

$= \frac{a'}{b'} + \frac{c'}{d'}$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{acb'd'}{bdb'd'} = \frac{(a'b)(c'd)}{bdb'd'} = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'}$$

Exe: check that $(qf(R), +, \cdot)$ is a field using above results
Ans:

$qf(R) = \left\{ \frac{a}{b} \mid b \neq 0, a, b \in R \right\}$

as, $\forall x, y \in qf(R)$ $x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in qf(R)$ as $b \neq 0, d \neq 0$

$x-y \in Qf(R)$ as $x-y = \frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd} \in Qf(R)$ as $bd \neq 0$

x^{-1} exist if $x \neq 0$, $x^{-1} \in Qf(R)$ and $1, 0$ exist (this was shown above)

so, $(Qf(R), +, \cdot)$ is a field

Exe: ① give examples of domain R, not PID

② find r: irreducible, but $\langle r \rangle$ not maximal

③ show that $\langle r \rangle$: prime ideal $\Rightarrow \langle r \rangle$ is irreducible
$\nLeftarrow$ (find example)

④ R: UFD, then $r \neq 0 \in R$ is irreducible iff r is prime

Ans: ① $\mathbb{Z}[X]$ is ID as

for $f(x)g(x) = 0$ $f, g \in \mathbb{Z}[X]$

as polynomials are of finite degree

$f(n)g(n) = 0 \ \forall n \in \{1, 2, .. 2\max\{\deg(f), \deg(g)\} + 2\}$

then from PHP $g(n_i) = 0$ or $f(n_i) = 0$ for atleast $\max\{\deg(f), \deg(g)\} + 1$

$\Rightarrow g \equiv 0$ or $f \equiv 0$

as more zeros than degree

so, $\mathbb{Z}[t]$ is PID

now, $\langle 2, t \rangle = \{ 2\alpha + t\beta \mid \alpha, \beta \in \mathbb{Z}[t] \}$

$\langle 2, t \rangle = 2f(t) + t g(t)$ for $f, g \in \mathbb{Z}[t]$

now if $\exists h(x) \in \mathbb{Z}[t]$ s.t

$\langle 2, t \rangle = \langle h(t) \rangle$

then

case I: $h(t)$ deg $= 0$

in this case, as $2 \in \langle 2, t \rangle$
$h(t)$ has to be 1 or 2, not 1 as then $\langle h(t) \rangle = \mathbb{Z}[t]$

so, $h(t) = 2$
but then
$t \in \langle 2, t \rangle$ but $t \notin \langle h(t) \rangle$

case II: deg $h(t) \geq 1$

were, as $2 \in \langle 2, t \rangle$ but $\deg(h(t)) \geq 1$ so, $2 \notin \langle h(t) \rangle$

so, $\nexists\, h(t)$ s.t $\langle 2, t \rangle = \langle h(t) \rangle$
$\Rightarrow \mathbb{Z}[t]$ not PID

② $2 \in \mathbb{Z}[t]$ is irreducible (as 2 is prime in $\mathbb{Z}$)

now, $\langle 2 \rangle = \{2f(t) \mid \forall f(t) \in \mathbb{Z}[t]\}$

$\subseteq \langle 2, t \rangle$ (trivial)

so, $\langle 2 \rangle$ is not maximal

also, $1 \notin \langle 2, t \rangle$ so, $\langle 2, t \rangle$ is proper ideal

③ let $I = I_1 \cap I_2$ be a prime ideal

then $I \subseteq I_1$ and $I \subseteq I_2$

if not irreducible

then

$I_1 \setminus I \neq \phi$, $I_2 \setminus I \neq \phi$

let

$\alpha \in I_1 \setminus I$, $\beta \in I_2 \setminus I$

then

as $\alpha \cdot \beta \in I_1 \cdot I_2 \subseteq I_1 \cap I_2$

$\Rightarrow \alpha \cdot \beta \in I_1 \cap I_2$

$\Rightarrow \alpha \cdot \beta \in$ prime ideal I

$\Rightarrow \alpha \in I$ or $\beta \in I$

but $\alpha \notin I$ and $\beta \notin I$ this is a contradiction

so, $I = I_1$ or I_2 i.e I is irreducible

Converse not true as

$\mathbb{Z}[\sqrt{3}]$

$N(a + b\sqrt{3}) = |a^2 + 3b^2|$

$N(x) = 0 \Leftrightarrow |a^2 + 3b^2| = 0$

$\Leftrightarrow a^2 = 3b^2 = 0$

$\Leftrightarrow a = 0, b = 0 \quad x = 0$

$N(xy) = N(x)N(y)$

as $N((a+\sqrt{3}b)(c+\sqrt{3}d)) = N(ac + \sqrt{3}ad + \sqrt{3}bc - 3bd)$

$= |(ac - 3bd)^2 + 3(ad + bc)^2|$

$N(a+\sqrt{3}b)\,N(c+\sqrt{3}d)$

$= |a^2 + 3b^2||c^2 + 3d^2|$

$= |a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2|$

$= |a^2c^2 + 9b^2d^2 + 6acbd + 3a^2d^2 + 3b^2c^2 - 6abcd|$

$= |(ac - 3bd)^2 + 3(ad + bc)^2|$

$N(x) = 1$ iff x is a unit

as

$N(x) = 1 \quad |a^2 + 3b^2| = 1, |(a - \sqrt{3}b)(a + \sqrt{3}b)| = 1$

$x(a - \sqrt{3}b) = 1$

or $x(\sqrt{3}b - a) = 1$

same for converse direction

now if $2 = x \cdot y$ x, y not units

then

$N(2) = 4 = N(x)\,N(y)$

$N(x), N(y) \neq 2$

$\Rightarrow N(x) = N(y) = 2$

$\Rightarrow 2 = a^2 + 3b^2$

not possible

$\Rightarrow 2$ is irreducible by contradiction

but $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

$2 \nmid (1+\sqrt{-3})$ or $(1-\sqrt{-3})$

$\Rightarrow 2$ is not prime in $\mathbb{Z}[\sqrt{-3}]$

so, 2 irreducible but not prime

(4) r is prime $\Rightarrow r$ is irreducible

is already above

if r is reducible

then for $ab \in (P) \setminus \{0\}$

$ab = cp$

$a = p_1 \dots p_k$, $b = q_1 \dots q_m$, $c = r_1 \dots r_n$ } irreducibles

$p_1 \dots p_k q_1 \dots q_m = r_1 \dots r_n p$

$r_1 \dots r_n$ have one of $p_1 \dots p_k, q_1, \dots q_m$ ($\because$ uniqueness)

$\Rightarrow p \mid p_i$ or q_j for some i, j

$\Rightarrow p \mid a$ or $p \mid b$

$\Rightarrow a$ or $b \in (p)$

$\Rightarrow p$ is prime

Exe: show that $(R^\infty, +, \cdot)$ is ring

Ans: $\underset{\sim}{a}, \underset{\sim}{b} \in R^\infty$

$\exists\, n_1, n_2 \in \mathbb{N}$ s.t

$\underset{\sim}{a} \in R^{n_1}$ $\underset{\sim}{b} \in R^{n_2}$

so, $n = \max(n_1, n_2) \Rightarrow \underset{\sim}{a}, \underset{\sim}{b} \in R^n$ (extended with 0s)

$\Rightarrow$ as R^n is a ring

$\underset{\sim}{a} \cdot \underset{\sim}{b} \in R^n$, $\underset{\sim}{a} - \underset{\sim}{b} \in R^n$

$\Rightarrow \underset{\sim}{a} \cdot \underset{\sim}{b} \in R^\infty$, $\underset{\sim}{a} - \underset{\sim}{b} \in R^\infty$

Exe: $\tilde{\varphi}(f(t) + g(t)) = \tilde{\varphi}(f(t)) + \tilde{\varphi}(g(t))$

Ans:

$\varphi : R \to S$

$\to R(t)$

$$f(t) = \sum_{i=0}^{n} \alpha_i t^i$$

$$g(t) = \sum_{i=0}^{m} \beta_i t^i$$

$$\tilde{\varphi}(f(t)+g(t)) = \tilde{\varphi}\left(\sum_{i=0}^{n} \alpha_i t^i + \sum_{i=0}^{m} \beta_i t^i\right)$$

$$= \sum_{i=1}^{n} \varphi(\alpha_i) s^i + \sum_{i=1}^{m} \varphi(\beta_i) s^i$$

$$= \tilde{\varphi}(f(t)) + \tilde{\varphi}(g(t))$$

and $$\tilde{\varphi}(f(t).g(t)) = \tilde{\varphi}\left(\sum_{i=0}^{n} \alpha_i t^i \cdot \sum_{i=0}^{m} \beta_i t^i\right)$$

$$= \tilde{\varphi}\left(\sum_{j=0}^{m}\sum_{i=0}^{n} \alpha_i \beta_j t^{i+j}\right)$$

$$= \sum\sum \varphi(\alpha_i)\varphi(\beta_j) s^{i+j}$$

$$= \sum \varphi(\alpha_i) s^i \cdot \sum \varphi(\beta_j) s^j$$

$$= \tilde{\varphi}(f(t)) \cdot \tilde{\varphi}(g(t))$$

ex: $\mathbb{C}[t] \xrightarrow{\varphi} \mathbb{C}[t]$

$\varphi|_{\mathbb{C}} = id$ $\varphi(t) = f(t)$ deg $f \geq 2$, then φ is not surjective and so not an automorphism

similarly deg $f = 0$ not possible then from property only

$\tilde{\varphi}: t \longmapsto at+b$ $a \neq 0$ form

Ans: $\mathbb{C}[t] \xrightarrow{\varphi} \mathbb{C}[t]$

$\varphi|_{\mathbb{C}} = id$ $\varphi(t) = f(t)$ deg $f \geq 2$

$\varphi: t \longmapsto f(t)$ if φ is bijective then $f(t)$ deg ≥ 2

$\Rightarrow f(t) = \sum_{i=0}^{n} \alpha_i t^i$ deg n $\alpha_n \neq 0$

then $t^{n+1} \in \mathbb{C}[t]$

if $\exists\, g(t) \in \mathbb{C}[t]$ $\varphi(g(t)) = t^{n+1}$

so, $g(f(t)) = t^{n+1}$

$\Rightarrow g\left(\sum_{i=1}^{n} \alpha_i t^i\right) = t^{n+1}$

then deg $g = 0$ as if deg $g \geq 1$

then $\exists (\alpha_n t^n)^{\deg g}$ term

but right side max degree $n+1$

so, g is constant

but then $\alpha = t^{n+1}$ is not true

so, φ is not surjective, φ not bijective

similarly if $\varphi : t \longrightarrow c$ some constant
then φ is bijective
trivial to see $\varphi(g(t)) = g(c) \in \mathbb{C}$

so, $t \in \mathbb{C}[t]$ but as $t \notin \mathbb{C}$
$\Rightarrow$ no $g(t) \in \mathbb{C}[t]$ s.t
$\varphi(g(t)) = t$
so, φ is not surjective and so
only automorphisms of $\mathbb{C}[t]$ is
$t \longmapsto at + b \quad a \neq 0$

Exe: ① R: domain $\Rightarrow R[t]$ is domain
② $R[t]$ is PID $\Leftrightarrow$ R is field
③ K field, then units of $K[t]$ = units of K

Ans:
① R: domain then
for $a, b \in R$, $a \cdot b = 0$
$\Rightarrow a = 0$ or $b = 0$

then $R[t]$ is s.t for $g(t) \in R[t], f(t) \in R[t]$
s.t
$g(t) f(t) = 0$
then let $m = \max\{\deg g, \deg f\}$
then $g(t) = \sum_{i=0}^{m} \alpha_i t^i$

$f(t) = \sum_{i=0}^{m} \beta_i t^i \quad \alpha_i, \beta_i \in R$

$$g(t)f(t) = \sum_{i=0}^{m}\sum_{j=0}^{m} \alpha_i \beta_j t^{i+j} = 0$$

$$\Rightarrow g(t)f(t) = (\alpha_0\beta_0, \alpha_1\beta_0 + \alpha_0\beta_1, \alpha_2\beta_0 + \alpha_1\beta_1 + \alpha_0\beta_2 \ldots, \alpha_m\beta_0 + \cdots \alpha_0\beta_m)$$

now if $\alpha_0\beta_0 = 0$

Case I: $\beta_0 \neq 0, \alpha_0 = 0$

then $\alpha_0 = 0$, and so $\alpha_1\beta_0 = 0 \Rightarrow \alpha_1 = 0$

$\alpha_2\beta_0 = 0 \Rightarrow \alpha_2 = 0$ and similarly $\alpha_i = 0 \ \forall i \in \{0, \ldots m\}$

$\Rightarrow g(t) \equiv 0$

Case II: $\alpha_0 \neq 0, \beta_0 = 0$
then similar to above $f(t) \equiv 0$

case III: $\alpha_0 = 0$ and $\beta_0 = 0$

then

$\alpha_1 \beta_1 = 0$ and so above steps will continue till we hit non-zero coeff of f or g (always possible)

so, $f \equiv 0$ or $g \equiv 0$

② $R[t]$ is PID iff R is field

($\Rightarrow$) $R[t]$ is PID then

for any

$0 \neq a \in R$ $t \in R[t]$

(a, t) is an ideal

so,

$\exists\, c(t) \in R[t]$ s.t

$(c(t)) = (a, t)$

$\exists\, b(t) \in R[t]$ s.t

$a = c(t)\, b(t) \Rightarrow b(t) = b \in R,\ c(t) = c \in R$ as $\deg a = 0$

$\exists\, d(t) \in R[t]$ s.t

$t = d(t)\, c(t)$

$\Rightarrow t = d(t)\, c$

then $d(t) = et + f$ $e, f \in R$

$\Rightarrow t = c[et + f]$

then $ce = 1$

$\Rightarrow 1 \in (c(t)) = (c) = R[t]$

$\Rightarrow (a, t) = R[t]$

so, $\exists\, \gamma(t), \gamma'(t) \in R[t]$ s.t

$a\gamma(t) + \gamma'(t)\, t = 1$

let $t = 0$ then

$a\gamma(0) = 1$

$\Rightarrow \gamma(0)$ is inverse of a

$\forall\, a \neq 0$ in R, $\exists\, \gamma(0)$ inverse of a

$\Rightarrow R$ is a field

($\Leftarrow$) If R is a field

then

$\forall a, b \in R[t]$, $a \neq 0$, $b \neq 0$ $\deg(ab) \geq \deg(a)$

and from division theorem of polynomials forms over fields

$\forall a, b \in R[t]$, $b \neq 0$ $\exists\, q, \gamma \in R[t]$ s.t $a = qb + \gamma$

where $\deg(\gamma) < \deg(b)$ or $\gamma = 0$

q, γ are unique

then deg is Euclidean valuation on $R[t]$

$\Rightarrow R[t]$ is ED

$\Rightarrow R[t]$ is PID

③ K is a field then $\forall r \in$ unit of $K[t]$

$r = \sum_{i=1}^{n} \alpha_i t^i$ s.t $\alpha_n \neq 0$ $\deg(r) = n$

then if $n \geq 1$ then

$\sum_{i=1}^{n} \alpha_i t^i$ is not invertible as if so, then $\exists g(t) \in R[t]$

s.t $\left(\sum_{i=1}^{n} \alpha_i t^i\right)(g(t)) = 1$

$\Rightarrow \deg\left(g(t)\left(\sum_{i=1}^{n} \alpha_i t^i\right)\right) = 0$

but $\deg\left(g(t).\left(\sum_{i=1}^{n} \alpha_i t^i\right)\right)$

$\geq \deg\left(\sum_{i=1}^{n} \alpha_i t^i\right) \geq n \geq 1$

$\Rightarrow 0 \geq 1$

this is a contradiction

so $n = 0$

$\Rightarrow r \in$ unit of K ($\because K$ is a field)

trivial to see if $r \in$ unit of K then $r \in$ unit of $K[t]$

so both are same

20th Jan:

R: Ring containing $\mathbb{Q}$

Defn: (F-algebra) R is a ring containing field F

R, S - $\mathbb{Q}$-algebras (both are $\mathbb{Q}$-algebra)

$\varphi: R \to S$ is $\mathbb{Q}$-algebra homomorphism if $\varphi|_{\mathbb{Q}} = id$

φ: Ring homomorphism

Eg: $\{\mathbb{Q}\text{-algebra homomorphisms } \mathbb{Q}[X] \xrightarrow{\varphi} \mathbb{Q}\}$

$\varphi: \mathbb{Q}[X] \to \mathbb{Q}$

$\varphi|_{\mathbb{Q}} = id$ then $\varphi: X \mapsto q \in \mathbb{Q}$

$\Rightarrow \{\mathbb{Q}\text{-algebra homomorphism } \mathbb{Q}[X] \xrightarrow{\varphi} \mathbb{Q}\} \leftrightarrow \mathbb{Q}$ (Bijection)

$\varphi \mapsto \varphi(X)$

Eg: $\{\mathbb{Q}\text{-alg homo } \mathbb{Q}[x,y] \xrightarrow{\varphi} \mathbb{Q}\} \leftrightarrow \mathbb{Q}^2$ (Bijection)

where $\varphi: x \mapsto q_1$, $y \mapsto q_2$

as $\varphi \mapsto (\varphi(x), \varphi(y))$

we want $\mathbb{Q}$-alg homo

$\varphi: \frac{\mathbb{Q}[x]}{\langle x+3 \rangle} \xrightarrow{\varphi} \mathbb{Q}$

$\mathbb{Q}[\bar{x}] = \frac{\mathbb{Q}[x]}{\langle x+3 \rangle}$

$\mathbb{Q}[x]$

$\bar{x}+3=0$ in $\frac{\mathbb{Q}[x]}{(x+3)}$

$\Rightarrow \varphi(\bar{x}+3)=0$ ($\because \varphi$ is homomorphism)

$\varphi(\bar{x}) = -3$

0 element as $\frac{\mathbb{Q}[x]}{\langle x+3 \rangle}$

so, $\varphi: x \mapsto -3$ or only one φ $\mathbb{Q}$-alg homo

similarly $\frac{\mathbb{Q}[x]}{\langle x^2+1 \rangle} \xrightarrow{\varphi} \mathbb{Q}$

but $x^2+1=0$ has no solution in $\mathbb{Q}$

so, $\varphi(x^2+1)=0$ is not possible

$\varphi: x \mapsto q$

$\varphi(x^2+1) \neq 0$ as $q \in \mathbb{Q}$

or no $\mathbb{Q}$-alg homo possible

Eg: $\frac{\mathbb{Q}[x]}{\langle x^2+1 \rangle} \to \mathbb{C}$ $x^2+1=0$ has 2 solution in $\mathbb{C}$, $x = \pm i \Rightarrow \varphi_1: x \mapsto i$, $\varphi_2: x \mapsto -i$

are two $\mathbb{Q}$-alg homo

$$\varphi: \frac{\mathbb{Q}[x]}{\langle x^2+1\rangle} \longrightarrow \mathbb{C}$$

Eg:

$$\varphi: \frac{\mathbb{Q}[x,y]}{\langle x^2+y^2-1\rangle} \longrightarrow \mathbb{Q} \quad \varphi \text{ is } \mathbb{Q}\text{-alg homo}$$

$$\varphi(x^2+y^2-1)=0 \Rightarrow x^2+y^2=1$$

or,

$$\left\{ \varphi: \frac{\mathbb{Q}[x,y]}{\langle x^2+y^2-1\rangle} \longrightarrow \mathbb{Q} \;\middle|\; \varphi \text{ is } \mathbb{Q}\text{-alg homo} \right\} \overset{\text{bijection}}{\longleftrightarrow} S^1 \cap \mathbb{Q}^2$$

$$(\pm 1, 0), (0, \pm 1)$$

$$\left(\pm\frac{3}{5}, \pm\frac{4}{5}\right)$$

Eg:

$$\left\{ \frac{\mathbb{Q}[x,y]}{\langle x^3+y^3-1\rangle} \longrightarrow \mathbb{Q} \right\} \overset{\text{bijection}}{\longleftrightarrow} \left\{ (a,b) \in \mathbb{Q} \;\middle|\; a^3+b^3=1 \right\}$$

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

← fermats last theorm

Theorm: (Fermat's last theorm) $\{(a,b) \in \mathbb{Q}^2 \mid a^n+b^n=1\} = \{\text{either } a=0 \text{ or } b=0\}$

now,

$$\left\{ \frac{\mathbb{Q}[x_1, x_2, \ldots x_n]}{\langle f_1, f_2, \ldots f_\gamma\rangle} \xrightarrow{\varphi} S \right\} \overset{\text{bijection}}{\longleftrightarrow} \left\{ (s_1, s_2, \ldots s_n) \in S^n \;\middle|\; f_i(s_1, s_2, \ldots s_n)=0 \;\forall\, i=1,2,\ldots \gamma \right\}$$

$f \in \mathbb{Q}[x_1, x_2 \ldots x_n]$

S is some $\mathbb{Q}$-algebra

$\mathbb{Q}[x_1, x_2 \ldots x_n]$

Eg:

$$\left\{ \frac{\mathbb{Q}[x_1, x_2, x_3]}{\langle x_1^2-1, x_2^2-2^2, x_3^2-3^2\rangle} \longrightarrow \mathbb{Q} \right\} \overset{\text{bijection}}{\longleftrightarrow} \{(\pm 1, \pm 2, \pm 3)\} \hookrightarrow \text{total } 8$$

Eg: $2t \in \mathbb{Q}[t]$ is irreducible

as if reducible

then

$2t = f_1 f_2 \quad f_1, f_2 \in K[t] \setminus K$

$\Rightarrow \deg f_1, \deg f_2 \geq 1$ ($\because$ all units have deg 0 in $\mathbb{Q}$)

but

$\deg(f_1 \cdot f_2) = \deg(f_1) + \deg(f_2) \geq 2$

but

$\deg(2t) = 1 < 2$

this is a contradiction

Note: K is field, $f \in K[t]$

(i) $f \in K$ is not irreducible ($K^\times = \{\text{units}\}$)

(ii) $\deg f = 1 \Rightarrow f$ is irreducible

Note: $\deg f \geq 2$, f has a root in $K \Rightarrow f$ is reducible

but $\nLeftarrow$ as $(t^2+1)^2 \in \mathbb{Q}[t]$ is reducible but no root

Note: $\deg f \leq 3$ then
f is irreducible $\Leftrightarrow f$ has no root in K

Exe: $\deg f \leq 3$ then
f is reducible iff f has atleast one root in K → done down

Defn: K is a field, K is algebrically closed if $f \in K[t] \setminus K$ then f has a root in K

Eg: $\mathbb{C}$ is algebrically closed (fundamental theorm of algebra)

Defn: $f \in R[t]$, R is any UFD, here $R = \mathbb{Z}$

$f \in \mathbb{Z}[t]$, $f = a_n t^n + \cdots + a_0$, $a_n \neq 0$
$\deg f = n$

if $\gcd(a_n, \ldots a_0) = 1$ then f is a primite polynomial

Eg: $4t^2+3t+4$; primite in $\mathbb{Z}[t]$
$4t^2+10t+4$; not primitive $\mathbb{Z}[t]$

Note: If $R = K$ (field)
$f \in K[t]$ $f(t) = a_n t^n + \cdots + a_0$ $a_n \neq 0$

$\Rightarrow \gcd(a_n, \ldots a_0) = 1$ ($\because$ all are units in K)

$\Rightarrow f$ is a primite elemnt of $K[t]$, $\forall f \in K[t]$

Exe: $f(t) \in \mathbb{Q}[t]$ $f(t) = \alpha \cdot g(t)$ $\alpha \in \mathbb{Q}$, $g(t) \in \mathbb{Z}[t]$
then $g(t)$ is primitive
$\mathbb{Q} = qf(\mathbb{Z}) = \left\{ \frac{m}{n} ; n, m \in \mathbb{Z}, n \neq 0 \right\}$
→ done down

Theorm: (gauss) ① $f, g \in \mathbb{Z}[t]$ primitive $\Rightarrow f.g$ is primitive

② $f \in \mathbb{Z}[t] \setminus \mathbb{Z}$ irreducible in $\mathbb{Z}[t]$

$\Rightarrow f$ is irreducible in $\mathbb{Q}[t]$
$\nLeftarrow f = 2t$ irreducible in $\mathbb{Q}[t]$
but reducible in $\mathbb{Z}[t]$

proof: ① assume $f.g$ is NOT primitive
then
$\exists$ prime $p \in \mathbb{Z}$ which divides all coeffs of fg

$$\varphi : \mathbb{Z}[t] \to \mathbb{Z}/p\mathbb{Z}[t]$$
$$a_n t^n + \cdots + a_0 \longmapsto \bar{a}_n t^n + \cdots \bar{a}_0$$

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & \searrow & \uparrow \\ \cap & & \cap \\ \mathbb{Z}[t] & \to & \mathbb{Z}/p\mathbb{Z}[t] \\ t & \longmapsto & t \end{array}$$

so, $\varphi(fg) = 0 \Rightarrow \bar{f}\bar{g} = 0$ $\bar{f} = \varphi(f)$, $\bar{g} = \varphi(g)$

$\mathbb{Z}/p\mathbb{Z}$ is ID $\Rightarrow \mathbb{Z}/p\mathbb{Z}[t]$ is ID ($\because$ done before R domain $\Rightarrow$ R[t] domain)

$\Rightarrow \bar{f} = 0$ (wlog case)

then all coeff of f are divisible by p

$\Rightarrow f$ is not primitive

this is a contradiction, so fg is primitive

② assume f is reducible in $\mathbb{Q}[t]$, given $f \in \mathbb{Z}[t] \setminus \mathbb{Z}$ irreducible in $\mathbb{Z}[t]$

$f = g.h \quad g, h \in \mathbb{Q}[t]$ deg g, deg $h \geq 1$

$g = \alpha g_1$

$h = \beta h_1$ $\quad \alpha, \beta \in \mathbb{Q}$ $\quad g_1, h_1 \in \mathbb{Z}[t]$ primitive ($\because$ done before)

$f = (\alpha\beta)\, g_1 h_1$

$g_1 h_1$ is primitive from first part $\in \mathbb{Z}[t]$

let $\alpha\beta = \frac{m}{n}$

$\Rightarrow nf = m g_1 h_1$

as f is irreducible in $\mathbb{Z}[t] \setminus \mathbb{Z}$

gcd of coeff of $f = 1$

$\Rightarrow$ gcd (coeff of nf) $= \pm n$

gcd (coeff of $m g_1 h_1$) $= \pm m$

$\Rightarrow n = m$ ($\because$ taking coeff of both sides)

content (nf) = gcd of coeffs of nf

$= \pm n$

content $(m g_1 h_1) = \pm m$

$\Rightarrow \pm n = m$

so, $f = \pm g_1 h_1$

but as f is irreducible on $\mathbb{Z}[t]$

but $\exists\ g_1, h_1 \in \mathbb{Z}[t] \setminus \mathbb{Z}$ ($\because$ deg(h_1), deg$(g_1) \geq 1$) s.t $f = g_1 h_1$ this is a contradiction

Theorm: $f \in \mathbb{Z}[x]$ primitive, deg $f \geq 1$, then f: irreducible/$\mathbb{Z}$ $\Leftrightarrow$ f irreducible/$\mathbb{Q}$

proof:

($\Rightarrow$) this follows from gauss

($\Leftarrow$) let f be reducible in $\mathbb{Z}[t]$ with deg ≥ 1

so, $\exists\ f_1, f_2 \in \mathbb{Z}[t]$ s.t $f = f_1 f_2$ as $f \in \mathbb{Z}[t]$ is primitive

deg $f_1 \geq 1$, deg $f_2 \geq 1$ as if deg $f_i = 0$ then we can take a constant (not possible here) but now f is reducible in $\mathbb{Q}[t]$, this is a contradiction

Theorm: (mod p irreducibility) Let f be primitive in $\mathbb{Z}[t]$
$f = a_n t^n + \cdots a_0 \in \mathbb{Z}[t]$, $p \in \mathbb{Z}$ prime
$p \nmid a_n$ ($p \nmid lc(f)$ = Leading coeff')

$$\mathbb{Z}[t] \longrightarrow \mathbb{Z}/p\mathbb{Z}[t]$$

$\bar{f}$ is irreducible $\Rightarrow$ f is irreducible in $\mathbb{Z}[t]$

proof:

Assume f is reducible in $\mathbb{Z}[t] \Rightarrow f = gh$ $g, h \in \mathbb{Z}[t]$

$$\Rightarrow \bar{f} = \bar{g}\bar{h}$$

$\bar{f}$ is irreducible $\Rightarrow$ $\bar{h}$ or $\bar{g}$ is unit

wlog $\bar{g}$ is unit
then $\bar{g} \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$

$$p \nmid lc(f) = lc(gh) = lc(g)lc(h)$$

$$\Rightarrow \overline{lc(gh)} = \underbrace{\overline{lc(g)}}_{\neq 0} \underbrace{\overline{lc(h)}}_{\neq 0} \neq 0 \quad (\because p \nmid lc(f))$$

$$\Rightarrow deg(g) = deg(\bar{g}) \text{ and } deg(h) = deg(\bar{h})$$

$$deg(\bar{g}) = 0 \Rightarrow deg(g) = 0$$

$\Rightarrow g$ is constant $\in \mathbb{Z}$

now $f = gh$ s.t $g \in \mathbb{Z}$
but f is primitive
$\Rightarrow g = \pm(1)$
this is a contradiction

Note: In above theorm, If f is not primite then
$f = 2t$ (reducible)
but $\bar{f} = -t$ ($p = 3$) irreducible

Note: if $p \mid a_n$ then also not true as

$f = 2t^2 + t$
$p = 2$ $\bar{f} = t$ irreducible
but f is reducible

also converse not true

exe: $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[t]$ is irreducible → look down

exe: $\mathbb{Z}/p\mathbb{Z}^*$ is abelian group under multiplication

ans: It is abelian as
for $\bar{a}, \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ $a' = \bar{a} + np \in \mathbb{Z}$ $n, m \in \mathbb{Z}$
$b' = \bar{a} + mp \in \mathbb{Z}$

$\bar{a}' = \bar{a}$

$a'b' = (\bar{a}+np)(\bar{b}+mp) = \bar{a}\bar{b} + kp$

$b'a' = (\bar{b}+mp)(\bar{a}+np) = \bar{b}\bar{a} + k''p$

$\overline{a'b'} = \overline{b'a'} \Rightarrow \bar{a}\bar{b} = \bar{b}\bar{a}$ ($\because a', b'$ abelian in $\mathbb{Z}^*$)

So is abelian, it is also cyclic as

Exe: deg $f \leq 3$ then
f is reducible iff f has atleast one root in K

Ans:
($\Rightarrow$) if f is reducible then

$\exists f_1, f_2 \in K[t]$ deg f_1, deg $f_2 \geq 1$
s.t $f = \alpha f_1 f_2$ $\alpha \in$ unit of K

$\deg f = \deg f_1 + \deg f_2$

$\Rightarrow 3 = \deg f_1 + \deg f_2$

$\Rightarrow \exists f_1$ or f_2 s.t
deg f_1 or deg $f_2 = 1$

$\Rightarrow \exists \alpha$ root in K

($\Leftarrow$) trivial as then f has root α

$f = f'(t-\alpha)$

Exe: $f(t) \in \mathbb{Q}[t]$ $f(t) = \alpha . g(t)$ $\alpha \in \mathbb{Q}$, $g(t) \in \mathbb{Z}[t]$
then $g(t)$ is primitive

$\mathbb{Q} = qf(\mathbb{Z}) = \left\{ \frac{m}{n} ; n, m \in \mathbb{Z}, n \neq 0 \right\}$

Ans: let $f(t) = \frac{a_0}{b_0} + \frac{a_1}{b_1} t + \cdots \frac{a_n}{b_n} t^n$

$b_i \neq 0$, $a_n \neq 0$ $a_i, b_i \in \mathbb{Z}$
($\because$ construction of $\mathbb{Q}$)

$= \left(\prod_{i=1}^{n} b_i\right)^{-1} (c_0 + c_1 t + \cdots c_n t^n)$

$c_i = \frac{a_i}{b_i} \prod_{i=1}^{n} b_i$

let $m = \gcd(c_0, c_1 \ldots c_n)$

then $f(t) = m \left(\prod_{i=1}^{n} b_i\right)^{-1} [a_0' + a_1' t + \cdots a_n' t^n]$

$a_i' \in \mathbb{Z}$ ($\because$ property of gcd)

and
$\gcd(a_0', \ldots a_n') = 1$

let $\alpha = m \left(\prod_{i=1}^{n} b_i\right)^{-1} \in \mathbb{Q}$

s.t $g(t) = \sum_{i=0}^{n} a_i' t^i \in \mathbb{Z}[t]$ is primitive

ex: $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[t]$ is irreducible

Ans:

f is primitive &

if f is reducible then $\exists\ f_1, f_2 \in \mathbb{Z}[t]$ s.t

$f(t) = f_1(t) f_2(t)$

$\deg f_1 \geq 1, \deg f_2 \geq 1$

now if $f_1 \to \deg 1$ $f_2 \to \deg 3$

let $f_1 = (x+\alpha)$ $f_2 = (x^3 + \beta x^2 + \varphi x + \delta)$

$f_1 f_2 = (x+\alpha)(x^3 + \beta x^2 + \varphi x + \delta)$

$= x^4 + \beta x^3 + \varphi x^2 + \delta x + \alpha x^3 + \alpha\beta x^2 + \alpha\varphi x + \alpha\delta$

$\alpha + \beta = 0$ $\alpha = -\beta$

$\varphi - \alpha\beta = -10$ $\varphi + \alpha^2 = -10$ $\varphi = -10 - \alpha^2$

$\delta + \alpha\varphi = 0$ $\delta + \alpha(-10 - \alpha^2) = 0$

$\alpha\delta = 1$

$\delta = 10\alpha + \alpha^3$

$\alpha(10\alpha + \alpha^3) = 1$

$\alpha^2(10 + \alpha^2) = 1$

as $\alpha^2 \geq 0$ never possible

& let f_1 be 2 deg

f_2 be 2 deg then

$f_1 f_2 = (x^2 + \alpha x + \beta)(x^2 + \varphi x + \delta)$

$= x^4 + x^3[\varphi + \alpha] + x^2[\delta + \alpha\varphi + \beta] + x[\alpha\delta + \beta\varphi] + \beta\delta$

$\varphi + \alpha = 0$ $\delta + \alpha\varphi + \beta = -10$

$\alpha = -\varphi$

$\alpha\delta + \beta\varphi = 0$ $\beta\delta = 1$

$\alpha\delta - \beta\alpha = 0$

$\alpha = 0$ or $\delta = \beta$

$\varphi = 0$

$\delta + \beta = -10$

$\beta\delta = 1$

$\beta = -10 - \delta$

$(-10 - \delta)(\delta) = 1$

$-10\delta - \delta^2 = 1$

but $\delta^2 + 1 + 10\delta = 0$

as $\Delta = 100 - 4 = 96$

not perfect square

$\delta \notin \mathbb{Z}$

$\delta = \beta$

$2\delta - \alpha^2 = -10$

$\beta^2 = 1 \Rightarrow \beta = \pm 1$

$\delta = \pm 1$

$-2 + \alpha^2 = +10$

$+2 + \alpha^2 = +10$

$\to \alpha \notin \mathbb{Z}$ in both cases

not possible

& f is irreducible by taking cases

ex: K be a field, G finite subgroup of $K^\times$, then G is cyclic

Ans:

we will show that

G be a finite group with n elements, $\forall d \mid n$

$\#\{x \in G \mid x^d = 1\} \leq d$ then G is cyclic

as here G is a finite subgroup then $x^d - 1$ has atmost d roots as K is a field

now let $d \mid n$ $G_d = \{a \in G \mid a^d = 1, d \text{ is lowest such number}\}$ then

① if $G_d \neq \phi$ then $\exists\ y \in G_d$ s.t.,

$\langle y \rangle \subseteq \{x \in G \mid x^d = 1\}$

as $y^d = 1$ s.t. d is lowest of such

so,

$(y^1)^d = 1,\ (y^2)^d = 1, \ldots$

$\Rightarrow \langle y \rangle \subseteq \{x \in G \mid x^d = 1\}$

but $\#\{x \in G \mid x^d = 1\} \leq d \Rightarrow \langle y \rangle = \{x \in G \mid x^d = 1\}$

$(\because |\langle y \rangle| = d)$

so, G_d is set of generators of cyclic group $\langle y \rangle$ of order d

$\#G_d = \phi(d)$ ($\because$ no of generators of group of order d)

② if $G_d = \phi$ then $\#G_d = 0$

$n = \#G$

$= \sum_{d \mid n} \#G_d \leq \sum_{d \mid n} \phi(d)$

now $\sum_{d \mid n} \phi(d) = n$ ($\because G$ is finite)

$\Rightarrow \#G_d = \phi(d)\ \forall\ d \mid n$

$\Rightarrow G_n \neq \phi$ as $n \mid n$

so, G_n is cyclic

ex: $\mathbb{F}_p^*$ is cyclic of order $p-1 = \langle a \rangle$, a is not a square in $\mathbb{F}_p^*$

proof:

from before we know $\mathbb{F}_p^*$ is sub group of field $(\mathbb{F}_p, +)$ and we have proved it is abelian

$\Rightarrow \mathbb{F}_p^*$ is cyclic of order $p-1$ as $n = p-1$ in prev result and $\phi(n) = \phi(p-1) > 0$

now let $a \in (\mathbb{Z}/p\mathbb{Z})^*$ s.t

$\phi(n)$ = no of numbers s.t $i \mid n$ for $1 \le i \le n$

if $\exists\ q \in (\mathbb{Z}/p\mathbb{Z})^*$ s.t $q = x^2$

then as $p-1$ is even (in case of $p>2$)

same for other direction

q is not a generator $\Leftrightarrow$ q is a perfect square

$\Rightarrow$ if q not a perfect square then it will be a generator

Exe: $f = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$ is s.t $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$ is reducible $\forall$ prime p

Ans: f is irreducible in $\mathbb{Z}[x]$ ($\because$ seen before)

now if $b = a^2$ not square $\Rightarrow bc$ is square
$c = a^3$ not square

Case I: 2 is a square in $\mathbb{F}_p^*$ $a^2 = 2$ for $a \in \mathbb{F}_p^*$

$x^2 - 10x^2 + 1 = (x^2-1)^2 - 8x^2$ $\quad 8 = 4a^2$

$= (x^2 - 1 - 2ax)(x^2 - 1 + 2ax)$

Case II: 3 is a square in $\mathbb{F}_p^*$ $b^2 = 3$ for $b \in \mathbb{F}_p^*$

$x^2 - 10x^2 + 1$ $\quad 12 = 4b^2$

$= (x^2+1)^2 - 12x^2$

$= (x^2 + 1 - 2bx)(x^2 + 1 + 2bx)$

Case III: 2 is not a square, 3 is not a square $\Rightarrow$ 6 is a square

$6 = c^2$ $\quad x^2 - 10x^2 + 1 = (x^2-5)^2 - 24$

$= (x^2-5)^2 - 4c^2$

$= (x^2 - 5 - 2c)(x^2 - 5 + 2c)$

So, converse to our theorem is not true and $\exists f$ s.t

$\bar{f}$ is not irreducible $\forall$ p

Theorem: (Eisenstein's criterion of irreducibility) $f = a_n t^n + \dots + a_0 \in \mathbb{Z}[t]$

p: prime, $p \nmid a_n$, $p \mid a_i$ $i = 0, 1, \dots n-1$ $\quad p^2 \nmid a_0$

then f is irreducible in $\mathbb{Q}[t]$

proof: let $\mathbb{Z}[t] \longrightarrow \mathbb{Z}/p\mathbb{Z}[t]$

$f \longmapsto \bar{f} = \bar{a}_n t^n$

if f is reducible in $\mathbb{Q}[t]$ then it is reducible in $\mathbb{Z}[t]$

$f = gh$ (gauss lemma)

$\bar{f} = \bar{g}\bar{h} = \bar{a}_n t^n$

$\bar{g} \mid \bar{a}_n t^n \Rightarrow \bar{g} = \bar{b}_r t^r$ $\quad g = b_r t^r + pb'_{r-1} \dots pb_0$

$\bar{h} \mid \bar{a}_n t^n \Rightarrow \bar{h} = \bar{c}_k t^k$ $\quad h = c_k t^k + \dots pc_0$

$$g(0)\,h(0) = p^2\, b_0 c_0$$

$p^2 \not| \; g(0)h(0) \rightarrow$ contradiction

23rd Jan:

Defn: Σ = collection of all sets

$X, Y \in \Sigma$ $X \sim Y$ if $\exists$ a bijection $f: X \to Y$

$[X]$ = equivalence class, X is called cardinal number

cardinal numbers $\mathcal{C}$: set of all cardinal numbers

$[X] \leq [Y]$ if $\exists$ an injective map $g: X \to X$

reflexive and transitive

Theorem: (Shroeder Bernstine) $[X] \leq [Y]$, $[Y] \leq [X]$ then $\exists\ X \xrightarrow[inj]{f} Y$

$\exists\ Y \xrightarrow[inj]{g} X$ then $X \to Y$ $[X] = [Y]$ i.e $\exists$ a bijection

now, if $|X|$ = infinite then

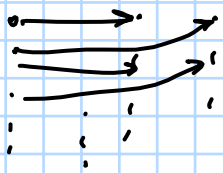
① $|X| = |X \times \{0,1\}|$ (to show $|\mathbb{R}| = |\mathcal{C}|$)

② $|X| = |X \times X|$

for ① $\Sigma = \{(A, \sigma) : \exists$ a bijection $\sigma: A \to A \times \{0,1\}$ and $A \subseteq X\}$

let $A = \{x_1, x_2 \ldots\} \subset X$ ($\because X$ has countable infinite subset)

$\exists\ \sigma : A \longrightarrow A \times \{0,1\}$



$0 \to 0,0$
$1 \to 0,1$
$2 \to 1,0$
$3 \to 1,1$
$\vdots$

so, $(A, \sigma) \in \Sigma$, $\Sigma \neq \phi$

$(A, \sigma) \leq (B, \tau)$ if $A \subseteq B$ and $\tau|_A = \sigma$

any chain $\{(A_i, \sigma_i), i \in I\}$ has an upper bound

(A, σ), $A = \bigcup_{i \in I} A_i$

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A \times \{0,1\} \\ \bigcup A_i & & \bigcup A_i \times \{0,1\} \end{array}$$

$\sigma|_{A_i} = \sigma_i$

so, by Zorn's lemma, $\exists$ a maximal element

now maximal element $M \subseteq X$

Exe: construct a bijection $\sigma: X \longrightarrow X \times \{0,1\}$ from maximal element, similarly for $\sigma: X \longrightarrow X \times X \to$ done done

def: K is a field $\mathrm{char}(K)=0$, then $\mathbb{Q}$-prime subfield

$$\mathbb{Q} = \left\{ \frac{n\cdot 1}{m\cdot 1} ;\ m\neq 0,\ n,m\in\mathbb{Z} \right\}$$

$\mathrm{char}(K)=p>0$, then $\mathbb{F}_p = \mathbb{Z}\cdot 1$: prime subfield

def: $X\subset K$, the subfield X of K generated by

$$X = \bigcap_{X\subset F} F,\quad F: \text{subfield of } K$$

smallest subring:

smallest subring of K generated by $X = \left\{ f(x_1 \dots x_n) \,\middle|\, f\in\mathbb{Z}[t_1 \dots t_n] \right\}$
X is finite

$$\varphi : \mathbb{Z}[t_1 \dots t_n] \longrightarrow K$$
$$1 \longmapsto 1$$
$$t_i \longmapsto x_i \quad \text{(unique homomorphism)}$$

img φ = smallest required subring of K generated by x

if x is not finite, x be arbitary union of finite sets

$$\mathbb{Z}[X] \subset K \leftarrow \text{integral domain}$$
$$\uparrow \text{integral domains}$$

so, smallest field $\supseteq \mathbb{Z}[X]$

K_0 = prime subfield of K then $qf(\mathbb{Z}[X]) = K_0(X)$

$$= \left\{ \frac{f(x_1 \dots x_n)}{g(x_1 \dots x_n)} ;\ f,g\in\mathbb{Z}[t_1,\dots t_n],\ g(x_1 \dots x_n)\neq 0 \right\}$$

eg: $K=\mathbb{C}$, $X=\{\sqrt{2}\}$, $\mathrm{char}(\mathbb{C})=0 \Rightarrow$ smallest subfield contains $\mathbb{Q}$

smallest subfield for $X = \mathbb{Q}(X) = \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} : f,g\in\mathbb{Z}[t], g(\sqrt{2})\neq 0 \right\}$

smallest ring generated by $\sqrt{2}$:

$$\mathbb{Z}[\sqrt{2}] = \left\{ a+b\sqrt{2} \mid a,b\in\mathbb{Z} \right\}$$

$$qf(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2}) = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} ;\ c+d\sqrt{2}\neq 0,\ a,b,c,d\in\mathbb{Z} \right\}$$

$$= \left\{ \alpha+\beta\sqrt{2} ;\ \alpha,\beta\in\mathbb{Q} \right\}$$

$c,d\in\mathbb{Z}$ $c-d\sqrt{2}\neq 0$

$$\Rightarrow \left(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}\right)\left(\frac{c-d\sqrt{2}}{c-d\sqrt{2}}\right) = \frac{ac-ad\sqrt{2}+bc\sqrt{2}-2bd}{c^2-2d^2}$$

$= \alpha + \beta\sqrt{2} \quad \alpha, \beta \in \mathbb{Q}$

so, subring of $\mathbb{C}$ generated by $\{\mathbb{Q} \cup \sqrt{2}\} = \mathbb{Q}(\sqrt{2})$

$(3+\sqrt{2})^{-1} = \frac{1}{3+\sqrt{2}}\left(\frac{3-\sqrt{2}}{3-\sqrt{2}}\right) = \frac{(3-\sqrt{2})}{7}$

Eg: $X = i$ then $\mathbb{Z}[i] = \{a+ib \,;\, a, b \in \mathbb{Z}\}$

$\mathbb{Q}(i) = qf(\mathbb{Z}[i]) = \left\{\frac{a+ib}{c+id} \,;\, a,b,c,d \in \mathbb{Z},\ c+id \neq 0\right\}$

$\Rightarrow \mathbb{Q}(i) = \{\alpha + \beta i \,;\, \alpha, \beta \in \mathbb{Q}\}$

Note: above $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$

↑ ring generated by $\sqrt{2}$ on $\mathbb{Q}$

$f : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[\sqrt{2}]$

$f(t) = \sqrt{2}, \quad f|_{\mathbb{Q}} = id$

then f becomes surjective

$t^2 - 2 \in \ker(f)$

as t^2-2 is irreducible in $\mathbb{Q}[t]$

$\Rightarrow \langle t^2-2 \rangle$ is maximal ideal

$\Rightarrow \ker f = \langle t^2-2 \rangle$ is maximal ideal

$\Rightarrow \frac{\mathbb{Q}[t]}{\langle t^2-2 \rangle} \cong \mathbb{Q}[\sqrt{2}]$

↑ field ($\because \langle t^2-2 \rangle$ is maximal ideal)

$\Rightarrow \mathbb{Q}[\sqrt{2}]$ is a field

similarly $\mathbb{Q}(i) = \mathbb{Q}[i]$

$\Rightarrow \frac{\mathbb{Q}[t]}{\langle t^2+1 \rangle} \cong \mathbb{Q}[i]$ ← field

↑ field ($\because \langle t^2+1 \rangle$ is maximal ideal)

$\Rightarrow \mathbb{Q}[i]$ is field

Eg: $\mathbb{Z}\left[\underset{\alpha}{(2)^{\frac{1}{3}}}\right] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\}$

then $\mathbb{Q}((2)^{\frac{1}{3}}) = qf\left(\mathbb{Z}[(2)^{\frac{1}{3}}]\right)$

$\mathbb{Q}[(2)^{\frac{1}{3}}] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$

as $f : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[(2)^{\frac{1}{3}}]$

$f|_{\mathbb{Q}} = id \qquad f(t) = \alpha$ $\quad f$ is surjective

$\ker(f) = \langle t^3 - 2 \rangle$ ← irreducible

$\frac{\mathbb{Q}[t]}{\langle t^3-2 \rangle} \cong \mathbb{Q}[(2)^{\frac{1}{3}}]$

$\Rightarrow \mathbb{Q}[(2)^{\frac{1}{3}}]$ is a field

$\Rightarrow \mathbb{Q}((2)^{\frac{1}{3}}) = \mathbb{Q}[(2)^{\frac{1}{3}}]$

also, if $\beta = 1 + 2\alpha + \alpha^2$ then we can find β^{-1}

as $1 + 2\alpha + \alpha^2 = 1 + 2t + t^2 + \ker(f)$

$\ker f = \langle t^3 - 2 \rangle$

$t^3 - 2 = (1 + 2t + t^2)(q(t)) + r(t)$

$\Rightarrow \quad 0 = (1 + 2\alpha + \alpha^2)\overline{(q(t))} + \overline{r(t)}$

$\Rightarrow \quad 0 = \beta(\overline{q(t)}) + \overline{r(t)}$

$q(t) = t - 2$

$r(t) = 3t$ ← if complex, we can repeate process again

$0 = \beta(\alpha - 2) + 3\alpha$

$\beta^{-1} = -\frac{(\alpha - 2)}{3\alpha}$

$= -\frac{(\alpha)^2(\alpha - 2)}{3 \cdot 2}$

$= -\frac{\alpha^3}{6} + \frac{2\alpha^2}{6}$

$= -\frac{1}{3} + \frac{1}{3}\alpha^2$ is inverse of β

Ex: for $\mathbb{Q}[\sqrt[4]{2}]$ field, find $(\alpha+2)^{-1}$ → done down

generally, $\mathbb{Q}[\alpha]$ $\alpha = \sqrt[3]{2}$ then $t^3 - 2 = \underbrace{(t^2+1)}_{\beta = \alpha^2+1} t + (-t - 2)$

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

$\Rightarrow \quad (\alpha^2+1)\alpha = (2 + \alpha)$

$\Rightarrow \quad (\alpha^2+1)^{-1} = \frac{\alpha}{\alpha+2}$

similarly $t^3 - 2 = (t+2)(t^2 - 2t + 4) - 10$

$0 = (\alpha+2)(\alpha^2 - 2\alpha + 4) - 10$

$\Rightarrow \frac{10}{\alpha+2} = \alpha^2 - 2\alpha + 4$

$\Rightarrow \frac{1}{\alpha+2} = \frac{\alpha^2 - 2\alpha + 4}{10} \Rightarrow (\alpha^2+1)^{-1} = \frac{\alpha}{\alpha+2} = \frac{\alpha^3 - 2\alpha^2 + 4\alpha}{10}$

Def: $M \supset K$ is field, M/K is a field extension

$X \subset M$ subset

$K(X)$: subfield of M/K generated by X

= subfield of M generated by $K \cup \{X\}$

Eg: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ = subfield of $\mathbb{C}/\mathbb{Q}(\sqrt{2})$ generated by $\sqrt{3}$

($\mathbb{C}/\mathbb{Q}(\sqrt{2})$ → field extension)

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ = subfield of $\mathbb{C}/\mathbb{Q}$ generated by $\{\sqrt{2}, \sqrt{3}\}$

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

($\mathbb{Q}(\sqrt{2})$: generate over $\sqrt{2}$; $(\sqrt{3})$: further over $\sqrt{3}$)

Exe: show that $\mathbb{Q}(i+3) = \mathbb{Q}(i)$ → done down

Exe: show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ so, just show $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ as other side is trivial → done down

Def: $\alpha \in \mathbb{C}$, algebraic number if α is a root of some $f(t) \neq 0 \in \mathbb{Q}[t]$

Eg: $\mathbb{Q}$ all algebraic numbers

$\gamma \in \mathbb{Q}$, is a root of $t - \gamma$

$\sqrt{2}$ is algebraic as $t^2 - 2$ root, similarly $\sqrt{5}$ $\forall \gamma \in \mathbb{Q}$

similarly we can get many

Let $\overline{\mathbb{Q}}$ = set of all algebraic numbers

Eg: $\sqrt{2} \in \overline{\mathbb{Q}}$, $\sqrt{3} \in \overline{\mathbb{Q}}$ then let $\alpha = \sqrt{2} + \sqrt{3}$

$$\Rightarrow \alpha^2 = 2 + 3 + 2\sqrt{6}$$
$$\Rightarrow \alpha^2 - 5 = 2\sqrt{6}$$
$$\Rightarrow \frac{\alpha^2}{2} - \frac{5}{2} = \sqrt{6}$$
$$\Rightarrow \frac{\alpha^4}{4} + \frac{25}{4} - \frac{5\alpha^2}{2} = 6$$
$$\Rightarrow \frac{t^4}{4} + \frac{25}{4} - \frac{5t^2}{2} - 6 = 0 \text{ has root } \sqrt{2} + \sqrt{3}$$

or $f(t) = (t^2 - 5)^2 - 24$ $\quad f(\gamma) = 0$

$\gamma = \sqrt{2} + \sqrt{3}$

Exe: $\alpha, \beta \in \overline{\mathbb{Q}}$ then ① $\alpha + \beta \in \overline{\mathbb{Q}}$

② $\alpha\beta \in \overline{\mathbb{Q}}$

③ $\frac{1}{\alpha} \in \overline{\mathbb{Q}}$

→ done down

Note: from above, we get $\overline{\mathbb{Q}}$ is a field, $\overline{\mathbb{Q}}$ is algebraically closed field
↑ linear ones ⇔ irreducible

Exe: show that $\overline{\mathbb{Q}}$ is countable → done down

Defn: $\alpha \in \mathbb{C} \setminus \overline{\mathbb{Q}}$ is a transidental number

Eg: $e = \sum_{n \geq 0} \frac{1}{n!} \in (2,3)$ is transidental

π = area of circle is transidental

Eg: $\pi+e$, $\pi-e$ both are not algebric as if so then

$(\pi+e)+(\pi-e)$
$(\pi+e)-(\pi-e)$
⇒ atleast one of $\pi+e$ or $\pi-e$ is transidental
(∵ both not algebric)

Exe: construct a bijection $\sigma: X \longrightarrow X \times \{0,1\}$ from maximal element,
similarly for $\sigma: X \longrightarrow X \times X$

Ans:
let M be maximal element of

$$\Sigma = \{(A,\sigma) \mid \sigma : A \to A \times \{0,1\} \text{ is bijection}, A \subseteq X\}$$

now
if $M \neq X$ then $X \setminus M \neq \phi$

Case I: $X \setminus M$ is finite

in this case as X is uncountable, M is uncountable
let $|X \setminus M| = n = \{x_1, x_2, \ldots x_n\}$
then
let $\{y_1, y_2, \ldots\} \subseteq M$ be a countable subset of M
then
$\exists \sigma: M \longrightarrow M \times \{0,1\}$ s.t σ is a bijection
$y_i^\circ \longmapsto (z_i, \delta_i^\circ)$ $\forall i \in \mathbb{N}$

then let σ' be s.t

$\sigma'(x_i) = (z_i, \delta_i^\circ)$

$\sigma'(y_i^\circ) = (z_{i+n}^\circ, \delta_{i+n}^\circ)$
$\forall m \in M \setminus \{y_1, y_2, \ldots\}$
$\sigma'(m) = \sigma(m)$

then $\sigma': X \longrightarrow M \times \{0,1\}$ is a bijective map
as ① σ' is one-one
$\sigma'(x) = \sigma'(y)$
if $\sigma'(x) = \sigma'(y) = (z_k, \sigma_k)$
then trivial
same if
$\sigma'(x) = \sigma'(y) = m \neq (z_k, \sigma_k)$ $\forall k \in \mathbb{N}$
then also trivial

② σ' is onto
this is also trivial as $\forall (z_i, \sigma_i) \in M \times \{0,1\}$
$\exists x$ s.t $\sigma'(x) = (z_i, \sigma_i)$

$\forall\ y \in M \times \{0,1\} \setminus \{(x_i, \sigma_i), i \in \mathbb{N}\}$
$\exists\ x$ s.t $\sigma^{-1}(x) = \sigma(x) = y$

so, $|X| = |M \times \{0,1\}|$
also similarly $|M| = |X \times \{0,1\}|$ by σ^{-1}

but as $|M \times \{0,1\}| = |M|$
$\Rightarrow |X| = |X \times \{0,1\}|$

Case II: $X \setminus M$ is infinite
then $\exists \{x_1, x_2, \ldots\} \in X \setminus M$ countable
s.t
$A = \{x_1, x_2, \ldots\}$

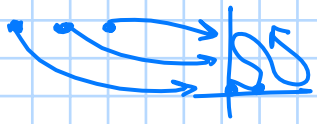
$\sigma : A \longrightarrow A \times \{0,1\}$ is a bijection (shown above)
so, M is not maximal
as
$M \cup A$ is also possible
so, this is a contradiction

a similar proof will work for $|X| = |X \times X|$, where

$\mathcal{E} = \{(A, \sigma) \mid \sigma : A \longrightarrow A \times A$ is a bijection, $A \subseteq X\}$
then $(A, \sigma) \leq (B, \mu)$

$\mathcal{E} \neq \phi$ as for $A = \{x_1, x_2 \ldots\}$

$\sigma : A \longrightarrow A \times A$ i.e $\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ bijection map



$\{(A_i, \sigma_i) \mid i \in I\}$ then $\bigcup_{i=1}^{\infty} A_i$ s.t $\sigma|_{A_i} = \sigma_i$ is maximal element

so, $\sigma : A \longrightarrow A \times A$

or by Zorn's lemma maximal element M similar to above
if $X \setminus M$ = infinite then contradiction

if finite, then again similar construction to get $|X| = |X \times X|$

Ex: for $\mathbb{Q}[\sqrt[4]{2}]$ field, find $(\alpha+2)^{-1}$
Ans:

$f : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[\sqrt[4]{2}]$ $\quad \alpha = \sqrt[4]{2}$

$f(t) = \alpha$

then
$t^4 - 2 \in \ker f$ and irred in $\mathbb{Q}[t]$
$\Rightarrow \langle t^4 - 2 \rangle = \ker f$
$\Rightarrow \frac{\mathbb{Q}[t]}{\langle t^4 - 2 \rangle} \cong \mathbb{Q}[\sqrt[4]{2}]$ ← field

$t^4 - 2 = (t+2)(t^3 - 2t^2 + 4t - 8) + 18$

$t+2 \;\big)\; t^4 + 2 \;\big(\; t^3 - 2t^2 + 4t - 8$
$t^4 + 2t^3$
$-2t^3 + 2$
$-2t^3 - 4t^2$
$4t^2 + 2$
$4t^2 + 8t$
$-8t + 2$
$-8t - 16$
18

$\Rightarrow 0 = (\alpha+2)(\alpha^3-2\alpha^2+4\alpha-8)+18$

$\Rightarrow (\alpha+2)^{-1} = \left(\frac{-\alpha^3+2\alpha^2-4\alpha+8}{18}\right)$

Exe: Show that $\mathbb{Q}(i+3) = \mathbb{Q}(i)$

Ans:

$f : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[i+3]$

$f(t) = i+3$

$(t-3)^2+1 \in \ker(f)$

↳ irreducible

$\Rightarrow \mathbb{Q}[i+3]$ is a field

and so, $\mathbb{Q}[i+3] = \mathbb{Q}(i+3) \cong \frac{\mathbb{Q}[t]}{\langle (t+3)^2+1 \rangle}$

similarly $\mathbb{Q}[i] = \mathbb{Q}(i)$

now,

$\mathbb{Q}(i) = \{a+ib \mid a,b \in \mathbb{Q}\}$

$\mathbb{Q}(i+3) = \{a+(i+3)b \mid a,b \in \mathbb{Q}\}$

$= \{a+ib+3b \mid \underbrace{a+3b}_{a'}, b \in \mathbb{Q}\}$

$= \{a'+ib \mid a', b \in \mathbb{Q}\}$

$= \mathbb{Q}(i)$

Exe: Show that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ so, just show $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ as other side is trivial

Ans:

$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \left\{ \frac{f(\sqrt{2}+\sqrt{3})}{g(\sqrt{2}+\sqrt{3})} \; ; \; f,g \in \mathbb{Z}[t],\ g(\sqrt{2}+\sqrt{3}) \neq 0 \right\}$

$\alpha = \sqrt{2}+\sqrt{3}$

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

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

$\frac{1}{\alpha} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

now, $\alpha - \frac{1}{\alpha} = 2\sqrt{2}$

$\frac{\alpha}{2} - \frac{1}{2\alpha} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\frac{\alpha^2-1}{2\alpha} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

also, similarly $\frac{\alpha}{2} + \frac{1}{2\alpha} = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\frac{\alpha^2+1}{2\alpha} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

then this follows trivially

Ex: $\alpha, \beta \in \bar{\mathbb{Q}}$ then ① $\alpha+\beta \in \bar{\mathbb{Q}}$

② $\alpha\beta \in \bar{\mathbb{Q}}$

③ $\frac{1}{\alpha} \in \bar{\mathbb{Q}}$

Ans: if $n \in \mathbb{N}$, $\alpha \in \mathbb{C}$ and $\theta_1, \theta_2, \ldots \theta_n \in \mathbb{C}$ not all zero s.t

$$\alpha\,\theta_i = a_{i,1}\theta_1 + a_{i,2}\theta_2 + \cdots a_{i,n}\theta_n \quad i = 1,2,\ldots n$$

n^2 coefficient $a_{i,j} \in \mathbb{Q}$ then

$$M = \begin{vmatrix} \alpha - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ & \alpha - a_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{n,1} & \cdots & \cdots & \alpha - a_{n,n} \end{vmatrix} = 0$$

$\det(M) = 0 \Rightarrow \alpha^n + b_1\alpha^{n-1} + \cdots b_n = 0$ form determinant

$b_i \in \mathbb{Q}$

$\Rightarrow \alpha \in \bar{\mathbb{Q}}$

now, let $\alpha, \beta \in \bar{\mathbb{Q}}$ then $\alpha^m + a_1\alpha^{m-1} + \cdots a_m = 0 \quad a_i \in \mathbb{Q}\ i \in \{1,\ldots m\}$

$\beta^r + b_1\beta^{r-1} + \cdots b_r = 0 \quad b_j \in \mathbb{Q}\ j \in \{1,\ldots r\}$

let $n = mr$ and let $\theta_1, \theta_2, \ldots \theta_n$ be

$$1,\ \alpha,\ \alpha^2, \alpha^3, \ldots \alpha^{m-1},\ \beta,\ \beta\alpha,\ \ldots \beta\alpha^{m-1}, \ldots\ \beta^{r-1}\alpha^{m-1}$$

so, $\theta_i \in \mathbb{C}\ \forall i \in \{1,2,\ldots rm\}$

so, for any $\theta_j = \alpha^s\beta^t \quad s = 0,1,\ldots m-1,\ t = 0,1,\ldots r-1$

$$\alpha\theta_j = \alpha^{s+1}\beta^t$$

$$= \begin{cases} \text{some } \theta_k \text{ ; } s+1 \le m-1 \\ (-a_1\alpha^{m-1} - \cdots - a_m)\beta^t \text{ ; } s+1 = m \end{cases}$$

in either case we see that

$$\alpha\theta_j = h_{j,1}\theta_1 + h_{j,2}\theta_2 + \cdots + h_{j,n}\theta_n \quad \text{for } h_{i,j} \in \mathbb{Q}$$

similarly

$$\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n \quad \text{for } k_{i,j} \in \mathbb{Q}$$

$$\Rightarrow (\alpha+\beta)\theta_j = (h_{j,1}+k_{j,1})\theta_1 + \cdots + (h_{j,n}+k_{j,n})\theta_n$$

for $h_{j,i} + k_{j,i} \in \mathbb{Q}$

$\Rightarrow \alpha+\beta \in \bar{\mathbb{Q}}$ (∵ above)

similarly,

$$\alpha\beta\theta_j = \alpha^{s+1}\beta^{t+1} = \begin{cases} \text{some } \theta_k \text{ ; } s+1 \le m-1,\ t+1 \le r-1 \\ (-a_1\alpha^{m-1} \cdots - a_m)\beta^{t+1};\ t+1 \le r-1,\ s+1 = m \\ (\alpha^{s+1})(-b_1\beta^{r-1} \cdots - b_r);\ t+1 = r,\ s+1 \le m-1 \\ (-a_1\alpha^{m-1} \cdots - a_m)(-b_1\beta^{r-1} \cdots - b_r);\ t+1 = r,\ s+1 = m \end{cases}$$

in every case

$$\alpha\beta\theta_j = c_{j,1}\theta_1 + c_{j,2}\theta_2 + \cdots c_{j,n}\theta_n \text{ ; } c_{i,j} \in \mathbb{Q}$$

$\Rightarrow \alpha\beta \in \bar{\mathbb{Q}}$

now as $\alpha^m + a_1\alpha^{m-1} + \cdots a_m = 0$

$$1 + \frac{a_1}{\alpha} + \frac{a_2}{\alpha^2} + \cdots + \frac{a_m}{\alpha^m} = 0$$

$\Rightarrow \frac{1}{\alpha} \in \bar{\mathbb{Q}}$ as if $a_m = 0$ then we take a_{m-1}, or so on all cant be equal to 0 as $1 \neq 0$

Exe: Show that $\bar{\mathbb{Q}}$ is countable

Ans:

now let $a_1, a_2, \ldots a_m \in \mathbb{Q}$

$$A_{a_1,a_2,\ldots a_m} = \{ q \in \bar{\mathbb{Q}} \mid q \text{ is root of } x^m + a_1x^{m-1} + \cdots a_m = 0 \}$$

then $A_{a_1,a_2,\ldots a_m}$ is finite as by fundamental theorm of algebra it will have m roots in $\mathbb{C}$

$|A_{a_1,a_2,\ldots a_m}| = m$

now for fixed m, let

$$A_m = \bigcup_{a_1,a_2,\ldots a_m \in \mathbb{Q}} A_{a_1,a_2,\ldots a_m}$$ then this is countable union of finite sets

as $|\mathbb{N}| = |\underbrace{\mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}}_{m \text{ times}}|$

so, $|A_m| = |\mathbb{N}|$ or A_m is countable $\forall$ m

now, $\bar{\mathbb{Q}} = \bigcup_{m=1}^{\infty} A_m$ ← countable union of countable sets is countable

$\Rightarrow \bar{\mathbb{Q}}$ is countable

27th Jan :

Quiz-1 : 3 to 4 pm 4th Feb

Defn : $M|_K$ field extension, $\alpha \in M$ is algebraic over K if $\exists\, f(t) \neq 0 \in K[t]$ s.t $f(\alpha)=0$

Note : Above $\exists$ unique K-alg homomorphism

$$\varphi_\alpha : K[t] \longrightarrow M$$

$\ker(\varphi_\alpha) \neq 0$ iff α is algebraic
$\ker(\varphi_\alpha) = 0$ iff α is not algebraic

$\varphi_\alpha|_K = id$, $\varphi_\alpha(t)=\alpha$ and $\ker(\varphi_\alpha) \neq 0$ iff α is alg over K

Defn : if $\alpha \in M$ is not algebraic over K, then α is transcendental over K

we had defined $\overline{\mathbb{Q}}$ = algebraic numbers s.t $\forall \alpha \in \overline{\mathbb{Q}}\ \exists\, f \in \mathbb{Q}[t]$ s.t $f(\alpha)=0$

i.e $\alpha \in \mathbb{C}$ is algebraic number iff α is algebraic number over $\mathbb{Q}$

Eg: $\sqrt{2}$ is algebraic / $\mathbb{Q}$

π is transcendental / $\mathbb{Q}$

$\mathbb{C}/\mathbb{R}$ $\pi \in \mathbb{C}$ is algebraic $/\mathbb{R}$ as $f(t) = t - \pi \in \mathbb{R}[t]$, $f(\pi)=0$

similarly π is algebraic / $\mathbb{Q}(\pi)$, $t-\pi \in \mathbb{Q}(\pi)[t]$

π is algebraic / $\mathbb{Q}(\pi^5)$

$\mathbb{Q}(\pi^5) \subset \mathbb{Q}(\pi)$

$t^5 - \pi^5 \in \mathbb{Q}(\pi^5)[t]$

now, $K(t)|_K$ $t \in K(t)$ is not algebraic over K, as if t is algebraic over K

$\Rightarrow \exists\, 0 \neq f(x) \in K[x]$ s.t $f(t)=0$

$\Rightarrow f(t)=0 \Leftrightarrow f(x) \equiv 0$ (contradiction)

$\Rightarrow t$ is transcendental over K

Defn : $M|_K$ field extension, $\alpha \in M$: algebraic over K if $f(t) \neq 0 \in K[t]$ s.t $f(\alpha)=0$ then $f(t)$ = annihilating polynomial of α over K

$\varphi : K[t] \longrightarrow M$ $\quad \varphi|_K = id$, $\varphi(t)=\alpha$ (α is algebraic/K)

$\ker(\varphi) = \langle m(t) \rangle$ $\quad m(t) \neq 0$
($\because$ polynomial over fields are PIDs)

$\Rightarrow \frac{K[t]}{\langle m(t) \rangle} \cong im(\varphi)$; subring of M

$\frac{K[t]}{\langle m(t) \rangle}$ domain ($\because im(\varphi)$ is domain) $\Rightarrow \langle m(t) \rangle$ is prime ideal = maximal ideal ($\because K[t]$ is PID)

$\Rightarrow \frac{K[t]}{\langle m(t) \rangle}$ is field $\cong im(\varphi) = K[\alpha]$

$\Rightarrow m(t)$ is irreducible polynomial in $K[t]$

so, $\frac{K[t]}{\langle m(t) \rangle} \cong K[\alpha] \subset M$ (field)

so, $K(\alpha)=K[\alpha]$ ($\because K(\alpha)$ = smallest field of $K\cup\{\alpha\}$ in M)

now M/K is field extension, if α is algebraic/K then

$K[\alpha]$ is a field and
$K(\alpha)=K[\alpha]\cong \frac{K[t]}{\langle m(t)\rangle}$ where $\langle m(t)\rangle=\ker\varphi$
$m(t)\neq 0$, irreducible

$\varphi: K[t]\longrightarrow M$ $\quad\varphi$ is unique
$\varphi|_K=id$ $\quad\varphi(t)=\alpha$

Note: we can assume that $m(t)$ is monic and irreducible, then $m(t)$ becomes unique such monic and irreducible polynomial in $K[t]$ s.t $m(\alpha)=0$

Exe: show that $m(t)$ is unique, i.e if $\exists\, m'(t)$ s.t m' is monic and irreducible, then $m'(t)=m(t)$ → done down

Defn: $m(t)$ is minimal polynomial of α over K

Exe: $m(t)$ is monic polynomial in $K[t]$ then following are equivalent (FAE)
① $m(\alpha)=0$, m is irreducible → done down
② m is minimal polynomial of α over K
③ if $f(t)\in K[t]$ s.t $f(\alpha)=0$ then $m(t)\mid f(t)$ in $K[t]$

now if M/K, $a\in M$ transcendental/K, $\varphi: K[t]\longrightarrow M$ $\quad\varphi|_K=id$, $\varphi(t)=\alpha$
$\ker\varphi=0$
$K[t]\cong \text{im}(\varphi)=K[\alpha]$
↖ image not a field

Eg: ① $\alpha=\sqrt[4]{2}$ algebraic/$\mathbb{Q}$

$\min(\alpha)=t^4-2$ $\quad K=\mathbb{Q}$

② $\min(\alpha)=t^2-\sqrt{2}$ is minimal polynomial over $\mathbb{Q}$

$K=\mathbb{Q}(\sqrt{2})$

③ $\min(\alpha)=t^4-2$
$\mathbb{Q}(\sqrt{3})$ ↑ $K=\mathbb{Q}(\sqrt{3})$
monic and irreducible over $\mathbb{Q}(\sqrt{3})$

Exe: show that t^4-2 is irreducible in $\mathbb{Q}(\sqrt{3})[t]$

Ans:
$\varphi: \mathbb{Q}(\sqrt{3})[t]\longrightarrow \mathbb{C}$

$\varphi|_{\mathbb{Q}(\sqrt{3})}=id$ $\quad\varphi(t)=\sqrt[4]{2}$

$\ker(\varphi)\ni t^4-2$
↑
$\ker(\varphi)=\langle m(t)\rangle$ irreducible factor of t^4-2 is minimal
then
$m(t)\mid t^4-2$ in $\mathbb{Q}(\sqrt{3})[t]$

$\Rightarrow m(t)\mid (t-\alpha)(t+\alpha)(t-i\alpha)(t+i\alpha)$
then combination of 2 or 3 of them is not a polynomial over $\mathbb{Q}(\sqrt{3})$

as $t^2-\alpha^2$ not in $\mathbb{Q}(\sqrt{3})[t]$

$(t-\alpha)(t-i\alpha)$ on i, so not in $\mathbb{Q}(\sqrt{3})[t]$

$(t-i\alpha)(t+i\alpha) = t^2+\alpha^2$ not in $\mathbb{Q}(\sqrt{3})[t]$

now combination of 3 will have i, if not

then $(t-\alpha)(t^2+\alpha^2) = t^3+t\alpha^2-t^2\alpha-\alpha^3$ not in $\mathbb{Q}(\sqrt{3})[t]$

or $(t+\alpha)(t^2+\alpha^2)$

$= t^3+t\alpha^2+\alpha t^2+\alpha^3$ not in $\mathbb{Q}(\sqrt{3})[t]$

so, $m(t) = t^4-2$, and from above proof, we get

$m(t)$ is minimal

eg: $e^{2\pi i/p} = \alpha$ is prime p then α is algebraic as

$(t^p-1)(\alpha) = 0$

$t^p-1 = (t-1)(1+t+\cdots+t^{p-1}) \Rightarrow$ minimal polynomial is $f(t)$

$\alpha-1 \neq 0$ $\quad$ $f(t)$ is irred

exe: $f(t)$ is irreducible iff $f(t+1)$ is irreducible

Ans:

As $f(t) \in \mathbb{Q}[t]$ then trivially $\varphi(f+g) = f(t+1)+g(t+1)$, $\varphi(f\cdot g) = f(t+1)\,g(t+1)$

$\varphi: \mathbb{Q}[t] \longrightarrow \mathbb{Q}[t]$, $p \to 0$, $1 \to 1$

$t \longmapsto t+1$ and onto, one-one trivial

$\varphi|_{\mathbb{Q}} = Id$, we have seen that φ is an automorphism

so, $f(t)$ irred iff $f(t+1)$ irreducible

$f(t)$ reducible iff $f(t+1)$ is reducible

exe: show that above $f(t)$ is irreducible in $\mathbb{Q}[t]$ → done down

now, we have given $f(t) \in K[t]$, we want to find field extension M/K s.t $\exists \alpha \in M$ $f(\alpha) = 0$ (deg $f \geq 1$)

exe: $f(t) \in \mathbb{Q}[t]$ $f(t)$ has root α in $\mathbb{C}$ take $M = \mathbb{C}$

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

eg: let $f(t) \in K[t]$, we may assume that $f(t)$ is irreducible as if not then $f = f_1 \cdots f_r$ (irreducible) let $f = f_1$ for $f_1(\alpha) = 0$

also we may assume f is monic

from above example we have $f(t) \in K[t]$ monic, irreducible we want to find M s.t M/K and M has root of $f(t)$

assume, M/K is found, and $\exists \alpha \in M$ s.t $f(\alpha) = 0$

$\Leftrightarrow f(t)$ is the minimal polynomial of α

so, $\frac{K[t]}{\langle f(t)\rangle} \cong K[\alpha] \subset M$ so let $M = \frac{K[t]}{\langle f(t)\rangle}$ field $\bar{t} = \alpha$

↑ field

↑ image of t

$\varphi(t) = \alpha$

Eg: $f(t)=t^3-2 \in \mathbb{Q}[t]$ (irreducible, monic) $f(t)$ has 3 roots

$M_1=\mathbb{Q}[\sqrt[3]{2}]$, $M_2=\mathbb{Q}[\omega\sqrt[3]{2}]$, $M_3=\mathbb{Q}[\omega^2\sqrt[3]{2}]$

$\frac{\mathbb{Q}[t]}{\langle t^3-2\rangle}=\mathbb{Q}[\alpha]$ $\quad \alpha=\underset{\alpha_1}{\sqrt[3]{2}}, \underset{\alpha_2}{\omega\sqrt[3]{2}}, \underset{\alpha_3}{\omega^2\sqrt[3]{2}}$

$\mathbb{Q}[\alpha] \cong M_i \quad i=1,2,3$

$\varphi: \mathbb{Q}[t] \longrightarrow \mathbb{Q}[\sqrt[3]{2}]$

$t \longmapsto \sqrt[3]{2}$

$\varphi|_{\mathbb{Q}}=id \quad \ker(\varphi)=\langle t^3-2\rangle$

$\Rightarrow \frac{\mathbb{Q}[t]}{\langle t^3-2\rangle} \cong \mathbb{Q}[\sqrt[3]{2}]$

$\mathbb{Q}[t] \xrightarrow{\varphi} \mathbb{Q}[\sqrt[3]{2}] \hookrightarrow \mathbb{Q}[\alpha_1]$

$\pi: \mathbb{Q}[t] \to \frac{\mathbb{Q}[t]}{\langle t^3-2\rangle}$

$\Rightarrow \frac{\mathbb{Q}[t]}{\langle t^3-2\rangle} \cong M_1 \cong M_2 \cong M_3$

Note: Above $\alpha_1, \alpha_2, \alpha_3$ conjugate over $\mathbb{Q}$ as all three roots together

Def: $M|K$, $M'|K$ field exist K-homomorphism $\varphi: M \to M'$ is a ring homomorphism with $\varphi|_K=id$

Exe: $M|K$, $M'|K$, $\varphi: M \to M'$ is K-homomorphism

(i) let, $\alpha \in M$: algebraic over K
$f(t)=\min_{K} \alpha \in K[t]$ ← minimal polynomial
then $\varphi(\alpha)$: algebraic over K and $\min_K \varphi(\alpha)=f(t)$ → above down

(ii) let, $\alpha \in M$: transcendental / K then $\varphi(\alpha)$ is transcendental over K

$\varphi(f(t))=\varphi(t^n+a_1t^{n-1}+\dots+a_n)=t^n+\varphi(a_1)t^{n-1}+\dots+\varphi(a_n)$
$=f(t)$ as $\varphi|_K=id$

Exe: $\varphi, \psi: M \to M'$ K-homomorphism, let $M=K(X)$, $X \subset M$ subset
↑ subfield of $M|K$ generated by X

if $\varphi(x)=\psi(x) \ \forall\, x \in X$ → above down
then $\varphi=\psi$

Theorem: $M|K$, $\alpha \in M$ transcendental over K then $K(\alpha) \cong K(t)$

proof: $K[t] \xrightarrow{\varphi} M$, $\varphi|_K=id$, $\varphi(t)=\alpha$ is injective as $\ker(\varphi)=0$

so, $f(t) \neq 0 \Rightarrow f(\alpha) \neq 0$

$K[t] \xrightarrow{\varphi} M \xrightarrow{f(\alpha)/g(\alpha)} \tilde{\varphi}$ as $g(\alpha) \neq 0$ α is transcendental

$K[t] \to K(t) \xrightarrow{f(t)/g(t)}$

$\tilde{\varphi}$ is also injective, so $K(t) \cong img(\tilde{\varphi}) = K(\alpha)$ (← $\ker(\tilde{\varphi}) = 0$ as $f(\alpha) \neq 0$)

now if α: radical/K, then $K(\alpha) \cong K(t)$

now, $\alpha \in \mathbb{C}$: algebraic number $\quad \mathbb{Q}[\alpha] \cong \mathbb{Q}(\alpha)$

$$\varphi \left(\frac{\mathbb{Q}[t]}{\langle m(t) \rangle} \right) \quad m(t) = \min_{\mathbb{Q}} \alpha$$

$\deg m(t) = n$, $\mathbb{Q}[\alpha] = \{ a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1} \; ; a_i \in \mathbb{Q} \}$

if α^n then we just substitute with $m(\alpha) = 0$, $\alpha^n + t_1\alpha^{n-1} + \cdots t_n = 0$

now if $\beta = a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1} \neq 0 \in \mathbb{Q}[\alpha]$

then for β^{-1}: $g(t) = a_0 + a_1 t + \cdots a_{n-1} t^{n-1}$

$\varphi(g(t)) = \beta$

$\gcd(m(t), g(t)) = 1$ ($\because m(t)$ is irred and $\deg g < \deg m$)

$\Rightarrow 1 = f_1(t) m(t) + f_2(t) g(t)$ ($\because$ division algorithm)

then $\varphi(1) = 1$

$\varphi(f_1(t)\, m(t)) = 0$

$1 = \varphi(f_2(t))\, \varphi(g(t))$

$1 = f_2(\alpha) g(\alpha) \Rightarrow 1 = f_2(\alpha)\beta$

$\Rightarrow \beta^{-1} = f_2(\alpha)$

Exe: now that $m(t)$ is unique, i.e if $\exists\, m'(t)$ s.t m' is monic and irreducible, then $m'(t) = m(t)$

Ans: Let $m(t)$ be minimal polynomial for $\alpha \in M$

$\varphi : K[t] \longrightarrow M$ s.t $\varphi|_K = id$ $\quad \varphi(t) = \alpha$

$\ker \varphi = \langle m(t) \rangle$

now if $\exists\, m'(t)$ s.t

$\ker \varphi = \langle m'(t) \rangle$ then $\langle m'(t) \rangle = \langle m(t) \rangle$

$\Rightarrow \exists\, \alpha \in K[t]$ $\; m'(t) = \alpha(t)\, m(t)$

but as m' is irreducible ($\because$ (does proof))

$\Rightarrow \alpha(t) = \alpha \in K$

but as m', m monic

$\Rightarrow \alpha = 1$

$\Rightarrow m(t) = m'(t)$

Exe: $m(t)$ is monic polynomial in $K[t]$ then following are equivalent (FAE)

① $m(\alpha)=0$, m is irreducible
② m is minimal polynomial of α over K
③ If $f(t)\in K[t]$ s.t $f(\alpha)=0$ then $m(t)\mid f(t)$ in $K[t]$

Ans:

② ⇒ ① As $m(t)$ is minimal polynomial

$\ker(\varphi)=\langle m(t)\rangle$

$\Rightarrow \frac{K[t]}{\langle m(t)\rangle} \cong \text{img}(\varphi)$ ↑ domain

$\Rightarrow \frac{K[t]}{\langle m(t)\rangle}$ is domain

$\Rightarrow \langle m(t)\rangle$ is prime

$\Rightarrow \langle m(t)\rangle$ is maximal

$\Rightarrow m(t)$ is irreducible ($\because K[t]$ is PID)

also as $\forall f\in\ker(\varphi)$, $f(\alpha)=0 \Rightarrow m(\alpha)=0$

① ⇒ ② if m is irreducible and $m(\alpha)=0$

$\Rightarrow m\in\ker(\varphi)$

but as $\langle m(t)\rangle$ is maximal and $\langle m(t)\rangle \subseteq \ker\varphi$

$\Rightarrow \ker(\varphi)=\langle m(t)\rangle$

so, $m(t)$ is minimal polynomial when we make it monic

② ⇒ ③ as $m(t)$ is minimal polynomial, $\ker(\varphi)=\langle m(t)\rangle$

$\varphi: K[t]\longrightarrow M$
$\varphi|_K = id$ $\varphi(t)=\alpha$

then
$f(t)\in K[t]$ s.t $f(\alpha)=0 \Rightarrow f(t)\in\ker(\varphi)=\langle m(t)\rangle$
$\Rightarrow \exists\, h(t)\in K[t]$ s.t
$h(t)m(t)=f(t)$
$\Rightarrow m(t)\mid f(t)$ in $K[t]$

③ ⇒ ② as $\forall f\in\ker(\varphi)$, $m\mid f$ ($\because f(\alpha)=0$ for $f(t)\in K[t]$)

$\Rightarrow \ker(\varphi)\subseteq\langle m(t)\rangle$
but $m\in\ker(\varphi)$
$\Rightarrow \langle m(t)\rangle\subseteq\ker(\varphi)$
$\Rightarrow \langle m(t)\rangle=\ker(\varphi)$

Exe: Show that above $f(t)$ is irreducible in $\mathbb{Q}[t]$

Ans: as $f(t)$ irred iff $f(t+1)$ irred

$$f(t+1)=\frac{(x+1)^p-1}{(x+1)-1}=\frac{\sum_{i=0}^{p}\binom{p}{i}(x)^i-1}{x}=\frac{\sum_{i=1}^{p}\binom{p}{i}x^i}{x}=\sum_{i=1}^{p}\binom{p}{i}x^{i-1}$$

$$=x^{p-1}+\cdots+\binom{p}{p-2}x+p$$

then by eulines criteria, $p \nmid a_{p-1}$, $p \mid a_i$ $i = p-2, p-3, \ldots 0$
& $p \nmid a_0 = p$

so, $f(t+1)$ is irreducible
$\Rightarrow f(t)$ is irreducible

Exe: $M|K$, $M'|K$, $\varphi: M \to M'$ is K-homomorphism

(i) let, $\alpha \in M$: algebric over K
$f(t) = \min_K \alpha \in K[t]$ ← minimal polynomial
then $\varphi(\alpha)$: algebric over K and $\min_K \varphi(\alpha) = f(t)$

(ii) let, $\alpha \in M$: transidental / K then $\varphi(\alpha)$ is transidental over K

Ans:

(i) $\varphi: M \to M'$ s.t $\varphi|_K = id$

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

$\alpha \in M$, algebric over K $f(t) = \min_K \alpha \in K[t]$

as $\exists f \in K[t]$ s.t $f(\alpha) = 0$
then $\varphi(f(\alpha)) = 0$
$\Rightarrow f(\varphi(\alpha)) = 0$

or $\exists f \in K[t]$
s.t $\varphi(\alpha) \in M'$ $f(\varphi(\alpha)) = 0$
$\Rightarrow \varphi(\alpha)$ is algebric over K

now, minimal polynomial of $\varphi(\alpha)$

let $K[t] \xrightarrow{\psi} M \xrightarrow{\varphi} M'$
$t \mapsto \alpha$

now $\varphi \circ \psi|_K = id$ as $\psi|_K = id$
$\varphi|_K = id$
← unique

and $\varphi \circ \psi(t) = \varphi(\alpha) \in M'$

then $\ker(\varphi \circ \psi) = \langle m(t) \rangle$
↑ minimal polynomial of $\varphi(\alpha) \in M'$

but as M, M' is field
$\ker(\varphi) = 0$

$f \in \ker \varphi \circ \psi \Leftrightarrow f \in \ker(\psi)$

$\Rightarrow \ker \varphi \circ \psi = \langle f(t) \rangle$
as $f(t)$ is unique (∵ done above)

$\Rightarrow f(t)$ is $\min_K(\varphi(\alpha))$

(ii) now if α is transcendental, i.e $\deg \psi = 0 \Rightarrow \deg(\varphi \circ \psi) = 0$

$\Rightarrow \varphi(\alpha)$ is transcendental (unique)

Exe: $\varphi, \psi : M \to M'$ K-homomorphism, let $M = K(X)$, $X \subset M$ subset (↑ subfield of $M|_K$ generated by X)

if $\varphi(x) = \psi(x)\ \forall\ x \in X$

then $\varphi = \psi$

Ans: $M = K(X)$

$\psi, \varphi : M \to M'$ K-homomorphism

$\varphi|_K = id$ i.e $\psi|_K = id$

$$K(X) = \left\{ \frac{f(x)}{g(y)} \ \forall\ x, y \in X,\ f(t), g(t) \in K[t],\ g(y) \neq 0 \right\}$$

then

$\varphi(x) = \psi(x)\ \forall\ x \in X$

$\varphi(f(x)) = f(\varphi(x))$ ($\because$ similar to above)

$= f(\psi(x)) = \psi(f(x))$

$\Rightarrow \varphi\left(\frac{f(x)}{g(y)}\right) = \varphi(f(x))(\varphi(g(y)))^{-1}$

$= \psi(f(x))(\psi(g(y)))^{-1}$

$= \psi\left(\frac{f(x)}{g(y)}\right)$

So, $\varphi = \psi$ as $\varphi(t) = \psi(t)\ \forall\ t \in M$