MA419
LC001

tputhen@gmail.com
106-F math department

2 quizes	10% x 2
midsem	30%
endsem	50%

29th July :

Algebra : Performing operations
Studying action of operations of objects
study of Equations ← that's it

$ax+b=0 \quad a\neq 0$
$x=-\frac{b}{a}$

cubic ✓ (degree = 3)
quatic ✓ (degree = 4)

$ax^2+bx+c=0 \quad a\neq 0$

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

degree 5
galva: degree 5 sol (genral Eq) does not Exist

see

field automorphisms

$\sigma : \mathbb{C} \to \mathbb{C}$
σ is bijective
$\sigma(x+y)=\sigma(x)+\sigma(y)$
$\sigma(xy)=\sigma(x)\sigma(y)$
$\sigma(0)=0$
$\sigma(1)=1$

show: $\sigma(a)=a$
$\forall a \in \mathbb{Q}$

$f(x)=a_n x^n + a_{n-1}x^{n-1} + \dots a_0$
$a_n \neq 0$ as $\sigma(a_n)=a_n$
$a_i \in \mathbb{Q}$
$=(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$
$\alpha_i \in \mathbb{C}$
$R(f)=\{\alpha_1,\alpha_2,\dots\alpha_n\}$

$G(f)=\left\{\hat{\sigma} \;\middle|\; \begin{array}{l}\hat{\sigma}: R(f)\to R(f) \\ \sigma \text{ field automorp}\end{array}\right\}$

$1 \in G(f)$
σ, τ field aut.
$\tau\circ\sigma$ field aut.

$\widehat{\tau\circ\sigma} = \hat{\tau}\circ\hat{\sigma}$

now, $\sigma(f(x)) = a_n\sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + \dots a_0$

$\hat{\sigma} : R(f) \to R(f)$
$(x^2+1)=(x+i)(x-i)$
$\sigma(z)=\bar{z}$

Hat operation:
$\hat{\sigma} : x \to \sigma(x)$
$\hat{\sigma} : R(f) \to R(f)$

$a\neq 0 \quad ax^3+bx^2+cx+d$

$|G(f)| = \begin{cases} 3 \\ 6 \end{cases}$

field automorphism :
$\sigma : F \to F$
bijective map that preserves all algebric property.

$\sigma(x+y)=\sigma(x)+\sigma(y)$
$\sigma(xy)=\sigma(x)\sigma(y)$
$\sigma(0)=0$
$\sigma(1)=1$ ← field
$\sigma : \mathbb{C} \to \mathbb{C}$

now for $a \in \mathbb{Q}$ $a = p/q$ where $p,q \in \mathbb{Z}$ and $\gcd(p,q)=1$

as $\sigma(p/q) = \sigma(p)\cdot\sigma\left(\frac{1}{q}\right)$
$=(p)\,\sigma\left(\frac{1}{q}\right) = \frac{p}{q}$

proof of :
$\sigma\left(\frac{1}{q}\right)=\frac{1}{q}$

$\sigma(1)=1$
$\sigma\left(\frac{p}{q}\cdot\frac{q}{p}\right)=1$
$1=\sigma\left(\frac{p}{q}\right)\cdot\sigma\left(\frac{q}{p}\right)$
$1=pq\,\sigma\left(\frac{1}{q}\right)\sigma\left(\frac{1}{p}\right)$
$\frac{1}{pq}=\sigma\left(\frac{1}{q}\right)\sigma\left(\frac{1}{p}\right)$
for $p=1$
$\frac{1}{q}=\sigma\left(\frac{1}{q}\right)$

S_n is basically group that contains all permutation if n is in $\mathbb{N}$ (finite)

see S_n ↑ Symmetry group

Example: $A = \{1, 2, \ldots\ldots n\}$

$G = S_n = \{ f : A \to A \mid f \text{ is bijective function} \}$

(most imp. example)

(every finite group is a <u>subgroup</u> of S_n)

<u>group</u>: <u>Defn</u>: G is a group if $G \neq \phi$,

↓ see: three properts. $G \times G \to G$

Abelian group ⇒ $ab = ba \ \forall a, b \in G$

(i) $a.(b.c) = (a.b).c$ assosiativity

(ii) $\exists e \in G$ st $ae = ea = a \ \forall a \in G$ identity

(iii) for $a \in G$, $\exists b \in G$ st $a.b = e = b.a$

$b = a^{-1}$ inverse

see: $H \leq G$ if $H \neq \phi$, $e \in H$, $a, b \in H$

$\Rightarrow a^{-1}, b^{-1}, a.b \in H$ (closed)

<u>subgroup</u>: $H \leq G$ if i) $H \neq \phi$

ii) $e \in H$

iii) $a, b \in H \Rightarrow a.b \in H$

$a^{-1}, b^{-1} \in H$

<u>denotion</u>: $H \leq G$

see examples

↑ and proofs

<u>group homomorphism</u>: G, G' groups $\phi : G \to G'$ function

ϕ is a group homomorphism

if i) $\phi(e_G) = e_{G'}$

ii) $\phi(xy) = \phi(x)\phi(y)$

$\Rightarrow \phi(x^{-1}) = \phi(x)^{-1}$

$\phi : G \to G'$

↓

group homomorphism if

① $\phi(e_g) = e_{g'}$

② $\phi(xy) = \phi(x)\phi(y) \Rightarrow \phi(x^{-1}) = \phi(x)^{-1}$

↷ finite group

<u>Theorm</u>: let G be a finite group

(cayley's theorm) then $\exists \phi : G \to S_n$

ϕ is group homomorphism

ϕ is one-one

(Every group is isomorphic to a group of permutations)

Note: $A = G = \{e = a_1, a_2, \ldots a_n\}$

$|G| = n$

$\phi : G \to S_n$

when $S_n = \{ f : A \to A \mid f \text{ is bijection} \}$

<u>proof</u>:

to prove:

let G be a given group $\exists \phi : G \to S_G$

$\forall a \in G$ we define $f_a : G \to G$

$f_a(x) = ax \ \forall x \in G$

now, $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ ∴ one-one

also, let b be any element in G

then

$x = a^{-1}b$ is in G

$f_a(x) = ax = \cancel{a}(\cancel{a^{-1}}b) = b$

so $\forall b \in G$ there is an $x = a^{-1}b$ s.t

$f_a(x) = b$ ∴ <u>onto</u>

now, f_a is a permutation on set of elements of G

$$G' = \{ f_a \mid a \in G \} = S_G$$

$\downarrow$

groups of permutation

now is G' a group:

① for $\forall f_a, f_b \in G'$

$$f_a f_b(x) = f_a(f_b(x)) = f_a(bx)$$
$$= a(bx)$$
$$= (ab)x$$
$$= f_{ab}(x)$$

as $f_{ab} \in G'$
closed

② $f_e(x) = e.x = x$

$$f_e = I_G$$

$$f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$$

now ϕ is group homomorphism:

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

let $\phi(a) = f_a$
onto as for $x = a^{-1}b$
one-one (proved) } one-one + onto }

$\phi(a)\phi(b) = f_a f_b = \phi(ab)$ ∴ <u>isomorphism</u> } Homomorphism

<u>Cyclic groups</u>: G is cyclic if $\exists\, a \in G$ s.t

$$G = \{ a^n \mid n \in \mathbb{Z} \}$$
$$a^0 = e$$
$$a^{-2} = (a^2)^{-1}$$

<u>Thm</u>: G is cyclic and infinite $\Rightarrow G \cong \mathbb{Z}$

<u>proof</u>: $G = \{ a^n \mid n \in \mathbb{Z} \}$

now $\psi : \mathbb{Z} \to G$
$n \to a^n$
s.t $\psi(n) = a^n$

now
$$\psi(n+m) = a^{n+m} = a^n . a^m$$
$$\psi(n+m) = \psi(n).\psi(m) \quad \therefore \text{Homomorphic}$$

now $G = \{ a^n \mid n \in \mathbb{Z} \}$, $\forall x \in G$
$\exists\, n \in \mathbb{Z}$ st $x = a^n$ so every

element is an image of atleast one elemt n in $\mathbb{Z}$

∴ surjective

now, one-one: let's suppose it does not happen, then

let $a^n = a^m$

$n > m$, $n \neq m$

$a^r = a^{n-m} = e$ (many one st)

$a^0 \nearrow$

$a^r \nearrow$

now, if $a^r = e$

$\{a^0, a^1, a^2, \dots a^{r-1}, e, a, a^2 \dots\}$

$= \{a^0, a^1, a^2, \dots a^{r-1}\}$

$|a| < \infty$ $\ast$

∴ φ is one-one

as φ is homomorphic and bijective

$\mathbb{Z} \cong G$

$n \geq 2$ $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots \overline{n-1}\}$

$\bar{i} = i \bmod n$

Thm: $n = |G| < \infty \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$

↳ cyclic

proof: let $\phi : \{0, 1, 2 \dots n-1\} \longrightarrow G = \langle a \rangle$

now $r \longrightarrow a^r$

$\phi(r) = a^r$

now, ϕ is homomorphic with $\mathbb{Z}/n\mathbb{Z}$ as:

$\phi(r+m) = a^{r+m} = \phi(r)\,\phi(m)$

also ϕ is one-one as:

if $\phi(r) = \phi(m)$

$a^r = a^m$

$a^{r-m} = a^0$ if $r > m$

and $= a^{kn}$

$r - m = kn$ $r = kn + m$

but as $r<n$ and $m<n$
$r = m$
as $kn+m>n$
$\forall k \geq 1$
$\Rightarrow k=0$
$\therefore \underline{r=m}$

also $|\mathbb{Z}/_n\mathbb{Z}| = n$
and $|G| = n$
so $\underline{\text{onto}}$.
$\therefore \mathbb{Z}/_n\mathbb{Z} \cong G$

Thm: (lagrang)

$H \leq G$ | $|G| < \infty$
$\Rightarrow |H| \,\big|\, |G|$

proof: $H = \{e=h_1, \ldots h_r\}$

now $|H| = r$
$|G| = n$

now $|H| = |G|$
or $|H| < |G|$

if $|H| = |G|$, done

$|H| < |G|$ then:
let
$g_i \in G \setminus H$

$g_2H = \{g_2h_1, g_2h_2, \ldots g_2h_r\}$

now, $g_2h_i = g_2h_j$
$\Rightarrow h_i = h_j$
(one-one)

and ① $|g_2H| = |H| = r$ (onto)

now, let $g_2H \cap H \neq \phi$

then $\exists$ an elemet s.t
$g_2h_i = h_j$
$g_2 = h_j h_i^{-1} \in H$

as $g_2 \in G \setminus H$

$g_2 = h_j h_i^{-1} \in H$ ⨳

so $g_2H \cap H = \phi$

now $H = \{e = h_1, h_2, \dots h_r\}$

$g_2 H = \{g_2 h_1, g_2 h_2, \dots g_2 h_r\}$

$G = H \sqcup g_2 H$

$|G| = 2r$

or $g_3 \in G \setminus H_1 \sqcup H g_2$

$g_3 H = \{g_3 h_1, \dots g_3 h_r\}$

$G = Hg_1 \sqcup Hg_2 \cup \dots Hg_m$

$|G| = mr$

$r = |H| \mid |G|$

some more properties :

$a \overset{H \leq G}{\sim} b$ if $b = ah$ for some $h \in H$

reflexive as $a = a(e)$

symmetric $b = ah$

and

then $a = bh^{-1}$

so $b \sim a$

transitive: $a = bh$

$b = ch$

then $a = ch^2$

$h^2 \in H$

$a \sim b$, $b \sim c$

$\Rightarrow a \sim c$

Cosets : $[g_\alpha]$ is called a coset of

H in G $[g_\alpha] = g_\alpha H$

$= \{g_\alpha h \mid h \in G\}$

$g_\alpha h \sim g_\alpha$

$g_\alpha H \subseteq [g_\alpha]$

if $g' \in [g_\alpha]$ $g' = g_\alpha h$

Note : $G/\Omega = \{[g_\alpha] \mid g \in G\}_{\alpha \in \Omega}$

second proof: $G = g_1 H \sqcup g_2 H \sqcup \dots g_r H$

$H \longrightarrow g_P H$

$h \rightarrow g_i h$

$|g_iH| = |H| = s$

$|G| = rs = r|H|$

Note: $Hg = \{hg \mid h \in H\}$

$G = \bigsqcup_{\alpha \in \Lambda} Hg_\alpha$

↑

left

if $\psi : \ell_H G \rightarrow G R H$ ← left

$\psi(gH) = Hg^{-1}$

3rd Aug : cosets : $H \leq G$

$gH = \{gh \mid h \in H\}$ left cosets

$Hg = \{hg \mid h \in H\}$ right cosel

eg: H be subgroup of $\mathbb{Z}/6\mathbb{Z}$

$H \leq \mathbb{Z}/6\mathbb{Z}$

$H = \{ 0, 3 \}$

so $0 + H = 3 + H = H$

$1 + H = 4 + H = \{1, 4\}$

$2 + H = 5 + H = \{2, 5\}$

Note : $H \leq G$ and $g_1, g_2 \in G$

$$g_1H = g_2H \Leftrightarrow Hg_1^{-1} = Hg_2^{-1}$$

$$\Updownarrow$$

$$g_1H \subset g_2H$$

$$\Updownarrow$$

$$g_2 \in g_1H$$

$$\Updownarrow$$

$$g_1^{-1}g_2 \in H$$

Theorm : let H be a subgroup of a group G. The numbes of left cosets of H in G is same as number of right cosets in H in G.

proof :

$L_H = \{gH \mid g \in G\}$

$R_H = \{Hg \mid g \in G\}$ now, let $\phi : L_H \rightarrow R_H$

$\phi(gH) = Hg^{-1}$

now for ϕ to be bijetive :

if $g_1H = g_2H$

then $\Rightarrow g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$

$\Rightarrow g_1 = g_2h_2h_1^{-1}$

as $h_2 \in H$

and $h_1^{-1} \in H$

$h_2h_1^{-1} \in H$

$\Rightarrow g_1 = g_2 h_3$

now $g_2^{-1} g_1 = h_3$

$\Rightarrow g_2^{-1} = h_3 g_1^{-1}$

$\Rightarrow g_2^{-1} \in Hg_1^{-1}$

similary $g_1^{-1} \in Hg_2^{-1}$

so $g_1H = g_2H$

$\Rightarrow Hg_1^{-1} = Hg_2^{-1}$ (opposite is also true) as $\phi(g_1H) = Hg_1^{-1}$

$\phi(g_2H) = Hg_2^{-1}$

$\phi(g_1H) = \phi(g_2H)$

$\Rightarrow Hg_1^{-1} = Hg_2^{-1}$

$\Rightarrow g_1H = g_2H$

$\therefore$ one-one

also for g^{-1} $\phi(g^{-1}H) = Hg \quad \forall g \in G$

$\therefore$ onto

So ϕ is bijective

$\therefore |L_H| = |R_H|$

group : $- \; a.(b.c) = (a.b).c$

$\exists e$ s.t $ae = ea = a \quad \forall a \in G$

$a \in G, \exists b \in G \quad ab = ba = e$

$b = a^{-1}$

subgroups : $1_G \in H$

$a, b \in H \Rightarrow ab \in H$

$a \in H \Rightarrow a^{-1} \in H$

permutation group : $[n] = \{1, 2, \ldots n\}$

$$S_n = \{ f : [n] \to [n] \mid f \text{ is bijective} \}$$

permutation group on n letters

$$\begin{Bmatrix} 1 \\ 2 \\ \vdots \\ n \end{Bmatrix} \to \begin{Bmatrix} 1 \\ 2 \\ \vdots \\ n \end{Bmatrix} \qquad |S_n| = n(n-1) \cdots 1 = n!$$

$S_n \leftarrow$ symmetric group

notations :

one-line notation

$\pi = 231654$

i.e. $123456 \nearrow$

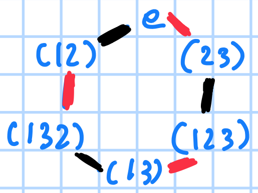
permutation diagram

cycle notation

$\pi = (123)(46)$

Eg : $\{123, 132, 213, 231, 321, 312\}$

$e \quad (23) \quad (12) \quad (132) \quad (13) \quad (123)$



$S_3 = \langle (1,2), (2,3) \rangle$

Group homomorphism :

$$f : G \to H$$
$$f(e_G) = e_H$$
$$f(xy) = f(x)f(y)$$
$$f(xx^{-1}) = f(e_g) = e_H$$
$$\shortparallel$$
$$f(x)f(x^{-1}) = e_H$$
$$\text{so} \quad f(x^{-1}) = (f(x))^{-1}$$

Note : if f is bijective, it is isomorphysm

Trivial homorphism :

$$\phi : G \to H \quad \phi(g) = e_H$$
$$\forall g \in G$$

Isomorphism : bijective homorphism

automorphism : isomorphism of group to itself.

Langrage's theorm : $|G| < \infty$

$H \leq G$

$|H| \mid |G|$

$a \sim b$

$a = bh \quad \exists\, h \in H$

gH coset

$G = g_1H \sqcup g_2H \cdots\cdots g_nH$

$|g_iH| = |H|$

$|G| = s|H|$

cor : p prime $|G| = p$

$\Rightarrow G$ is cyclic $(G \cong \mathbb{Z}/p\mathbb{Z})$

proof : let $H = \langle a \rangle$

$e \neq a \in G$

$H \leq G$

H is a subgroup

$|H| > 1 \quad \{e, a\} \subseteq H$

$a \in G$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq G$

$H \leq G$

$|H| \mid |G|$ but as $|G| = p$

$\Rightarrow |H| = 1$ or p

as $|H| > 1$

$\Rightarrow |H| = p$

$\langle a \rangle = H = G$

Note : order of a group G = size = $|G|$

order of elemt $g \in G = |g| := |\langle g \rangle|$

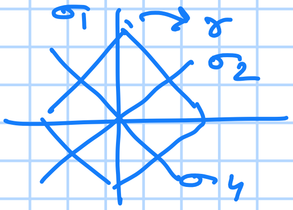
is either $k \geq 1$ s.t

$g^k = e$

or ∞ if no such k exist.

Dihedral groups – D_{2n} is a group of symmetries of a regular n-gon. order $= 2n$

eg D_8 = group of symmetries of square



$$\{\overbrace{1, r, r^2, r^3}^{\text{rotations}}, \underbrace{f, fr, fr^2, fr^3}_{\text{reflections}}\}$$

$$D_2n = \langle r, f \mid r^n = 1, f^2 = 1, rfr = f \rangle$$

Quaternion group : Q_8

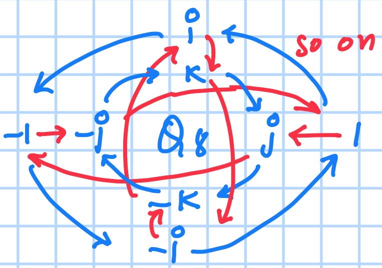
: 4th root of unity

$\{1, i, -i, j, -j, k, -k, -1\}$

$i^2 = j^2 = k^2 = -1$

$ij = k$

$ji = -k$



Matrix group :

$K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$ Note : $K = \mathbb{Z}/p\mathbb{Z}$ $GL_n(\mathbb{Z}/p\mathbb{Z})$

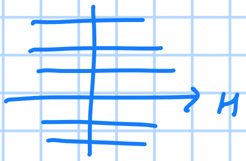
$GL_n(K) = \{A \mid A \text{ n×n matrix } |A| \neq 0\}$ $SL_n(\mathbb{Z}/p\mathbb{Z})$

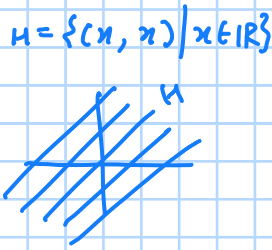
$SL_n(K) = \{A \mid A \in GL_n(K), \det A = 1\}$

Also : $(\mathbb{R}^n, +)$ $\bar{0} = (0 \dots 0)$

$\mathbb{R}^2$ $H = \{(a, 0) \mid a \in \mathbb{R}\}$

$(\alpha, \beta) + H = (\alpha + a, \beta)$





Heisenberg group :

$$H_3(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \; a, b, c \in F \right\}$$

$F = \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}/p\mathbb{Z} \dots$

$|H_3(\mathbb{Z}/p\mathbb{Z})| = p^3$

Alternating groups :

Set of even permutations in S_n is alternating group, denoted by A_n.

$K = \mathbb{R}$ $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ — ith $I = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \; 1 \end{pmatrix}$

$f : \{e_1, e_2 \dots e_n\} \longrightarrow \{e_1, \dots e_n\}$

$A(f) = [f(e_1), \dots \dots f(e_n)]$

$|A(f)| = \pm 1$

$A_n = \{\sigma \mid |\sigma| = 1\}$

$S_n = A_n \cup \sigma_1 A_n \cup \sigma_2 A_n \dots$

$\sigma_1, \sigma_2 \in A_n$

$|\sigma_1| = -1 = |\sigma_2|$

$|\sigma_2^{-1} \sigma_1| = -1 \cdot -1 = 1$

$\sigma_2 A_n = \sigma_1 A_n$

as $\sigma_i A_n = \sigma_1 A_n$

$S_n = A_n \cup \sigma_1 A_n$

$|S_n| = 2|A_n|$

$|A_n| = \frac{1}{2} n!$

Group multiplication : (Direct products)

$e_{G \times K} = (e_G, e_K)$

$(a,b)^{-1} = (a^{-1}, b^{-1})$

$(g_1, k_1) \cdot (g_2, k_2) = (g_1 g_2, k_1 k_2)$

$$A \times B = \{(a,b) \mid a \in A,\ b \in B\}$$

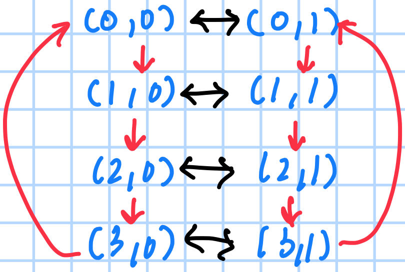
Defn: The direct product of group A and B is the set $A \times B$ and the group operation is done componet wise.

if $(a,b), (c,d) \in A \times B$
$(a,b) * (c,d) = (ac, bd)$
A and B are called factors

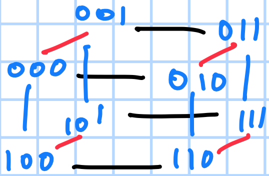
Eg: $D_8 \times \mathbb{Z}_4$

$(rf, 3) * (r^3, 1) = (rfr^3, 1+3)$
$= (r^2 f, 0)$

$\mathbb{Z}_4 \times \mathbb{Z}_2$



$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$



Note: sometimes direct product of cyclic group is cyclic $(\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6)$

Note: $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ iff $\gcd(n,m) = 1$

The fundamental theorem of finite abelian groups:

Every finite abelian group A is isomorphic to a direct product of cyclic groups

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \mathbb{Z}_{k_m} \quad \text{for } \forall\ k_i \in \mathbb{N}$$

* $k_i = p_i^{d_i}$ for p_i prime $d_i \in \mathbb{N}$ (prime powers)
* k_i is a multiple of k_{i+1} (elementary divisors)

$|A| = 200$
$A \cong \mathbb{Z}_{200}$
$A \cong \mathbb{Z}_{100} \times \mathbb{Z}_2$
$\vdots$

$A \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2}$
$\vdots$

Kernals: $\phi : G \to H$
Homomorphism

A kernal of a homomorphism $\phi : G \to H$ is the set
$\ker(\phi) := \phi^{-1}(e_H) = \{k \in G \mid \phi(k) = e_H\}$

kernal is the 'preimage' of identity.
(null space types)

Note: $f: G \to H$

be group homomorphism

$\ker(f) = \{g \in G \mid f(g) = e_H\}$

$e_g \in \ker(f)$

$g_1, g_2 \in \ker(f)$

$f(g_1 g_2) = f(g_1) f(g_2) = e_H$

so $g_1 g_2 \in \ker(f)$

if $g \in \ker(f)$

$f(g g^{-1}) = e_H$

$f(g) f(g^{-1}) = e_H$

$f(g^{-1}) = e_H$

$g^{-1} \in \ker f$

ker F is a group.

Note: $f: G \to H$

$\ker(f)$

$k \in \ker(f)$

$x \in G$

$$f(x k x^{-1}) = f(x) f(k) f(x^{-1})$$
$$= f(x) e_H f(x)^{-1}$$
$$= e_H$$

so, $\forall x \in G$

$x k x^{-1} \in \ker(f)$

Normal subgroups: K is normal subgroup if given $x \in G$, $k \in K$

$x k x^{-1} \in K$

$K \trianglelefteq G$

G/K = left coset of K in G for $K \trianglelefteq G$

$= \{gK \mid g \in G\}$

$g_1 K \cdot g_2 K = g_1 g_2 K$

for $g_1 = g_1' k_1$

$g_2 = g_2' k_2$

$g_1 g_2 = g_1' k_1 g_2' k_2$

also as $x k x^{-1} \in K$

$(g_2')^{-1} k_1 g_2' = k_3 \in K$

$k_1 g_2' = g_2' k_3$

$g_1 g_2 = g_1' g_2' k_3 k_2$

$g_1 g_2 K = g_1' g_2' K$

so for $(gK)(g^{-1}K) = g g^{-1} K = e_H K$ ← identity

$g^{-1} K = (gK)^{-1}$

Ex: $G = \mathbb{R}^2$

H = x-axis $= \{(a,0) \mid a \in \mathbb{R}\}$ show $(3,1)H = (0,1)H$

$(3,1)H = \{(a+3, 1) \mid a \in \mathbb{R}\}$

$(0,1)H = \{(a+0, 1) \mid a \in \mathbb{R}\}$

$a + 3 = a'$

$(3,1)H = (0,1)H$

Ex G is abelian, every subgroup is normal.

let G be s.t $\forall\, a,b \in G$

$ab = ba$

also $H \leq G$, to prove: $H \trianglelefteq G$.

now if $H \leq G$, $\forall\, a,b \in H$

$\Rightarrow ab \in H$

and

$e_g \in H$

now, $\forall\, x \in G$ and $h \in h$

$xhx^{-1} = x.x^{-1}h = e_g h \in H$

so

$\forall\, x \in G$

$xhx^{-1} \in H$

$\therefore\ H \trianglelefteq G$

Eg: $K \trianglelefteq G$

$\eta : G \longrightarrow G/K$ (canonical map)

$g \longrightarrow gK$

$\ker(\eta) = \{g \mid gK = eK,\ g = eK \in K\}$ show η is group homomorphism.

$= \{g \mid g \in K\}$

$= K$

as $K \trianglelefteq G$ and $\eta : G \to G/K$

$g \to gK$

$n(g) = gK$

$n(g_1 g_2) = g_1 g_2 K = g_1K\, g_2K = \eta(g_1)\eta(g_2)$

as $K \trianglelefteq G$

also $n(e_g) = e_gK = K$ (idetity of $\{gK \mid g \in G\}$)

and, $n(g g^{-1}) = g g^{-1} K = K = n(g)\, n(g^{-1})$

as $n(g)\, n(g^{-1}) = $ idetity

$n(g^{-1}) = (n(g))^{-1}$

Theorm: $K \leq G$ $|G| = 2|K| \Rightarrow K \trianglelefteq G$ $(|G| < \infty)$

proof: let's say $xKx^{-1} \not\subset K$

now if $x \in K$ then $*$

if $x \notin K$ then

$K \sqcup xK = G$

$(xKx^{-1})K = xK$

$xk_1x^{-1} = xk_2$

$k_1x^{-1} = k_2$

$x = k_2 k_1^{-1} \in K$ $*$

so $xKx^{-1} \in K$, $\therefore\ K \trianglelefteq G$

Note: $A_n \trianglelefteq S_n$ as $|A_n| = \frac{1}{2}|S_n|$ and $(|S_n| < \infty)$

$A_n \leq S_n$

Subgroup not normal example: try taking non-abelian groups.

5th Aug: **Revision:**

ker(f): $f: G \to H$

$K = \ker(f)$

$= \{g \in G \mid f(g) = e_H\}$

$x \in G \quad k \in K$

$xkx^{-1} \in K$

Note: $\ker(f) \trianglelefteq G$

normal subgroup: let $H \leq G$, H is normal subgroup, if

$\forall x \in G, \forall h \in H$

$xhx^{-1} \in H$

$H \trianglelefteq G$

Theorm: If $H \leq \mathbb{Z}$, $H \neq \{0\}, \mathbb{Z}$ then $H = n\mathbb{Z}$ for some $n > 1$.

$= \{nm : m \in \mathbb{Z}\}$

proof: let $H \neq 0$, so $\exists x \in H, x \neq 0$

as $x \in H$

$-x \in H$

so H has a positive $\mathbb{Z}$

$\mathbb{P} = \{1, 2, \ldots\}$

$H \cap \mathbb{P} \neq \phi$

by well-ordering principle (set has a min)

$n = \min H \cap \mathbb{P}$

$n \in H$

as $n \in H$

$mn \in H, \forall m \in \mathbb{Z}$

$n\mathbb{Z} \subseteq H$

Now, let $x \in H$ be +ve

$x = qn + r \quad , \quad 1 \leq r \leq n-1$

as $qn \in H$,

as $n = \min H \cap \mathbb{P}$

$qn \in H$

$\Rightarrow r \in H$

as $r \in H$ but

$r < n = \min H \cap \mathbb{P}$

$\Rightarrow r = 0$

so, $x = qn \in n\mathbb{Z}$

$\Rightarrow H \subseteq n\mathbb{Z}$

for $x < 0$

$-x \in H$

$-x \in n\mathbb{Z}$

$\Rightarrow H \subseteq n\mathbb{Z}$

so $H = n\mathbb{Z}$

Theorm: G is cyclic, $|G| < \infty$, Then $G \cong \mathbb{Z}/n\mathbb{Z}$ where $n = |G|$

proof: let $G = \langle a \rangle$

$= \{a^0 = e, a, a^2, \ldots a^{n-1}\}$

$a^n = e$

$\psi \quad \mathbb{Z}/n\mathbb{Z} \to G$

$[p] \longrightarrow a^i$

① $[i] = [j]$

$i = j + nm$

$a^i = a^{j+nm} = a^j . a^{nm} = a^j$

so well defined

② $\psi([i]+[j]) = a^{i+j+r(n+m)} = a^{i+j}$

$= \psi([i]) \psi([j])$

∴ Homomorphism

③ ψ is surjective as for $\forall a^i$ in G

$\Rightarrow \psi([i]) = a^i$

so surjective.

④ one-one : $\psi([i]) = \psi([j])$

$a^{i+nm} = a^{j+nn}$

$a^i = a^j$

$a^{i-j} = a^0$

$i-j = nm$

$[i] = [j]$

$\therefore G \cong \mathbb{Z}/n\mathbb{Z}$

lemma : $f : G \to H$ group homomorphism

f is 1-1 $\Leftrightarrow \ker f = \{e_g\}$

($\Rightarrow$) given f is 1-1 and $f: G \to H$ is group homomorphism.

$f(x) = e_H = f(e_g)$

$\Rightarrow x = e_g$ (as f is 1-1)

so $\forall x$ s.t $f(x) = e_H$

$\Rightarrow x = e_g$

so $\ker(f) = \{e_g\}$

($\Leftarrow$) $\ker f = \{e_g\}$

then for $f: G \to H$ where f is group homomorp.

$\ker f = \{x \in G \mid f(x) = e_H\}$

$= \{e_g\}$

let $f(x) = f(y)$ now:

$f(xy^{-1}) = f(x) f(y^{-1})$

$= f(x) f(y)^{-1}$

$= f(x) f(y)^{-1}$

$= e_H$

so $xy^{-1} \in \ker f = \{e_g\}$

$\Rightarrow xy^{-1} = e_g$

$\Rightarrow x = y$ $\therefore f$ is 1-1

Isomorphism theorems :

① $f : G \to H$ is group homomorphism and f is onto then:

$$G/\ker(f) \cong H$$

proof : $K = \ker(f)$

$$f : G \longrightarrow H$$

$$\tilde{f} : G/\ker(f) \longrightarrow H$$

$$\tilde{f} : G/K \longrightarrow H$$

$$\tilde{f}(gK) = f(g)$$

$$g_1 K = g_2 K$$

$$g_1 = g_2 K$$

$$f(g_1) = f(g_2 K)$$

$$= f(g_2) f(K)$$

$$f(g_1) = f(g_2) e_H$$

$$f(g_1) = f(g_2)$$

so $\tilde{f}$ is cell defined

1) $\tilde{f}(eK) = f(e) = e_H$

2) $\tilde{f}(xK\, yK) = \tilde{f}(xyK) = f(xy) = f(xy) = f(x) + f(y)$

$$= \tilde{f}(xK) + \tilde{f}(yK)$$

$$\tilde{f}(xK\,yK) \quad = \tilde{f}(xK)\,\tilde{f}(yK)$$

$\tilde{f}$ is onto :

$h \in H$, f is onto. so

$\exists\, g \in G \quad f(g) = h$

$\tilde{f}(gK) = f(g) = h$

so $\tilde{f}$ is onto

$\tilde{f}$ is one-one:

$$\ker(\tilde{f}) = \{gK \mid \tilde{f}(gK) = e_H\}$$

$gK \in \ker \tilde{f}$

$f(g) = e_H$

so $g \in \ker(f) = K$

$gK = eK$

$\ker \tilde{f} = \{eK\} \Rightarrow f$ is 1-1

$\therefore \quad f : G \to H \quad$ s.t $\quad f$ is onto

$$G/\ker(f) \cong H$$

Ex: $f: G \to H$ group homomorphism

$E \trianglelefteq G$ $E \subseteq \ker f$

$\tilde{f}: G/E \to H$ show: ① $\tilde{f}$ is well-defined

$\tilde{f}(gE) = f(g)$ ② $\ker \tilde{f} \cong \frac{\ker f}{E}$

① $g_1E = g_2E$

then $g_1 = g_2h$ $h \in E$

now

$f(g_1) = f(g_2h)$

$= f(g_2)\, f(h)$

as $h \in E \subseteq \ker f$

so $f(h) = e_H$

$= f(g_2)\, e_H$

$f(g_1) = f(g_2)$

∴ $\tilde{f}$ is well-defined

② now $\ker \tilde{f} \cong \frac{\ker f}{E}$

$\Omega: \ker f \to \ker \tilde{f}$

① Ω is group Homomor
② onto ✓
③ $\ker(\Omega) = E$ ✓
} we have to construct this

$\tilde{f}: G/E \to H$

$\tilde{f}(gE) = f(g)$

$f: G \to H$

$\Omega: \ker f \to \ker \tilde{f}$

also $E \trianglelefteq G$ $E \subseteq \ker f$

$\Omega(k) = kE$

$\ker(\Omega) = \{x \in \ker f \mid \Omega(x) = E\}$

$= E$

$\Omega(k_1k_2) = k_1k_2E = k_1Ek_2E = \Omega(k_1)\Omega(k_2)$

as $E \trianglelefteq G$ and $\ker f \subseteq G$

$\tilde{f}: G/E \to H$

$\ker \tilde{f} = \{x \in gE \mid \tilde{f}(gE) = f(g) = e_H\}$

now $f(g) = e_H$

let $x \in \ker \tilde{f}$ then

$x \in gE$, now for this $g \in \ker f$

∴ $x \in kE$ ∴ $\ker f \subseteq \cup kE$

also if $k \in \ker f$

then $\tilde{f}(ke) = \tilde{f}(k)\tilde{f}(e)$

$= e_H$

so $\cup kE \subseteq \ker \tilde{f}$

∴ $\cup kE = \ker \tilde{f}$

Ω is onto as for any kE, it has a premage k in x.

so from isomorphism theorm ① as

$\Omega : \ker f \longrightarrow \ker \tilde{f}$ is group homo. and onto

$$\frac{\ker f}{\ker(\Omega)} \cong \ker \tilde{f}$$

$$\Rightarrow \frac{\ker f}{E} \cong \ker \tilde{f}$$

G is group
$H, K \leq G$
$HK = \{ hk \mid h \in H , k \in K \}$

Thm : $HK \leq G \Leftrightarrow HK = KH$ as sets $kh = h'k'$

proof : $(\Leftarrow)$ $HK = KH$

$e = ee \in HK$

$hk \in HK$

$$\underbrace{hk\,h'k'}_{} = h\underbrace{h''k''}_{}k' \in HK$$

$$(hk)^{-1} = k^{-1}h^{-1} = h''k'' \in HK$$

so $HK \leq G$

$(\Rightarrow)$ $HK \leq G$
let $k \in K$ $h \in H$
$k = ek \in HK$
$h = he \in HK$
so $kh \in HK$
$KH \subseteq HK$

now as $KH \subseteq HK$ we try to prove $HK \subseteq KH$:
let $hk \in HK$
as HK is a group
$(hk)^{-1} \in HK$
$\Rightarrow k^{-1}h^{-1} \in HK$
$\Rightarrow KH \subseteq HK$

so $KH = HK$

Theorm : $K \trianglelefteq G$, $H \leq G$
then $HK = KH$ and
$HK \leq G$

proof : now let $hk \in HK$ $\forall h \in H$ and $k \in K$
then
$hkh^{-1} \in K$
$hk \in Kh$
so $\forall hk \in HK$
$\Rightarrow hk \in KH$
$\therefore HK \subseteq KH$

now if $kh \in KH$
then $\Rightarrow hh^{-1}kh = hk' \in HK$
$KH \subseteq HK$

$\therefore KH = HK$
$\Rightarrow HK \leq G$

Theorem : $H \leq G$, $K \trianglelefteq G$ **Second isomorphism theorem**

$H \cap K \trianglelefteq H$

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

proof :

$$\begin{tikzcd} H \arrow[r, "i"] \arrow[dr, "\phi"'] & HK \arrow[d, "\eta"] \\ & \frac{HK}{K} \end{tikzcd}$$

$\eta : G \rightarrow G/N$

$g \rightarrow gN$

$N \trianglelefteq G$

$\phi : H \rightarrow HK/K$

$h \rightarrow hK$

$\Theta \in HK/K$

$\Theta = hk\,K$

$= (hK)(kK)$

$= hK$

$\phi(h) = hK = \Theta$

ϕ is onto

note if $h \in H \cap K$

$\phi(h) = hK = eK$

so $H \cap K \leq \ker \phi$

now, let $h \in \ker \phi$ then h is s.t $h \in H$ and

$hK = K$

as $K \trianglelefteq G$ $h \in K$

so $h \in H \cap K$

$\ker \phi \leq H \cap K$

as $K \trianglelefteq G$ and for $K \trianglelefteq HK$ as

① $e \in HK$

② if $k \in K$

$(h_1k_1)k(h_1k_1)^{-1}$

$= h_1k_1kk_1^{-1}h_1^{-1}$

$= h_1kh_1^{-1}$

$= k' \in K$

so $K \trianglelefteq HK$

$\therefore \ker \phi = H \cap K$

now, as $\phi : H \rightarrow HK/K$ is onto

and as $i : H \rightarrow HK$ is group homomorphism

as $i(h) = hk$ for some $k \in K$

$i(h_1h_2)$

$= h_1h_2k$

$= h_1h_2h_2^{-1}kh_2$

$= h_1kh_2$

$= i(h_1)\,i(h_2)$

and $\eta : G \rightarrow G/N$ s.t $N \trianglelefteq G$

then for $g \rightarrow gN$

$\eta(g) = gN$

$\eta(g_1g_2) = g_1g_2N$

$= g_1N\,g_2N$

$= \eta(g_1)\,\eta(g_2)$

ϕ is also group homomorphism

$\therefore$ $\phi : H \rightarrow HK/K$

where $\ker(\phi) = H \cap K$

$$\Rightarrow \frac{H}{H \cap K} \cong \frac{HK}{K}$$

Recall : $G = H \times K$

$H \cong H \times \{e_K\} = \{(h, e_K) \mid h \in H\}$

then $H \times \{e_K\} \trianglelefteq G$

as for $(h, e_K) \in H \times \{e_K\}$

$(h', k)(h, e_K)(h'^{-1}, k^{-1})$

$= (h'', e_K) \in H \times \{e_K\}$

similarly $K \cong \{e_H\} \times K \trianglelefteq G$

Also Note : $(H \times \{e_K\}) \cap (\{e_H\} \times K) = \{(e_H, e_K)\}$

Theorem : G is a group $H, K \trianglelefteq G$

$G = HK$

$H \cap K = \{e\}$

then $G \cong H \times K$

proof : $\varphi = \theta = hkh^{-1}k^{-1} \in K \cap H = \{e\}$

as $\underbrace{hkh^{-1}}_{\in K}k^{-1} \in K \cap H$

$h\underbrace{kh^{-1}k^{-1}}_{\in H}$

$hkh^{-1}k^{-1} = e$

$hk(kh)^{-1} = e$

$\Rightarrow \quad hk = hk$

so $\forall\, h, k \in H, K$

$hk = kh$

now $\phi : H \times K \longrightarrow G = HK$

$\phi(h, k) = hk$

$\phi((h_1, k_1)(h_2, k_2))$

$= \phi(h_1 h_2, k_1 k_2)$

$= h_1 h_2 k_1 k_2$

$= h_1 k_1 h_2 k_2$

$= \phi(h_1, k_1) \cdot \phi(h_2, k_2)$

$\therefore$ ϕ is group homomorphism

$\phi(h, k) = e$

$hk = e$

$h = k^{-1} \in H \cap K = \{e\}$

$h = e = k^{-1}$

$\Rightarrow k = e$

so $\ker(\phi) = \{(e, e)\}$

$\Rightarrow \phi$ is 1-1

to check if ϕ is onto:

for $h \in H$ and

$k \in K$

$\phi(h, k) = hk$

so $\forall\, hk \in G$ has

a preimage in (h, k)

$\therefore \phi$ is onto.

ϕ is 1-1, ϕ is onto, and ϕ is group homorphism. $G = HK \cong H \times K$

8th Aug :

first isomorphism theorm: $f : G \to H$ f is onto, f is group homomorphism

$$G/\ker(f) \cong H$$

$$\bar{f} : G/K \to H$$
$$\bar{f}(gK) = f(g)$$

Interesting: $f : G \to H$, $E \trianglelefteq G$, $E \subseteq \ker(f)$

$\bar{f} : G/E \to H$
$gE \to f(g)$

then $\ker(\bar{f}) \cong \frac{\ker(f)}{E}$

Intersting:

$H, K \leq G$
$HK = \{hk \mid h \in H, k \in K\}$

prop^n: $HK \leq G \Leftrightarrow HK = KH$

proof: $(\Leftarrow)$ trivial

$(\Rightarrow)$ let $k \in K$
$h \in H$
$k = e\, k \in HK$
$h = he \in HK$
$k.h \in HK$
$\Rightarrow KH \subseteq HK$ — ①

$g = hk \in HK$

$g = (g^{-1})^{-1} = \left(\overset{\text{as } g^{-1} \in HK}{(hk)^{-1}}\right)^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$

$HK \subseteq KH$ — ②

from ① and ②
$HK = KH$

2nd isomorphism theorm: $K \trianglelefteq G$, $HK = KH$
$HK \leq G$

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

proof: $\phi : H \to \frac{HK}{K}$ s.t $\ker(\phi) = H \cap K$

ϕ : onto
ϕ : group homorphism

$$\begin{tikzcd} H \arrow[r, dash] \arrow[dr, dash] & HK \arrow[d, dash] \\ & \frac{HK}{K} \end{tikzcd}$$

interesting: $G = HK$
$H, K \trianglelefteq G$, $H \cap K = \{e\}$

$$G \cong H \times K$$

third isomorphism theorem: $K \leq H \leq G$, $K \trianglelefteq G$, $H \trianglelefteq G$

then

$H/K \trianglelefteq G/K$

and $\dfrac{G/K}{H/K} \cong G/H$

proof: $f : G/K \to G/H$

now

$f(gK) = gH$

① **well defined**:

$g_1K = g_2K$

$g_1k_1 = g_2k_2$

$g_1 = g_2k_2k_1^{-1}$

as $K \leq H$

$k_2k_1^{-1} \in H$

$g_1H = g_2H$

∴ well defined

② **onto**:

$f(gK) = gH$ so $\forall g \in G$, s.t gH there is a pre image gK.

∴ onto

③ **Homomorphism**:

$$f(g_1K\, g_2K) = f(g_1g_2K) = g_1g_2H$$
$$= g_1H\, g_2H$$
$$= f(g_1)\, f(g_2)$$

∴ group homorphism

④ **ker(f)**:

$\ker(f) = \{ gK \mid f(gK) = H \}$

as $K \leq H$, if $g \in H$ then posible.

∴ $\ker(f) = H/K$

$$\therefore \quad \frac{G/K}{H/K} \cong G/H$$

now, $H/K \trianglelefteq G/K$

$H/K = \{ hK \mid h \in H \}$,

$G/K = \{ gK \mid g \in G \}$

Now as $H \trianglelefteq G$ and $K \trianglelefteq G$

① e of $G/K = K = e$ of H/K

② $h_1K \in H/K$ and $h_2K \in H/K \Rightarrow h_1h_2K \in H/K$

③ $h_1K \in H/K$ as $h_1h_1^{-1}K \in H/K$

$\Rightarrow h_1h_1^{-1}K = hK$

$\Rightarrow h_1^{-1}K = h_1^{-1}hK \in H/K$

$\Rightarrow h_1^{-1} \in H/K$

correspondance theorm : $N \trianglelefteq G$, correspondence of every subgroup of G/N and subgroup of G containing N is a bijection.

(every subgroup of G/N is of form H/N, where $N \leq H \leq G$)

proof: H' be a subgroup of G/N

$$\beta(H') = \{g \in G \mid gN \in H'\}$$

$\Rightarrow N \subseteq \beta(H') \subseteq G$

and

$\Rightarrow e_G \in N \quad \therefore \quad e_G \in \beta(H')$

if $x, y \in \beta(H')$

as $xN\,yN = xyN$

$\Rightarrow xy \in \beta(H')$

$(xN)^{-1} = x^{-1}N \Rightarrow x^{-1} \in \beta(H')$

$\therefore \beta(H') \leq G$ ——①

now let $N \leq H \leq G$

$\alpha(H) = \{hN \mid h \in H\} \subseteq G/N$

$\alpha(H) \leq G/N$ ——②

now, for $N \leq H \leq G$

$$(\beta \circ \alpha)(H) = \beta(H/N)$$
$$= \{g \in G \mid gN \in H/N\}$$
$$= H$$

$\beta \circ \alpha = I$

now $H' \leq G/N$

$$(\alpha \circ \beta)(H') = \alpha(\{g \in G \mid gN \in H'\})$$
$$= \{gN \in H'\}$$
$$= H'$$

$\alpha \circ \beta = I$

$\therefore$ $\alpha : X \to Y$

$\beta : Y \to X$ are bijection

finite cyclic group's subgroups are cyclic :

let $G = \langle a \rangle = \{1, a, \dots a^{n-1}\}$

$H \leq G$, $H \neq \{1\}, G$

$\exists\, a^r \in H$, $r \neq 0$, $r \geq 1$

$$\min\{r \mid r \geq 1,\ a^r \in H\} = c$$

$a^c \in H \Rightarrow \langle a^c \rangle \subseteq H$

now let $a^r \in H$, $r \geq 1$

$r = qc + \delta$ for $\delta \neq 0$

$0 \leq \delta \leq c-1$

$a^r = a^{qc} \cdot a^\delta$

$a^\delta \in H$ but as c is min

$\Rightarrow \delta = 0$, $\therefore H \leq \langle a^c \rangle$

$\Big\}$ $H = \langle a^c \rangle$

Qne: G is finite cyclic group, $H, K \trianglelefteq G$
$|H| = |K|$
$\Rightarrow H = K$

Proof: let $|H| = |K|$ and $H \neq K$
as H, K are also cyclic (proved above)
let
$H = \langle a^r \rangle$ $K = \langle a^m \rangle$
s.t $a^r \neq a^m \rightarrow a^{nm} \neq a^{nr}$ ✗
but $a^{nr} = a^{nm}$
as $|H| = n = |K|$
$a^{nr} = a^{nm}$
$\therefore H = K$

Lemma: F is a field, $G \leq F^*$, G is finite then G is cyclic

Proof: let
$H = \langle a^r \rangle \leq G$
$l = $ lcm of ord of all cyclic subgroups of G.
$a^l = 1$
so this will have l roots.
let $|G| = n$ as $l = \max\{|H_1|, |H_2|, |H_3|, \ldots\}$ ← cyclic subgroups of G
then $n \leq l$

if G is cyclic then also $n \leq l$, if G is not cyclic then also $n \leq l$

now let $g \in G$ s.t $\text{ord}(g) = l$ then
$l | n$
or $l \leq n$

as $l = \text{lcm}\{\ldots\}$
and if $a^{l_1} \in G$
and $a^{l_2} \in G$
then $a^{l_1 l_2} \in G$

$\Rightarrow l = n$
$G = \langle g \rangle$

Group actions: G acts on A if
$\exists$ $G \times A \to A$
$(g, a) \to g.a$
s/t 1) $ea = a, \forall a \in A$
2) $g_1(g_2 a) = (g_1 g_2) a$

Orbit: $\mathcal{O}_a = \{ga \mid g \in G\}$

Stabiliser: $G_a = \{g \in G \mid ga = a\}$

Note: $G_a \trianglelefteq G$
① as $e \in G_a$
② as $x \in G_a$ and $y \in G_a$
then $xya = x(ya) = x(a) = a$
$\therefore xy \in G_a$
③ $x \in G_a$ then
$(x^{-1}x)(a) = x^{-1}a = a \Rightarrow x^{-1} \in G_a$

Important: $\mathcal{O}_a \to G/G_a$
$ga \longrightarrow gG_a$

① $g_1 a = g_2 a$
$g_2^{-1} g_1 a = a$
$\Rightarrow g_2^{-1} g_1 \in G_a$
$\Rightarrow g_2 G_a = g_1 G_a$
$\therefore$ well defined

② $x \in G/G_a$
$x = gG_a$
$x = \mathcal{Q}(ga)$
$\mathcal{Q}$ is onto

③ $\mathcal{Q}(g_1 a) = \mathcal{Q}(g_2 a)$
$\Rightarrow g_1 G_a = g_2 G_a$
$g_1 = g_2 h$, $h \in G_a$
$g_1 a = (g_2 h) a$
$= g_2 (ha)$
$= g_2 a$
$\mathcal{Q}$ is 1-1

$\therefore \mathcal{Q}$ is bijection
$\mathcal{Q}: \mathcal{O}_a \longrightarrow G/G_a$

Conjugate : $O_x = \{ \underset{\text{conjugates of } x}{\underbrace{gxg^{-1}}} \mid g \in G \}$

$x \in O_x$

when $|O_x| = 1 \Rightarrow O_x = \{x\}$

$gxg^{-1} = x$

$gx = xg \quad \forall g \in G$

$x \in Z(G)$

Centre of group : $Z(G) = \{ x \in G \mid gx = xg \quad \forall g \in G \}$

Exe: $Z(G) \trianglelefteq G$

$Z(G) = \{ x \in G \mid gx = xg \quad \forall g \in G \}$

① $e \in Z(G)$

② if $x \in Z(G)$ and $y \in Z(G)$

$(gx)y = x(gy) = (xy)g$

$\therefore xy \in Z(G)$

③ $x \in Z(G)$

$g.e = e.g$

$g(x^{-1}x) = (x^{-1}x)g$

$gx^{-1}x = x^{-1}(gx)$

$gx^{-1} = x^{-1}g$

④ if $x \in Z(G)$

then $gxg^{-1} \in Z(G)$

$gx = gx$

$g(xgg^{-1}) = gx(g^{-1}g)$

$g(gxg^{-1}) = (gxg^{-1})g$

Theorm : $|G| = p^n_{n \geq 1}$ p is a prime

then $Z(G) \neq \{e\}$

proof:

G acts on A

$\sim$ on A

$a \sim b$ if $b = ga$ for some $g \in G$

$G = O_e \sqcup O_{g_1} \sqcup O_{g_2} \cdots \sqcup O_{g_l}$

$|G| = p^n$

$\Sigma |O_{g_i}| = p^n$

then $|O_{g_i}| = p^r$ for some r

$p^n = 1 + p^{r_1} + p^{r_2} + \cdots$

$\hookrightarrow$ as $|O_e| = 1$

$\Rightarrow p \mid 1$ $\ast$

let $Z(G) = \{e\}$ then

$Z(G) = \{ x \mid gx = xg, \forall g \in G \}$

$= \{e\}$

$O_e = \{ geg^{-1} \mid g \in G \}$

$= \{e\}$ as

$|O_e| = 1$

cor: $|G| = p^2 \Rightarrow G$ is abelian

proof: as $|G| = p^2$
$Z(G) \neq \{e\}$

let $Z(G) \neq G$
then
$|G| = p^2$
but as $|Z(G)| \neq 1$
$\Rightarrow |Z(G)| = p$

now, $|G/Z(G)| = p$, as prime, it is cyclic (thm)
$G/Z(G) = \{ a^i Z(G) \mid 0 \leq i < p-1 \}$

let $x, y \in G$
$xZ(G) = a^i Z(G)$
$yZ(G) = a^j Z(G)$

$x = a^i \alpha$
$y = a^j \beta \qquad \alpha, \beta \in Z(G)$

$xy = a^i \alpha a^j \beta$
$= a^{i+j} \alpha \beta$
$yx = a^j \beta a^i \alpha$
$= a^{i+j} \alpha \beta = xy$
but this means
$Z(G) = G$
so $Z(G) \neq G$ *

As $Z(G) = G$
$\Rightarrow G$ is abelian

Note: $|G| = p^3$ doesn't necs mean G is abelian.

counter example:

$$H(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

$|H(\mathbb{Z}/p\mathbb{Z})| = p^3$

12th Aug:

group actions: G acts on A

$G \times A \to A$

$(g,a) \to g.a$

s.t

① $ea = a \quad \forall a \in A$

② $g_1(g_2 a) = (g_1 g_2) a \quad \forall g_1, g_2 \in G$, $a \in A$

$G_a = \{g \in G \mid ga = a\}$ stabiliser

$O_a = \{ga \mid g \in G\}$ orbit

Note: $|O_a| = |G/G_a|$

$ga \to gG_a$

conjugate action: $A = G$

$\underbrace{g.a = gag^{-1}}_{\text{action}}$

$|O_a| = 1$

then $O_a = \{ga \mid g \in G\}$

as $|O_a| = 1$

only one ∴ $gag^{-1} = a$

as $a \in O_a$

$ga = ag \quad \forall g \in G$

∴ $a \in Z(G)$

as $Z(G) = \{a \mid ga = ag \ \forall g \in G\}$

∴ $|O_a| = 1 \Leftrightarrow a \in Z(G)$

Important: $|G| = p^r, r \geq 1$ then $Z(G) \neq \{e\}$

Theorem: (Cauchy's theorm) G is finite group and p prime s.t $p \mid |G|$ then $\exists x \neq e$ s.t $x^p = e$

proof: $S = \{(x_1, x_2, \dots x_p) \mid x_i \in G, \ x_1 x_2 \dots x_p = e\}$

$|S| = |G|^{p-1} \to p \mid |S|$

$H = \{1, \sigma, \sigma^2, \dots \sigma^{p-1}\}$

$|H| = p$ $\quad \sigma(x_1, x_2, \dots x_p) = (x_2, x_3, \dots x_p, x_1)$

$x_1 x_2 \dots x_p = e$

$\Rightarrow x_2 x_3 \dots x_p = x_1^{-1}$

$\Rightarrow x_2 x_3 \dots x_p x_1 = e$

$\therefore (x_2, x_3, \dots x_p, x_1) \in S$

$\alpha \in S$ s.t
then $O_\alpha = \{h.\alpha \mid \forall h \in H\}$

$\downarrow$ $\{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$

$|O_\alpha| \mid |H| = p$

$|O_\alpha| = 1$ or p

if $|O_\alpha| = 1$
$h.\alpha = \alpha$
$\Rightarrow \underline{(x^p = 1)}$

$|O_\alpha| = p$

$$|S| = |Z(G)| \overset{\curvearrowright \text{orbits}}{+} \sum_{\alpha \in S} |G/G_\alpha| = |G|^{p-1}$$

$$p \mid |Z(G)| + \sum_{\alpha \in S} |G/G_\alpha|$$

$|S| = |G|^{p-1} = k + sp$
as O_α will have 1 or p elements.
if $|O_\alpha| = 1$
$\alpha \in Z(G)$
similarly

$|S| = k + sp$
$p \mid k + sp \Rightarrow p \mid k$
but as $k \geq 1$
$\Rightarrow k \geq 2$
$\therefore \exists x \neq e$ s.t
$(x, x, \ldots x)$ has orbit 1
$x^p = e$

Sylow's theorems:

1> $|G| = p^r m$, p prime $r \geq 1$, $p \nmid m$
Then $\exists H \leq G$ s.t $|H| = p^r$.

Defn: A subgroup H of G of order p^r is called sylow p-subgroup of G.

2> H, K are two p-sylow subgroup of G
then H, K are conjugate. $\rightarrow$ $\exists g \in G$ s.t $\underline{K = gHg^{-1}}$ } meaning of two subgroups being conjugates.

$\mathrm{Sylow}_p(G) = \{H \mid H \leq G,\ |H| = p^r\}$

$n_p = \#\mathrm{Sylow}_p(G)$

3> $\cdot\ n_p \mid m$
$\cdot\ n_p \equiv 1 \pmod p$

i.e $k n_p = m$ and also
$n_p = 1 + k'p$ for
some k, k'

Important observation: If $n_p=1$ $\{gHg^{-1} \mid g\in G\}=\{H\}$

$\hookrightarrow$ conjugates of H

$\Rightarrow gHg^{-1}=H \ \forall g\in G$

$\Rightarrow H \trianglelefteq G$

Important observation: G is finite group $|G|=pq$
$p<q$ primes then
① $n_q=1$
② $n_p=1$ if $p \times q-1$

proof: as $n_q \equiv 1 \pmod q$
and $n_q \mid p$
$n_q=1+kq \mid p$
but as $q>p$
$\Rightarrow n_q=1$

also $n_p \equiv 1 \pmod p$
and
$n_p \mid q$
$\Rightarrow n_p=mq=1+kp$
but as $n_p \mid q \Rightarrow n_p=1$ or q
if $n_p=q$ then
$kp=q-1$
$\Rightarrow p \mid q-1$
$\therefore$ if $p \nmid q-1$
$\Rightarrow n_p=1$

lemma: $|G|=pq$, $n_p=1$, $n_q=1$ then H sylow p-subgroup,
K sylow q-subgroup

$G=HK \cong H\times K$

proof: Note: $H\trianglelefteq G$, $K\trianglelefteq G$, $HK\leq G$

$\frac{|HK|}{|K|}=\frac{|H|}{|H\cap K|}$
as $|H\cap K|=1$
$H\cap K=\{e\}$
and $|HK|=|G|$
$\Rightarrow HK=G$

or: as $K \lneq HK$
we $H,K \trianglelefteq G$
$h_1k_1=h_2k_2$
and $h_1=h_2$
$\Rightarrow k_1=k_2$

my **proof:** let $HK\leq G$
and $|HK|=|G|$
$\Rightarrow HK=G$
also now
$\psi: H\times K \longrightarrow HK$
$(h,k) \longrightarrow (hk)$
then ψ is one-one, onto, and homomorphic
$\therefore G=HK \cong H\times K$

__lemma__: $\gcd(m,n)=1$ then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

__proof__: If $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$a \to (a+m\mathbb{Z}, a+n\mathbb{Z})$

now $\ker(\varphi) = \{ a \in \mathbb{Z} \mid (a+m\mathbb{Z}, a+n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z}) \}$

$\Rightarrow m|a$ and $n|a$

$\Rightarrow mn|a$ ($\because \gcd(m,n)=1$)

$\Rightarrow \ker(\varphi) = mn\mathbb{Z}$

__Now__, $\overline{\Psi} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

① $\overline{\Psi}$ __is onto__: let $m\alpha + n\beta = 1$

(chinese reminder theorm)

then

$(x-y)(m\alpha + n\beta) = x-y$

$xm\alpha + nx\beta - my\alpha - ny\beta = x-y$

$m(x\alpha - y\alpha) + n(x\beta - y\beta) = x-y$

$y + (x-y)m\alpha = x + (y-x)n\beta$

let

$y + (x-y)m\alpha = x + (y-x)n\beta = a$

then $a = (y \bmod m, x \bmod n)$

for $(y \bmod m, x \bmod n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\exists \bar{a} \in \mathbb{Z}/mn\mathbb{Z}$

$\therefore \overline{\Psi}$ is injective

② $\overline{\Psi}$ __is homorphism__:

let $Q = (a+m\mathbb{Z}, b+n\mathbb{Z})$

$Q_1 = (a+m\mathbb{Z}, \bar{0}) = \overline{\Psi}(\alpha_1)$

$Q_2 = (\bar{0}, b+n\mathbb{Z}) = \overline{\Psi}(\alpha_2)$

now $\overline{\Psi}(\alpha_1) + \overline{\Psi}(\alpha_2) = Q_1 + Q_2 = Q = \overline{\Psi}(\alpha_1 + \alpha_2)$

③ $\overline{\Psi}$ is __one-one__: Trivial

$\therefore \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Ex: $|G|=15 \Rightarrow 15=\underset{p}{3}\times\underset{q}{5}$

as $3 \nmid 5-1$

$\Rightarrow n_3=1$ and $n_5=1$

$\therefore |G|=|HK| \therefore G\cong H\times K \cong \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$

$\therefore G$ is cyclic

$|G|=77=11\times 7$

$G\cong \underset{7}{H}\times\underset{11}{K} \cong \mathbb{Z}/77\mathbb{Z}$

$\therefore G\cong \mathbb{Z}/77\mathbb{Z}$

19th Aug:

The class equation:

$A = G$

as $g.a = gag^{-1}$

① $g.e = e$

② $(g_1g_2).a = g_1(g_2.a)$

Note: H, T conjugates if $\exists\, g \in G$ s.t $H = gTg^{-1}$

here $O_H = \{g.H \mid g.H = H\}$

orbit

$= \{gHg^{-1} \mid gHg^{-1} = H, g \in G\}$

$\therefore K \in O_H$

also $H \in O_H$

$\therefore$ if $H, K \in O_H$ then they are in conjugation

$|O_H|$ = no. of conjugates

Stabiliser:

$$G_a = \{g \in G \mid g.a = a\}$$

if we write it as H, K

→ ~~Normaliser of G wrt H~~

$$G_H = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$$

now, $|O_H| = |G/N_G(H)| = |G/G_H|$

centraliser: $C_G(H) = \{g \in G \mid gh = hg, \forall h \in H\}$

$$N_G(H) = \{g \in G \mid \underbrace{gHg^{-1} = H}_{\text{group action}}\}$$

$$N_G(\{s\}) = C_G(\{s\}) = \{g \in G \mid gsg^{-1} = s\}$$

let G be a finite group and let $g_1, g_2, \dots g_r$ be representative of distinct conjugacy classes of G, not contained in $Z(G)$ (centre)

then $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$

Note $C_G(g_i) = \{g \in G \mid g g_i g^{-1} = g_i\}$

if $|O_G(g_i)| = 1$

$\Rightarrow O_G(g_i) = \{g.g_i \mid \forall g \in G\}$

$\Rightarrow g g_i g^{-1} = g_i \ \forall g \in G$

$\therefore g_i \in Z(G)$

$$|G| = \underbrace{|\{1\}| + |\{z_1\}| + |\{z_2\}| + \cdots \cdots}_{|Z(G)|}$$

$$\left.\begin{matrix} + |O_{g_1}| \\ + |O_{g_2}| + \cdots \end{matrix}\right\} \sum_{i=1}^{r} |O_{g_i}| = |G/_{C_G(g_i)}|$$

Sylow's first theorem: $|G| = p^r m$, $r \geq 1$ and $p \times m$

then $\exists H \leq G$ s.t $|H| = p^r$

proof: S is a set
$|S| = p^r m$

$\Lambda = \{E \subseteq S \mid |E| = p^r\}$

set of subsets

$$|\Lambda| = \binom{p^r m = n}{p^r} = \frac{(n)(n-1)\cdots\cdots(1)}{(p^r)!\,(n-p^r)!} = \frac{(n)(n-1)\cdots\cdots(n-p^r+1)}{p^r!}$$

let $p \mid p^r - k$

$\Rightarrow k = p^i \alpha$

and $p \times \alpha$, $i < r$

$p^r - k = p^r - p^i\alpha = p^i(p^{r-i} - \alpha)$

now, $n-k = p^r m - k = p^r m - p^i \alpha = p^i(p^{r-i}m - \alpha)$

$p^i \mid p^r - k \Leftrightarrow p^i \mid p^r m - k = n-k$

$p^{i+1} \nmid p^r - k \Leftrightarrow p^{i+1} \nmid n-k$

$\Rightarrow p \nmid |\Lambda|$ as $\binom{n-k}{p^r-k}$ form, and

as $p^{i+1} \nmid (n-k)$

and

$p^{i+1} \nmid (p^r - k)$

now, $\Lambda = \{E \subseteq G \mid |E| = p^r\}$

as $p \times |\Lambda|$

Let there be a group action from $G \to \Lambda$

where

$g.E$ s.t $g.E = gE$ $\quad |G| = p^r m$

① $e.E = E$

② $(g_1 g_2).E = (g_1(g_2 E)) = g_1.(g_2 E)$

$\therefore$ $g.E$ is a group action.

now, $|gE| = |E| = p^r$

and $O_{v_i} = \{g v_i \mid g v_i = v_i\}$

$\Lambda = O_{v_1} \sqcup O_{v_2} \sqcup O_{v_3} \cdots\cdots O_{v_s}$ → Note $v_s \in \Lambda$

$|\Lambda| = |O_{v_1}| + \cdots\cdots |O_{v_s}|$

as $p \times |\Lambda|$

$\Rightarrow \exists\, v_i$ s.t $p \times |O_{v_i}|$

now $O_U = \{ gU \mid gU = U \}$

$p^r m = |\text{stab}(U)|\,|O_U| = |G|$

as $|G / \text{stab}(U)| = |O_U|$

$\text{stab}(U) = \{ g \in G \mid gU = U \}$

$|\text{stab}(U)| = p^r s$ as $p \nmid |O_U|$

$H = \text{stab}(U) = \{ g \in G \mid gU = U \}$

now, $HU = \{ hU \mid h \in H \} \subseteq U$

as $H = \text{stab}(U)$ if $h \in \text{stab}(U)$

$hU = U$

$\therefore HU \subseteq U$

now, $U = U_1 \sqcup U_2 \sqcup \dots U_l$

$|U| = p^r \longleftarrow |H| l = |U| = p^r$

$\Rightarrow |H| = p^j \Rightarrow |H| = p^r$

Theorm: $K \leq G$, $p \mid |K|$, $|G| = p^r m$, $H \in \text{Syl}_p(G)$

then $\exists\, g \in G$ s.t $gHg^{-1} \cap K$ is a sylow p-subgroup of K.

Note: if $K \in$ sylop subgroup$_K$ then

$K = gHg^{-1} \cap K$

$\Rightarrow gHg^{-1} = K$ → proof of second theorm.

of $\underline{K}$: this is important

proof: $S = G/H$

$|S| = m$

note: as $p \times m$

$\gcd(m, p) = 1$

let G act on S by:

$g.(aH) = gaH$

now, $O(aH) = \{ g.aH \mid g.aH = aH \}$

$= \{ aH \}$

$= S$

$\text{stab}(H) = \{ s \in G/H \mid s.H = H \}$

$= H$

$\text{stab}(gH) = \{ s \in G/H \mid s.gH = gH \}$

$s.gH = sgH = gH$

then $sgh_1 = gh_2$

$\Rightarrow sg = gk$

$\Rightarrow s \in gHg^{-1}$

$\therefore \text{Stab}(gH) \subseteq gHg^{-1}$

if $x \in gHg^{-1}$

then $x = gh_1g^{-1}$

$gh_1g^{-1}gH = gH$

$\therefore x \in \text{Stab}(gH)$

$gHg^{-1} \subseteq \text{Stab}(gH)$

$\therefore \text{stab}(gH) = gHg^{-1}$

now, as $(p, |S|) = 1$

and $O(gH) = S$

$\exists$ an orbit s.t

$p \nmid |O_{gH}|$

$\Rightarrow p \nmid |G/\text{Stab}_G(gH)|$

now let K be the subgroup

s.t $p \mid |K|$

$\text{Stab}_G(gH) = gHg^{-1}$

now, $L = \text{Stab}_K(gH) = gHg^{-1} \cap K$

now, $O(gH) = \{ g'gH \mid g'gH = gH \}$

$= S$, if $g' \in K$ then

also $\{ g'gH \mid g'gH = gH \}$

$= S$

as even if $g' \in K$

$g'gH \in S$

and $e \in K$

$\therefore |O(gH)| = |K/L|$ coprime with p

then $\frac{|K|}{|L|} = |K/L|$

$$\Rightarrow \underset{\substack{\downarrow \\ p^s m}}{|K|} = \underset{\substack{\downarrow \\ p^s}}{|L|}\; \underset{\substack{\downarrow \\ m \text{ coprime with } p}}{|K/L|}$$

$\therefore L \in \text{Syl}_p(K)$

Sylow's second theorem: $H_1, H_2 \in \text{Syl}_p(G)$ then $H_2 = gH_1g^{-1}$ for some $g \in G$

proof : using theorem already proved

$K \leq G$, $K \mid |P|$ then $\exists g \in G$ s.t $gHg^{-1} \cap K$ is a $\text{Sylow}_p(K)$

for $K \in \text{Sylow}_p(G)$
and
$H \in \text{Sylow}_p(G)$

$$K = gHg^{-1} \cap K$$

$$\therefore K = gHg^{-1}$$

$\therefore$ H, K are conjugates

Sylow's third theorem : $n_p = \#\text{Syl}_p(G)$
(i) $n_p \mid m$
(ii) $n_p \equiv 1 (\text{mod } p)$

proof : let $S = \#\text{Sylow}_p(G)$
by ② any two sylow p-sub are conjugate

$$N = \{g \in G \mid gHg^{-1} = H\} \supseteq H$$

$$\Psi : \text{Sylow}_p(G) \longrightarrow G/N = \{gN \mid g \in G\}$$
$\exists g \in G$ s.t
$K = gHg^{-1} \longrightarrow gN$

well defined : $gHg^{-1} = g_1Hg_1^{-1}$

$$g_1^{-1}gHg^{-1}g_1 = H$$

$$(g_1^{-1}g)H(g_1^{-1}g)^{-1} = H$$

so $g_1^{-1}g \in N \Rightarrow gN = g_1N$

onto: trivial

one-one: $g_1N = g_2N$
$g = g_1x$, $x \in N$

$$gHg^{-1} = (g_1x)H(g_1x)^{-1}$$
$$= g_1\underbrace{xHx^{-1}}g_1^{-1}$$
$$= g_1Hg_1^{-1}$$ as $x \in N$

$\therefore \Psi$ is one-one

$$\therefore |\text{Syl}_p(G)| = |G/N| = n_p$$

also $|G/H| = \frac{\cancel{p^\alpha}}{\cancel{p^\alpha}}.m = m = |G/N||N/H|$

$$m = n_p|N/H|$$

$$\therefore n_p \mid m$$

now for $n_p \equiv 1 \pmod p$

from ② ; H also acts on sylow p-sub by conjugation.

$h \cdot K = hKh^{-1}$ by conjugation

$O_K = \{ h \cdot K \mid h \in H \}$

group action as

① $h \cdot K$ for $h = e$

$e \cdot K = K$

② $(h_1 h_2)k = h_1(h_2 k)$

So $\text{sylow}_p(G) = O_{K_1} \sqcup O_{K_2} \sqcup \cdots\cdots \sqcup O_{K_r}$

$O_K = \{K\}$ then

$hKh^{-1} = K \quad \forall h \in H$

now, $N(K) = \{ h \in H \mid hKh^{-1} = K \}$

as $hKh^{-1} = K \quad \forall h \in H$

$H \leq N(K)$

$\Rightarrow H = N(K)$

$K \trianglelefteq H = N(K)$

$\Rightarrow \quad K = H$

Note: $O_K = \{ hKh^{-1} \mid h \in H \}$

$$|O_K| = |H/G_H(K)| = \frac{|H|}{|G_H(K)|} = \frac{p^r}{|G_H(K)|}$$

$|O_K| \mid p \Rightarrow |O_K| = 1$ or p → this is because $\frac{p^r}{|G_H(K)|}$

Now, $|\text{sylow}_p(G)| = 1 + pk$

$\therefore n_p = 1 + pk$

$\Rightarrow n_p \equiv 1 \pmod p$

groups of order p^2q:

$P \in Syl_p(G)$ n_p
$Q \in Syl_q(G)$ n_q (simple)

① $p > q \Rightarrow P \trianglelefteq G$
$n_p | q$ $n_p = 1 + pk$, $n_p = q \Rightarrow q > p$ ✱
$n_p = 1$
$\Rightarrow P \trianglelefteq G$

② $p < q$
$n_q = 1 \Rightarrow Q \trianglelefteq G$
$n_q \neq 1$
$n_q | p^2 \Rightarrow n_q = p, p^2 \equiv 1 + kq$
$n_q = p \Rightarrow$ $p > q$ ✱
$n_q = p^2 \Rightarrow$ $q | p^2 - 1$
$\Rightarrow q | (p-1)(p+1) \Rightarrow q | p+1$, $p+1$ is prime
$p = q - 1$
$\Rightarrow$ $q = 3$ $p = 2$
$|G| = 2^2 \cdot 3 = 12$

∴ if $|G| \neq 12$ and
$|G| = p^2 q$
G is <u>not</u> simple

groups of order $|G| = 12$:

$|G| = 12 = 2^2 \cdot 3$
$H \in Syl_2(G)$
$K \in Syl_3(G)$

now if $K \trianglelefteq G$ then G is not simple.

if $K \ntrianglelefteq G$ then $n_3 \equiv 1 \bmod 3$ and
$n_3 | 2^2$
$\Rightarrow$ $n_3 = 4$

$\{K_1, K_2, K_3, K_4\} = Syl_3(G)$

Note: $|K_i \cap K_j| = 1$
$|K_1 \sqcup K_2 \sqcup K_3 \sqcup K_4| = 1 + 2(4) = 9$

∴ $H \cap K_j = \phi$ ∴ $12 - 9 = \underset{\uparrow}{\underline{3}}$
new
and 1 e is H

$\Rightarrow$ $H = \{e, s_1, s_2, s_3\}$
or $\{H\} = Syl_2(G)$
∴ $H \trianglelefteq G$ ∴ G is <u>not</u> simple

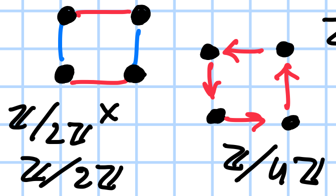
groups of small orders:

$|G| = 1 \Rightarrow G = \{e\}$

$|G| = 2 \Rightarrow G = \{1, a\}$ s.t $a^2 = 1$

$|G| = 3, 5 \Rightarrow G = \langle a \rangle$

$|G| = 4 = 2^2$
∴ G is abelian
now, $\mathbb{Z}/4\mathbb{Z} \cong G$
or
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong G$



group of order 6: $|G| = 6 = 2 \times 3$

$H = \{1, x, x^2\}$ $\quad x^3 = 1$

$K = \{1, y\}$ $\quad y^2 = 1$

$HK = G$

$G = \{1, x, x^2, y, xy, x^2y\}$

now if $yx = 1 \Rightarrow y = x^{-1} \Rightarrow x^{-1} = x^2$ ✗

$yx = x \Rightarrow y = 1$ ✗

$yx = y \Rightarrow x = 1$ ✗

$\therefore \quad yx = xy$ ——①

or $yx = x^2y$ ——②

$\therefore$ 2 cases

case ① is $\mathbb{Z}/6\mathbb{Z}$

② $yx = x^2y$ $\quad S_3$ → as $yx = x^2y$

$x^3 = 1$ and $y^2 = 1$

$(yx)(y^{-1}(x^2)^{-1})$

$= (yx)(yx)$

$= (yx)^2 = 1$

$\therefore D_3$

group of order 30: $|G| = 30 \Rightarrow G$ is not simple.

$30 = 5 \times 2 \times 3$

$n_5 = 1$ or 6

$n_3 = 1$ or 10

if $n_5 = 6$ and $n_3 = 10$

then

$1 + 4(6) + 2(10)$

$= 1 + 24 + 20$

$= 45 > 30$ $*$

$\therefore \sim(n_5 = 6$ and $n_3 = 10)$

$\therefore n_5 = 1$ or $n_3 = 1$

$\therefore H$ or $K \trianglelefteq G$

$\therefore G$ is not simple.

22nd Aug :

Automorphims :

← a fuction that is group homomonophism + bjective

$\varphi : G \longrightarrow G$

↳ isomorphism

Aut(G) ← group of all automorphism

Note : If $H \trianglelefteq G$, then

$\varphi_g : H \longrightarrow H$

$h \longrightarrow ghg^{-1}$ → this are automorphisms

here $C_G(H) = \{ g \in G \mid ghg^{-1} = h, \forall h \in H \}$

now let $\varphi' : G \longrightarrow Aut(H)$

then, $\ker(\psi') = C_G(H)$

or $G/C_G(H) \cong Aut(H)$

this is important as for $H = G$

$G/Z(G) \cong Aut(G)$

also, $\psi' : G \to Aut(H)$

$g \longrightarrow \varphi_g$

↳ s.t $h \to ghg^{-1}$

is homomorphic as

$\varphi_{g_1}\varphi_{g_2} = \varphi_{g_1 g_2}$ (H is normal)

and ψ' is surjetive (trivial)

by first isomorphism theorm, $G/\ker(\psi') \cong Aut(H)$

where $\ker(\psi') = \{ g \in G \mid \varphi_g$ are trivial$\}$

$= \{ g \in G \mid ghg^{-1} = h, \forall h \in H \}$

$= C_G(H)$

Note : Automorphism of cyclic group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

proof : Aut(Z_n)

let $Z_n = \langle x \rangle$ if $\psi \in Aut(Z_n)$

then $\psi_i(x) = x^i$ for some $i \in \mathbb{Z}$

i is only defined mod n.

as ψ_i is isomorphism, order of x and x^i same.

$\therefore (i, n) = 1$ (gcd)

$\psi : Aut(Z_n) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$

$\psi_i \longmapsto i \bmod n$

as $\psi_i \circ \psi_j(x) = \psi_i(x^j) = x^{ij} = \psi_{ij}(x)$

also surjetive and one-one

$$\therefore \quad \mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$$

Note: $(\mathbb{Z}/p^n\mathbb{Z})^{\times}$ where p is an odd prime, will have ord $\varphi(p^n) = p^{n-1}(p-1)$
$\hookrightarrow$ euler totem function

$\therefore$ if $\mathrm{Aut}(Z_p) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

ord $\mathrm{Aut}(Z_p) = p-1$
ord $(\mathbb{Z}/p\mathbb{Z})^{\times} = p-1$

Semidirect products:

let $\varphi : K \longrightarrow \mathrm{Aut}(H)$ be a homomorphism
then $\varphi(k).h = khk^{-1}$ is our defined group action.

$$(h_1,k_1)(h_2,k_2) = (h_1\, k_1 \cdot h_2,\ k_1k_2)$$

Theorem: let H, K be groups and let φ be a homomorphism from K into aut (H).
let $\cdot$ denote left action of K on H determined by φ.
G be the set of ordered pair (h,k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1,k_1)(h_2,k_2) = (h_1\, k_1 \cdot h_1,\ k_1k_2)$$

(I) This makes G into a group of order $|H||K|$.
(II) The sets $\{(h,1) \mid h \in H\} = \tilde{H}$ and $\{(1,k) \mid k \in K\} = \tilde{K}$ are subgroups of G and $H \cong \tilde{H}$, $K \cong \tilde{K}$.

(III) $\tilde{H} \trianglelefteq G$
(IV) $\tilde{H} \cap \tilde{K} = 1$
(V) $\forall\, h \in H,\ k \in K$
$khk^{-1} = k.h = \varphi(k)h$

proof:
(I) G is a group as:

$$\begin{aligned}((a,x)(b,y))(c,z) &= (a\, x\cdot b,\ xy)(c,z)\\ &= (a x\cdot b\ xy\cdot c,\ xyz)\\ &= (a,x)(b\, y\cdot c,\ yz)\\ &= (a,x)[(b,y)(c,z)]\end{aligned}$$

$\therefore$ associativity

$$\begin{aligned}(a,b)(b^{-1}.a^{-1}, b^{-1}) &= (a\ b(b^{-1}a^{-1}), 1)\\ &= (a(b.b^{-1}).a^{-1}, 1)\\ &= (a.a^{-1}, 1)\\ &= (1,1)\end{aligned}$$

$\therefore$ inverse

$(a,b)(c,d) \rightarrow$ trivial
$(a,b)(1,1) \rightarrow$ trivial

$\therefore G$ is a group denoted by

$$G = H \rtimes_{\varphi} K$$
$\nwarrow$ homomorphism from $K \longrightarrow \mathrm{Aut}(H)$

as $G = \{(h,k) \mid h \in H, k \in K\}$
$|G| =$ no of h x number of k
$|G| = |H||K|$

(II) now $\tilde{H} = \{(h,1) \mid h \in H\}$
let
$\varphi : H \longrightarrow \tilde{H}$
$h \longmapsto (h,1)$
then ① well defined $h_1 = h_2 \Rightarrow (h_1,1) = (h_2,1)$
② onto trivial
③ one-one trivial
④ homorphism $\varphi(h_1)\varphi(h_2) = (h_1,1)(h_2,1) = (h_1h_2,1) = \varphi(h_1h_2)$

$\therefore \tilde{H} \cong H$

let $\tilde{K} = \{(1,k) \mid \forall k \in K)$
similarly from above
$K \cong \tilde{K}$

(III) let $(\alpha,1) \in \tilde{H}$ and let
$g \in G$ where
$g = (h,k)$
now, $g^{-1} = (k^{-1}.h^{-1}, k^{-1})$

$$
\begin{aligned}
g(\alpha,1)g^{-1} &= (h,k)(\alpha,1)(k^{-1}.h^{-1},k^{-1}) \\
&= (h\ k\cdot\alpha, k)(k^{-1}.h^{-1},k^{-1}) \\
&= (h\ k\cdot\alpha\ \cancel{k\cdot k^{-1}}\cdot h^{-1}, 1) \\
&= (h\ k\cdot\alpha\ h^{-1}, 1)
\end{aligned}
$$

Here there is one more proof in class that is that
$K \leq N_G(\tilde{H})$
but $N_G(\tilde{H}) = G$
$\therefore \tilde{H} \trianglelefteq G$

as $k\cdot\alpha \in H$
$h \in H$
and $h^{-1} \in H$
$\Rightarrow (h\,k\cdot\alpha\,h^{-1}, 1) \in \tilde{H}$

$\therefore \tilde{H} \trianglelefteq G$

(iv) as $\tilde{H} = \{(h,1) \mid \forall h \in H\}$
and
$\tilde{K} = \{(1,k) \mid \forall k \in K\}$
then $\tilde{H} \cap \tilde{K} = \{(1,1)\}$
as $h \in H, k \Rightarrow h = 1$
and $k \in H, k \Rightarrow k = 1$
$\therefore \tilde{H} \cap \tilde{K} = 1$

(V) Trivial

Def^n: H, K be groups and let $\varphi : K \longrightarrow \mathrm{Aut}(H)$ be a homomorphism.

$G = H \rtimes_{\varphi} K$ is a semidirect group

Theorm : H, K groups

$\varphi : K \to \mathrm{Aut}(H)$ be a homorphism

the following are equivalent :

(I) $H \rtimes K \cong H \times K$

(II) φ is trivial homorphism

(III) $\tilde{K} \trianglelefteq H \rtimes K$

proof :

(1) ⇒ (2)

By defination, if $H \rtimes K \cong H \times K$ then

$$(h, k \cdot h_2, k_1 k_2) = (h_1 h_2, k_1 k_2)$$
$$\Rightarrow \quad k \cdot h_2 = h_2$$
$$\Rightarrow \quad \varphi(k) h_2 = h_2$$

$\therefore$ φ is trivial

(2) ⇒ (3) if φ is trivial, then $hk = kh$, $\forall k, h \in K, H$

and also

$$G = H \rtimes K = (h, k)$$

let $(1, k) \in \tilde{K}$

and $(h, k) \in G$, then

$$(h, k)(1, k)(k^{-1} \cdot h^{-1}, k^{-1})$$
$$= (h, k^2)(k^{-1} \cdot h^{-1}, k^{-1})$$
$$= (h, k^2)(h^{-1}, k^{-1})$$
$$= (1, k) \in \tilde{k}$$

$\therefore$ $\tilde{k} \trianglelefteq H \rtimes K$

(3) ⇒ (1) If $\tilde{k} \trianglelefteq H \rtimes K$, then

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$
$$= (h_1 k_1 h_2 k_1^{-1}, k_1 k_2)$$

as $\tilde{K} \trianglelefteq H \rtimes K$

$$(h, k)(1, \alpha)(k^{-1} \cdot h^{-1}, k^{-1}) \in \tilde{k}$$

or

$$(h, k\alpha)(k^{-1} \cdot h^{-1}, k^{-1})$$
$$= (h (k\alpha \cdot k^{-1}) \cdot h^{-1}, k\alpha k^{-1})$$

$$h(k\alpha \cdot k^{-1}) \cdot h^{-1} = 1$$

$$h(k\alpha k^{-1} h^{-1})(k \alpha^{-1} k^{-1}) = 1$$

only if $h(k\alpha k^{-1} h^{-1}) = k\alpha k^{-1}$

$$h k' h^{-1} = k'$$
$$h k' = k' h$$

$\forall$ h, k

$$\therefore (h_1, k_1)(h_2, k_2)$$
$$= (h_1 h_2, k_1 k_2)$$

construction :

group of order pq :

as group of order pq with $p<q$
$n_q = 1$, $\therefore Q \trianglelefteq G$

also for P
if $p \nmid q-1$ then
$P \trianglelefteq G$
and $G \cong Q \times P$ is abelian

but if $p \mid q-1$ then :

as $\text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^{\times}$

$\Rightarrow \text{Aut}(Q) \cong (\mathbb{Z}/q\mathbb{Z})^{\times}$

now, $\text{ord Aut}(Q) = q-1$

as $p \mid |\text{Aut}(Q)|$

$\Rightarrow \exists\, x \in \text{Aut}(Q)$ s.t
$\text{ord } x = p$

now, $\varphi : P \to \text{Aut}(Q)$
s.t φ is homomorphism
defind as $\varphi(p) = (p^{p})^{i} = p^{pi}$
for $i \in \mathbb{N}$
as $i = 0,1,2,\ldots\ldots k$
(because $p \mid q-1$)
and $\text{ord}(Q) = q-1$

for $i=1$, $\exists$ a non-trivial homomorphism

also $G = Q \rtimes P$
φ is trivial $\Leftrightarrow P \trianglelefteq G$
$\Rightarrow$ $\sim(\varphi$ is trivial$)$ $\Leftrightarrow$ $\sim(P \trianglelefteq G)$
$\Rightarrow \exists\, \varphi$ which is non-trivial $\Leftrightarrow P \ntrianglelefteq G$

$\therefore$ as for $\varphi(p) = p^{pi}$ (non trival φ)

$P \ntrianglelefteq G$
$\therefore G$ is not abelian

group of order p^3 : (Note: p is odd)

as $p \mid \text{ord } G$

$G \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

let $H = \mathbb{Z}/p^2\mathbb{Z}$ $\quad K = \mathbb{Z}/p\mathbb{Z}$

then $\text{aut}(H) = \text{aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$

$|\text{aut}(\mathbb{Z}/p^2\mathbb{Z})| = (p)(p-1)$

now $\text{ord } K = p \mid |\text{Aut}(\mathbb{Z}/p^2\mathbb{Z})|$

$\therefore \exists$ a non-trivial φ which is:

$\varphi : K \to \text{Aut}(\mathbb{Z}/p^2\mathbb{Z})$

φ is homomorphism and

φ is non-trivial.

$\therefore G = H \rtimes K \ncong H \times K$

$\therefore G$ is not-abelian

if $H = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

then $\text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$ is group of all

ψ, s.t $\psi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is isomorphism

$(a,b) \to (c,d)$

$\varphi : \text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \to GL(\mathbb{Z}/p\mathbb{Z})$

$\underset{(a,b)\to(c,d)}{\psi} \longrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

φ is one-one as:

$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

then $\psi_1 = \psi_2$

φ is onto

φ is group homomorphism

$\text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$

now, $|GL_2(\mathbb{Z}/p\mathbb{Z})| = \left| \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A \;\middle|\; \det(A) \neq 0 \text{ and } a,b,c,d \in \mathbb{Z}/p\mathbb{Z} \right\} \right|$

← not zero

total: first row (p^2-1) ← not indep

second row (p^2-p)

$\therefore |GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$
$= p(p^2-1)(p-1)$

$\therefore p \mid |GL_2(\mathbb{Z}/p\mathbb{Z})| \Rightarrow p \mid |\text{Aut}(H)|$

$\therefore G$ is not abelian

2nd sept:

Ring : $(R,+,\cdot)$

$+ : R \times R \to R$

$\cdot : R \times R \to R$

1) $(R,+)$ is an abelian group with identity zero

2) $\begin{cases} a\cdot(x\cdot y) = (a\cdot x)\cdot y \\ \exists\, 1 \in R \text{ s.t } \quad a\cdot 1 = 1\cdot a = a \end{cases}$

↳ also called identity

3) distributive

$(a)\cdot(b+c) = a\cdot b + a\cdot c$

$(a+b)\cdot c = a\cdot c + b\cdot c \quad \forall a,b,c \in R$

Ring is commutative if $\forall a,b \in R$, $a\cdot b = b\cdot a$

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \; M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \; a,b,c,d \in \mathbb{R} \right\}$

5th sept :

Division ring : Ring with identity $1 \neq 0$ and also $\forall x \in R$ s.t $x \neq 0$ has a multiplicative inverse. i.e $\exists y \in R$ s.t
$$xy = 1 = yx \text{ for } x \neq 0$$

Field : commutative division ring is called a field

Some properties:

① $0.a = 0 = a.0 \quad \forall a \in R$
② $(-a)(b) = (a)(-b) = -(ab) \quad \forall a,b \in R$
③ $(-a)(-b) = ab$
④ If R has 1, then 1 is unique

$0.a = (0+0).a$
$\Rightarrow 0.a + 0 = 0.a + 0.a$
$\Rightarrow 0 = 0.a$

Zero divisor : $a \neq 0 \in R$ is called a zero divisor if $\exists\, b \in R \neq 0$
s.t $a.b = 0$
or $b.a = 0$

Unit : u in R is called unit, if $\exists\, v \in R$ s.t
$$u.v = v.u = 1$$
Set of units in R is $R^{\times}$

Field is a commutative ring where every non-zero element is a unit

Note : A zero divisor can never be a unit

$a.b = 0$
and $a.v = 1$
then $(a.v)b = b$
$\Rightarrow (a.b)v = b$
$\Rightarrow 0.v = b$
$\Rightarrow 0 = b$ ✱

} Field has no zero divisor

Integral domain : commutative ring with identity $1 \neq 0$ and every element is not a zero divisor

Note : Any finite integral domain is a field
as $x \mapsto ax$
then this is bijective (injective is trivial, surjective because finite)
$\therefore ab = 1$
$\forall a \in R \neq 0$ $\therefore$ field

Subring : Subgroup of R which is closed under multiplication → closed under subtraction and multiplication works

Also 1 is present

Quadratic integer rings :

$D \leftarrow$ squarefree integer
$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a,b \in \mathbb{Z}\}$
if $D \equiv 1 \bmod 4$
$$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{ a + b\left(\frac{1+\sqrt{D}}{2}\right) \,\middle|\, a,b \in \mathbb{Z} \right\}$$

} subring of $\mathbb{Q}[\sqrt{D}]$

$$\mathbb{Z}[\omega] \text{ where } \omega = \begin{cases} \sqrt{D} & ; D \equiv 2,3 \bmod 4 \\ \frac{\sqrt{D}+1}{2} & ; D \equiv 1 \bmod 4 \end{cases}$$

Polynomial rings: $R[X]$

elemt $a_0 + a_1 x + a_2 x^2 + \dots\dots a_n x^n$

$\mathbb{Z}[X]$ subring of $\mathbb{Q}[x]$

Note: if $1_R = 0_R$

then $x = 1 \cdot x = 0.x = 0$

$\forall x \in R$

or $R = \{0\}$ ← zero ring/trivial ring

Note: $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$

$p = a^2 + b^2, \quad a, b \in \mathbb{Z}$

p prime ↙ iff

$p = 2$ or

$p = 1 \mod 4$

Continuous functions:

$$C[a,b] = \{f : [a,b] \to \mathbb{R} \mid f \text{ is cont}\}$$

$$f+g : [a,b] \to \mathbb{R}$$

$$(f+g)(x) = f(x) + g(x)$$

$$f \cdot g : [a,b] \to \mathbb{R}$$

$$(f \cdot g)(x) = f(x) g(x)$$

∴ $C[a,b]$ is comm. ring

Non-commutative ring example:

Hamilton Quaternions

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

$$i^2 = j^2 = k^2 = -1$$

$$ij = k \quad ji = -k$$

} non-commutative (wrt multiplication)

Note: if $u \in \mathbb{R}$ is a unit then

if $u.v = 0$

$\Rightarrow v = 0$

proof: $u \cdot x = 0$ (R is commutative)

$uv = 1$ then

$v.(u.x) = 0.v$

$\Rightarrow v.u.\,x = 0.v$

$\Rightarrow x = 0$ as $v.u = 1$

∴ unit ⇒ non-zero divisor → Best to see is

non-zero divisor ⇏ unit

$fg = 1$ ie f is a unit

$f(x) \neq 0 \;\forall x \in [0,1]$

Best example to see when is

$f : [0,1] \to \mathbb{R}$

↳ cont $f(x) = x - \frac{1}{2}$

$f\left(\frac{1}{2}\right) = 0$

∴ f is not a unit

also f is NZD (Not zero divisor)

as $fg=0$ then $g=0$

for $x \neq \frac{1}{2}$ $f(x) \neq 0$

$\therefore$

$g(x)=0$

$\forall x \in [0,1] \setminus \{1/2\}$

as $g(x) \in C[0,1]$

$g(x)$ is cont at $\frac{1}{2}$

$\therefore g(x) \equiv 0$

$\therefore$ for $f \cdot g = 0$

$\Rightarrow g=0$

$\therefore f$ is <u>NZD</u>

<u>Ring homomorphism</u>: $\varphi : \overset{\nearrow \text{Ring}}{R} \to S \to \text{Ring}$

s.t (i) $\varphi(x+y) = \varphi(x) + \varphi(y)$ $f(0)=0$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$

(iii) $\varphi(1_R) = 1_S$

<u>Note</u>: here $\varphi(1_R) = 1_S$ is for our rings which contain identity.

<u>ker φ</u>: $\ker\varphi = \{x \in R \mid \varphi(x) = 0_S\}$

<u>Note</u>: Bijective ring homomorphism is an isomorphism

<u>Note</u>: ker φ is a subring

<u>Proof</u>: As

$\ker\varphi = \{x \in R \mid \varphi(x) = 0\}$

for $x, y \in \ker\varphi$

$\varphi(x+y) = \varphi(x) + \varphi(y) = 0$

$\Rightarrow x+y \in \ker\varphi$

and $\varphi(xy) = \varphi(x)\varphi(y)$

$\Rightarrow xy \in \ker\varphi$

also $0 \in \ker\varphi$

<u>And</u>: as $rx \in \ker\varphi$

$\forall r \in R$

and $xr \in \ker\varphi$

$\forall r \in R$

ker φ is also called <u>Ideal</u>

Quotient ring of R by $I = \ker\varphi$:

R/I is also a ring

for $\varphi : R \to S$

$\bar{\varphi} : R/I \to S$

R/I

cosets will be $r + I$ for some $r \in R$

$\therefore R/I = [r_1 + I] \sqcup [r_2 + I] \sqcup \ldots.$

and also ① $[r_1 + I] + [r_2 + I] = r_1 + r_2 + I$

<u>Note</u>: ② $(r_1 + I)(r_2 + I) = r_1 r_2 + I + \underset{\in I}{r_1 I} + \underset{\in I}{r_2 I}$

$= r_1 r_2 + I$

(as $I = \ker\varphi$)

Note: R/I Quotient is a ring iff I is closed under left and right multiplication by elements of R.

I is also called ideal

Ideals: Let R be a ring and I be a subset of R.

(1) $rI \subseteq I$
then I is left ideal

(11) $Ir \subseteq I$
then I is right ideal

$(I,+) \leq (R,+)$
$a \in R, x \in I \Rightarrow a \cdot x \in I$
and $x \cdot a \in I$

If both $rI \subseteq I$ and $Ir \subseteq I$ then called an ideal

Note: $(R/I, \cdot)$ is an abelian group as

$$(a+I)\cdot(b+I) = ab+I$$

well defined check:

$$a+I = a_1+I$$
$$b+I = b_1+I$$

then $a = a_1 + x$, $x \in I$
$b = b_1 + y$, $y \in I$
$a \cdot b = a_1 b_1 + z$, $z \in I$
$\Rightarrow a \cdot b + I = a_1 b_1 + I$

Eg:
for $\mathbb{Z}$, $n\mathbb{Z}$ is an ideal as
① $n\mathbb{Z} \subseteq \mathbb{Z}$
② for $x \in n\mathbb{Z}$
$x = nq$ for some $q \in \mathbb{Z}$
and as $b.x = n(bq)$ where $bq \in \mathbb{Z}$
$\in n\mathbb{Z}$
$\therefore$ ideal

Eg: $R = \mathbb{R}[x]$
and $f(x) = a_0 + a_1 x + \cdots a_n x^n$
$J = \{(x^2+1) f(x) \mid f(x) \in R\}$

① $(J,+) \leq (R,+)$
yes
② now if $u(x) \in J$
and $t(x) \in R$
then $u(x)t(x) \in J$
here for $u(x) = (x^2+1) u_1(x)$
$u(x)t(x) \in J$
$\therefore J$ is ideal

Subring: $S \subseteq R$ is a subring of R if

(a) $1_R \in S$
(b) $(S,+) \leq (R,+)$
(c) if $a, b \in S \Rightarrow a \cdot b \in S$

Here if $\mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots \bar{9}\}$ $S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$

← Not a subring as $1_{\mathbb{Z}/10\mathbb{Z}} \notin S$

but S has a new 1_S, so it is a ring

$S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$

then

$\bar{2} \cdot \bar{6} = \overline{12} = \bar{2}$ $\qquad \bar{6} = I_S$

$\bar{4} \cdot \bar{6} = \overline{24} = \bar{4}$

$\bar{6} \cdot \bar{6} = \overline{36} = \bar{6}$

$\bar{6} \cdot \bar{8} = \overline{48} = \bar{8}$

field: A commutative ring R is a field if

1) $1_R \neq 0_R$

2) every $x \in R \setminus \{0\}$ is a unit

ie $\exists\, y \in R$ s.t

$xy = 1$

Examples

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$,

$\mathbb{Q}[\sqrt{D}]$ $\longrightarrow$ squarefree integer

field

$K[X]$ then

$\longrightarrow$ is field of polynomials over K

$K[X_1, X_2, X_3, \dots X_n]$

$x_1^2 + x_2^2 + x_3 . x_4 . . x_n$

$R = K[[X]]$ then

$\uparrow$

field

as

$f \in R$

s.t $f = \sum_{i=0}^{\infty} a_i x^i$ this is legitimate as

$\frac{1}{1-xh} = 1 + xh + x^2h^2 + \dots$

for $f(x) = 1 + 2x + 3x^2 + \dots$

$= 1 - xh$

Ring homomorphism:

R, S rings

$f : R \longrightarrow S$ ring homomorphism

if

① $f(a+b) = f(a) + f(b)$

$f(0) = 0$

② $f(ab) = f(a) f(b)$

③ $f(1_R) = 1_S$

kerf: $\ker f = \{ x \in R \mid f(x) = 0 \}$

$\ker f \leqslant (R, +)$

and $\ker f$ is ideal

9th sept :

prop : I be ideal of R

(I) $I = R$ iff I contains a unit

(II) Assume R is commutative, then R is a field iff ideals are 0 and R.

proof :

(I) ($\Rightarrow$) $I = R$ then

$1 \in I$ $\therefore$ I contains an unit

($\Leftarrow$) if I contains a unit say u, v

then $u.v = 1$

then $r = r(u.v) = (r.u).v$

as $v \in I$

and $r.u \in I$

$(r.u).v \in I$

or $r \in I$

$\therefore$ $\forall r \in R, r \in I$

$\Rightarrow R = I$

(II) R is commutative

($\Rightarrow$) If R is a field then any ideal in R will have a unit $\Rightarrow I = R$

($\Leftarrow$) If $0, R$ are only ideals of R. $v \in R$

then $(v) = R$ least

$\nwarrow$ ideal generated by v

so $1 \in (v)$

$\Rightarrow v \in R$ s.t

$1 = uv$

i.e every u is a unit

corr : R is a field then non-zero ring homorphism of R into another ring is injection.

Here as R is a field, its ideals are 0 or R.

for $\varphi : R \to S$

$\ker(\varphi)$ is also an ideal of R

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

as $\ker(\varphi) \neq R$ as that makes $S = \{0\}$

(trivial case)

$\therefore$ $\ker(\varphi) = 0$

$\Rightarrow \varphi$ is one-one

Defn : maximal ideal :

An ideal M in any arbitrary ring S is called a maximal ideal if $M \neq S$ and the only ideals containg M are M and S.

Note : If R with $1 \neq 0$, then R has a maximal ideal (from Zorn's lemma)

Partial order : $\leq$ on A

(I) $x \leq x, \forall x \in A$

(II) $x \leq y$ and $y \leq x \Rightarrow x = y$, for $x, y \in A$

(III) $x \leq y$ and $y \leq z \Rightarrow x \leq z$, $\forall x, y, z \in A$

A is non-empty partially ordered

chain : $B \subseteq A$ is called chain if

$\forall x, y \in B$

$x \leq y$ or $y \leq x$ (ordered)

upper bound : $B \subseteq A$, then $u \in A$ s.t $b \leq u$ $\forall b \in B$ is upper bound

maximal element : $m \in A$ s.t $m \leq x$ for $x \in A$ then

$m = x$

Zorn's lemma: A non-empty partial ordered set in which every chain has an upper bound then A has a <u>maximal</u> <u>element</u>

↪ A non empty S
↪ every chain has upper bound
then $\exists m$ (maximal element)

Prop: In a ring with identity every proper ideal is containd in a maximal ideal

$R \rightarrow$ Ring
$I \rightarrow$ proper ideal $(R \neq \{0\})$

S = set of all proper ideals of R containg I.
① S is non-empty
② S is partially ordered
as for $J \in S$
$J \leq J$ (ideal of J)
if $I \leq J$ and $J \leq I$ then $J = I$
also $I \leq J$ and $J \leq K$ then $I \leq K$
③ C is a chain of S, we define

$$J = \bigcup_{A \in C} A$$

↑ union of all ideals in C.

④ J <u>is ideal</u>: J is non-empty $(0 \in J)$,
if $a, b \in J$
then $A, B \in C$ s.t
$a \in A$, $b \in B$
as $A \subseteq B$ or $B \subseteq A$ (defination of chain)
$\Rightarrow a - b \in J$
so J is closed under subtraction.

if $\forall A \in C$ is closed under left multiplication, so is J
same for right multiplication, hence J is closed under multiplication. $\therefore J$ is an ideal.

⑤ If J is not a proper ideal then $1 \in J$. Then by defination
$\exists A \in C$ s.t $1 \in A$
but as A is proper
$1 \notin A$
$\Rightarrow 1 \notin J$ $\therefore J$ is proper
⑥ This means that every chain has an upper bound in S.
By zorn's lemma, S has a maximal element, therefore the maximal (proper) ideal containg I.

Prop: Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

$(\Rightarrow)$ $\quad M \subsetneq M + Ra$
$0 \neq \bar{a} \in R/M$ $\quad \Rightarrow M + Ra = R$
$1 = m + ra$
in R/M
$\bar{1} = \bar{r}\bar{a}$
so $\forall$ $\bar{a} \in R/A$, $\exists \bar{r}$ s.t
$\bar{r} \cdot \bar{a} = \bar{1}$
$\therefore R/M$ is a field.

$(\Leftarrow)$ R/M is a field, and let I, $M \subsetneq I$

now $0 \neq \frac{I}{M} \leqslant \frac{R}{M}$ $\frac{I}{M}$ is an ideal of $\frac{R}{M}$

$0 \neq \bar{\alpha} \in I/M$

$\bar{\alpha}^{-1} \bar{\alpha} = \bar{1}$ (as R/M is a field, every element α, has $\bar{\alpha}^{-1}\bar{\alpha} = 1$)

$\Rightarrow \frac{I}{M} = \frac{R}{M}$ (so $\exists$ a unit in $\frac{I}{M}$)

$\Rightarrow I = R$ $\Rightarrow \frac{I}{M} = \frac{R}{M}$

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

$\{\bar{0}, \bar{1}, \dots \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z}$

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

then $a+b \in \mathbb{Z}/p\mathbb{Z}$

and also now if $\bar{a} \neq \bar{0}$ i.e

a is not a prime then

$\gcd(a, p) = 1$

$\Rightarrow av + pu = 1$

also as $av + pu = 1$

$\Rightarrow \bar{a}\bar{v} + \overline{pu} = \bar{1}$

$\Rightarrow \bar{a}\bar{v} = \bar{1}$

$\therefore$ $\mathbb{Z}/p\mathbb{Z}$ is a field

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

$p\mathbb{Z}$ is the maximal ideal

Also $\frac{\mathbb{R}[X]}{(x^2+1)} = \mathbb{C}$ as $\mathbb{C}$ is a field

(x^2+1) is a maximal ideal of $\mathbb{R}[X]$

Defn: Prime ideal:

R is commutative, Ideal P is prime ideal if $P \neq R$

ab of $a, b \in R$ is in P

then $a \in P$ or $b \in P$

$ab \in P$

$\Rightarrow a \in P$ or $b \in P$

Not true generally

$p\mathbb{Z}$'s prime ideals in $\mathbb{Z}$

also the maximal ideal as $\mathbb{Z}/p\mathbb{Z}$ is field

Prop: R is commut, P is a prime ideal in R iff R/P is integral domain.

→ no zero divisors

→ or if $ab = 0$ then $a = 0$ or $b = 0$ $\forall a, b \in R$

$(\Rightarrow)$ if $\bar{b}, \bar{a} \in R/P$ s.t $\bar{a}.\bar{b} = 0$

then $\Rightarrow a.b \in P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

$\Rightarrow R/P$ is integral domain

$(\Leftarrow)$ $a, b \in R$

and if $\bar{a}\bar{b} = 0$

then $\bar{a} = 0$

or $\bar{b} = 0$

$\Rightarrow$ $a \in P$ or $b \in P$

Note: If R is comm, then maximal ideal $\Rightarrow$ prime ideal

as maximal ideal,

R/I is a field

$\Rightarrow R/I$ an integral domain

$\Rightarrow I$ to be a prime ideal

Note: integral domain $\not\Rightarrow$ field

Integral domain – A comutative ring $R \neq \{0\}$ is said to be a domain if

$$ab=0 \Rightarrow a=0 \text{ or } b=0$$

$\mathbb{Z}$ is a domain
as $ab=0$
$\Rightarrow a=0$ or $b=0$

field is a domain (As multiplicative inverse present)

$ab=0$
$\Rightarrow a^{-1}(ab)=0$
$\Rightarrow a^{-1}(0)=0$
$\Rightarrow (a^{-1}a)b=0$
$\Rightarrow b=0$

$\mathbb{Z}/6\mathbb{Z}$
$\bar{2}\neq 0$
$\bar{3}\neq 0$
but $\bar{2}.\bar{3}=\bar{6}=\bar{0}$
$\therefore$ $\mathbb{Z}/6\mathbb{Z}$ not a domain

$K[X]$ is a domain
$f(x)\neq 0 = a_n x^n + \cdots\cdots$
$g(x)\neq 0 = b_m x^m + \cdots\cdots$
$f(x)g(x) = a_n b_m x^{n+m} + \cdots\cdots$
as $a_n\neq 0, b_m\neq 0$
$\Rightarrow a_n b_m \neq 0$
and $\sim(f(x)\neq 0, g(x)\neq 0 \Rightarrow f(x)g(x)\neq 0)$
is same as
$f(x)g(x)=0 \Rightarrow f(x)=0$ or $g(x)=0$
$\therefore$ $K[X]$ is a domain

Defn: An ideal M of R is said to be a maximal ideal of R if
1) $M\neq R$
2) $M\subseteq I \Rightarrow I=M$ or $I=R$
$I \trianglelefteq R$

Propn: M is maximal ideal iff R/M is a field.

($\Rightarrow$) If M is a maximal ideal, then $\exists\, a\in R$ s.t $a\notin M$ $(a\in R/M)$

$0\neq \bar{a}\in R/M$ then
$M \subsetneq M+Ra$
$\Rightarrow M+Ra=R$

Note $I\leq R$,
$J\leq R$
then $I+J=\{i+j\}\leq R$
and $a\in R$
$\Rightarrow Ra=\{ra \mid r\in R\}\leq R$
$\therefore$ Ra is an ideal
and $M+Ra$ is an ideal

and $M+aR=R$
$\Rightarrow m+ar=1$
as $1\in R$
$\Rightarrow \bar{a}\bar{r}=\bar{1}$
for $\bar{a},\bar{r}\in R/M$
now as $\bar{a}\bar{r}=\bar{1}$
$\bar{r}=(\bar{a})^{-1}$
or every a in R/M

($\Leftarrow$) R/M is a field
$M\subsetneq I$ Any ideal
and $\therefore 0\neq \frac{I}{M}\trianglelefteq \frac{R}{M}$
but as $\frac{R}{M}$ is a field
if $\bar{\alpha}\in \frac{I}{M}$
then $r\bar{\alpha}\in \frac{I}{M}$
$\forall\, r\in R/M$
for, $r=\bar{\alpha}^{-1}$
$\Rightarrow \bar{\alpha}^{-1}\bar{\alpha}\in \frac{I}{M}$
$\Rightarrow 1\in \frac{I}{M}$

as $1\in \frac{I}{M}$, $r\in R/M \Rightarrow r.(\bar{\alpha}^{-1}.\bar{\alpha})=(r\bar{\alpha}^{-1}).(\bar{\alpha})\in \frac{I}{M}$

∴ $r \in I/M$, $\forall R/M$

$\Rightarrow \frac{I}{M} = \frac{R}{M}$

<u>Note</u>: $\underbrace{\mathbb{Z}/p\mathbb{Z} \text{ is a field}}$ $\Leftrightarrow$ $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$

this we know, so $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$

(x^2+1) ← ideal generated by $\mathbb{R}[X]$, then $\frac{\mathbb{R}[X]}{(x^2+1)} = \mathbb{C}$

<u>Prime Ideal</u> - An ideal P of R is said to be a prime ideal of R if

1) $P \neq R$
2) $ab \in P \Rightarrow a \in P$ or $b \in P$

$p\mathbb{Z}$ is a prime ideal as if $ab \in p\mathbb{Z}$

$\Rightarrow ab = pm$

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

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

Also $\{0\}$ is a trivial prime ideal $\mathbb{Z}$

<u>propn</u>: P is a prime ideal in R $\Leftrightarrow$ R/P is an integral domain

(⇒) P is a prime ideal then if $\bar{a} \in R/P$, $\bar{b} \in R/P$ s.t $\bar{a}\bar{b} = \bar{0}$

then $ab \in P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

i.e R/P is a domain

(⇐) R/P is a domain, then

if $\bar{a}\bar{b} = 0$

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

now if $\bar{a}\bar{b} = 0$

$\Rightarrow ab \in P$

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

$\Rightarrow a \in P$ or $b \in P$

∴ $ab \in P \Rightarrow a \in P$ or $b \in P$

∴ P is prime ideal

<u>Poset</u>: $\leq$ relation

(i) $x \leq x$
(ii) $x \leq y$, $y \leq z$ $\Rightarrow x \leq z$

<u>Note</u>: if $(E, \leq)$ is a poset then $A \subseteq E$ we say $u \in E$ is an upper boud of A if $a \leq u$ $\forall a \in A$

<u>chain</u>: $\{e_\alpha\}_{\alpha \in \Lambda}$ is a <u>chain</u> in E if $\forall \alpha, \beta \in \Lambda$ then either $e_\alpha \leq e_\beta$ or $e_\beta \leq e_\alpha$

<u>Zorn's lemma</u> - $E \neq \phi$ $\leq$ partial order in E
- every chain has an upper bound

Then E has a maximal element ($u \in E$ st $u \leq x \Rightarrow u = x$)

<u>Theorm</u>: if $R = \{0\}$, then R has maximal ideal

<u>proof</u>: $\mathcal{E} = \{ I \mid I \text{ is ideal of } R, I \neq R \}$ → proper ideals

$\{0\} \in \mathcal{E}$ ∴ $\mathcal{E}$ is non-empty also ideals containg I

$I \leq J$ if $I \subseteq J$

$\{I_\alpha\}_{\alpha \in \Lambda}$ is chain in $\mathcal{C}$

now $\bigcup_{\alpha \in \Lambda} I_\alpha = J$

$0 \in J$, if $x, y \in J$

then $x \in I_\alpha$

$y \in I_\beta$

as $I_\alpha \subseteq I_\beta$

or $I_\beta \subseteq I_\alpha$

$x + y \in J$

$\Rightarrow (J, +) \leq (R, +)$

now, $r \in R$

$x \in J$

then $x \in I_\alpha$ for some α

$\Rightarrow rx \in I_\alpha$

$\Rightarrow rx \in J$

then $\bigcup_{\alpha \in \Lambda} I_\alpha = J$

$\uparrow$

J is also an ideal

if $J = R$

then $1 \in J = \bigcup_{\alpha \in \Lambda} I_\alpha$

then $\exists\, \alpha \in \Lambda$ s.t

$1 \in I_\alpha$

$\Rightarrow r.1 \in I_\alpha$

$\Rightarrow R = I_\alpha$ $\divideontimes$

$\therefore J \neq$

$\therefore J$ is the upper boud of $\{I_\alpha\}_{\alpha \in \Lambda}$

$\therefore \exists$ a maximal ideal M.

Def^n: Multiplicative closed set (m.c)

$R \neq \{0\}$

$S \subseteq R$ is m.c set

if 1) $1_R \in S$

2) $0_R \notin S$

3) $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$

examples of multiplicative sets:

$\mathbb{Z} - \{0\}$, $S = \{1, n, n^2, \ldots\ldots\}$

$n \geq 2$

$S = \mathbb{Z} \setminus p\mathbb{Z} = \mathbb{Z} - \{p\mathbb{Z}\}$

$= \{n \mid p \nmid n\}$

as $p \nmid 1$

$\Rightarrow 1 \in S$

also, as $p \mid 0$

$0 \notin S$

and if $p \nmid m$ and

$p \nmid n$ then

$mn \in S$

as $p \nmid mn$

Theorm: Let $R \neq 0$, S is a m.c in R. Then $\exists P$ prime in R s.t $P \cap S = \phi$

proof:

$\mathcal{C} = \{I \mid I \cap S = \phi\}$

$\{0\} \in \mathcal{C}$ ($\mathcal{C}$ is non-empty)

Let $I \leq J$ if $I \subseteq J$

ideals containg I

$\{I_\alpha\}_{\alpha \in \Lambda}$ is a chain

$$J = \bigcup_{\alpha \in \Lambda} I_\alpha$$

then as $I_\alpha \cap S = \phi \ \forall \alpha \in \Lambda$

$\Rightarrow J \cap S = \phi$

then Q be maximal elent in $\mathcal{C}$.

$ab \in Q$

and suppose $a \notin Q$ and $b \notin Q$ then

(using similar arg before)

$Q \subsetneq Q + aR$

and $Q \subsetneq Q + bR$

Note: $Q + aR, Q + bR \notin \mathcal{C}$

$\Rightarrow (Q + aR) \cap S \neq \phi$

and

$(Q + bR) \cap S \neq \phi$

$s_1 = u + ar \quad u \in Q$

$s_2 = v + bs \quad v \in Q$

$$s_1 s_2 = (u + ar)(v + bs)$$

$$= \underset{\in Q}{uv} + \underset{\in Q}{ubs} + \underset{\in Q}{arv} + \underbrace{arbs}_{\in Q}$$

but as $Q \cap S = \phi$, $s_1 s_2 \in Q$ $\quad *$

$\therefore$ if $ab \in Q$

$a \in Q$ or $b \in Q$

$\therefore Q$ is a prime ideal

10th sept -

Ring direct product - $R_1, R_2 \leftarrow$ two rings
$R_1 \times R_2$ (diret product)
$= \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$

① $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$

② $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$

③ $\bar{0}_R = (0_{R_1}, 0_{R_2})$

④ $1_R = (1_{R_1}, 1_{R_2})$

Defn: $A, B \xleftarrow{\text{ideals}}$ of R then A, B are comanial if $A + B = R$

Theorm: chinese remainder theorm, Let $A_1, \dots, A_k$ be ideals in R.
$R \to R/A_1 \times R/A_2 \cdots \times R/A_k$
$r \mapsto (r + A_1, r + A_2, \dots, r + A_k)$
is a ring homorphism with kernal $A_1 \cap A_2 \cap \cdots \cap A_k$

if A_i, A_j are comanial
then $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \dots A_k$
i.e surjetive map

$$\frac{R}{A_1 A_2 \dots A_k} = \frac{R}{A_1 \cap A_2 \cap \cdots A_k} \cong \frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \frac{R}{A_k}$$

proof:
for $k=2$, then induction follows
$A = A_1$
$B = A_2$
$\varphi : R \to \frac{R}{A} \times \frac{R}{B}$
$\varphi(r) = (r + A, r + B)$

now,
① well defined:
$r_1 = r_2$
then $r_1 + A = r_2 + A$
and $r_1 + B = r_2 + B$
$\therefore \varphi(r_1) = \varphi(r_2)$
$\therefore$ well defined.

② $\varphi(r_1) + \varphi(r_2) = (r_1 + A, r_1 + B) + (r_2 + A, r_2 + B)$
$= (r_1 + r_2 + A, r_1 + r_2 + B)$
$= \varphi(r_1 + r_2)$

③ $\varphi(r_1)\varphi(r_2) = (r_1 + A, r_1 + B)(r_2 + A, r_2 + B)$
$= (r_1 r_2 + \underbrace{Ar_2 + r_1 A + A}_{\in A}, r_1 r_2 + B)$
$= (r_1 r_2 + A, r_1 r_2 + B)$

$\therefore \varphi$ is a ring homophism

now,
$\ker(\varphi) = \{r \in R \mid (r + A, r + B) = (A, B)\}$
i.e $r \in A$ and $r \in B$
$= A \cap B$

now if $A+B=R$

and A, B are proper ideals then

$1 \notin A, \; 1 \notin B$

and so

$\exists \, x \in A, \; y \in B$

s.t $x+y=1$

$\varphi(x) = (0,1)$ $\quad$ ($\because$ if $x \in A$ and $x+y=1 \Rightarrow x=1-y \Rightarrow x \in 1+B$)

$\varphi(y) = (1,0)$

now (r_1+A, r_2+B) is an arbitrary element in $\frac{R}{A} \times \frac{R}{B}$

$$\begin{aligned}\varphi(r_1 y + r_2 x) &= \varphi(r_1 y) + \varphi(r_2 x) \\ &= \varphi(r_1)(1,0) + \varphi(r_2)(0,1) \\ &= (r_1 + A, 0) + (0, r_2 + B) \\ &= (r_1 + A, r_2 + B)\end{aligned}$$

$\therefore \forall \left(r_1 + A, \; r_2 + B\right) \in \frac{R}{A} \times \frac{R}{B}$

we have $r_1 y + r_2 x$ s.t

$\varphi(r_1 y + r_2 x) = (r_1 + A, r_2 + B)$

$\therefore$ surjective

$$\therefore \frac{R}{A} \times \frac{R}{B} \cong \frac{R}{A \cap B}$$

Now, for $c \in A \cap B$

$c = c \cdot 1 = c(x+y)$

$= cx + cy \quad \in AB$

as $c \in B$ and $x \in A$

and $c \in A$ and $y \in B$

$\therefore \; A \cap B \subseteq AB$

also $AB \subseteq A \cap B$ as

for $x \in AB$

$\exists \, a, b \in A, B$

s.t $x = ab$

also as $a(b) \in B$

and $(a) \cdot b \in A$

$\Rightarrow x \in A \cap B$

$\therefore \; AB \subseteq A \cap B$

then $AB = A \cap B$

now for k,

suppose $n=k$ is true

if $\underbrace{A_0, \; A_1 A_2 A_3} \ldots A_k$ $\qquad$ (the induction step is weak)

are coaxial we are done

$\forall \, i \in \{1, 2, \ldots k\}$

$\exists \, x_i \in A_0$ and $y_i \in A_i$

s.t $x_i + y_i = 1$ (given)

now,

$x_i + y_i \in y_i + A_0$

$\prod_{i=1}^{k} (x_i + y_i) \in \prod y_i + A_0$

or $1 = (x_1 + y_1) \cdots\cdots (x_k + y_k)$

element in $A_0 + (A_1 A_2 \ldots\ldots A_k)$

or $A_0 + A_1 A_2 \ldots\ldots A_k$ contains a unit

$\therefore A_0 + A_1 A_2 \ldots A_k = R$

Product of rings: $R_1, R_2, \ldots\ldots R_s$ rings

$R = R_1 \times R_2 \times \cdots R_s$

$(r_1, r_2, \ldots r_s) + (r_1', r_2', \ldots r_s') = (r_1 + r_1', r_2 + r_2', \ldots\ldots r_s + r_s')$

$(r_1, r_2, \ldots r_s) \cdot (r_1', r_2', \ldots r_s') = (r_1 r_1', r_2 r_2', \ldots\ldots r_s r_s')$

$\bar{0}_R = (0_{R_1}, 0_{R_2}, \ldots\ldots 0_{R_s})$

$1_R = (1_{R_1}, 1_{R_2}, \ldots\ldots 1_{R_s})$

Co-Maxial ideals -

I, J are said to be comaxial if $I + J = R$

$I + J = \{i + j \mid i \in I, j \in J\}$

Chinese remainder theorm - I, J are comaxial ideals

① $\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}$

② $I \cap J = IJ$

proof: $\varphi : R \longrightarrow R/I \times R/J$

$r \longmapsto (r + I, r + J)$

$\ker \varphi = I \cap J$

$R/I \cap J \hookrightarrow R/I \times R/J$

as $\varphi(r) = (r + I, r + J)$

and $\exists\, x, y \in I, J$

s.t

$x + y = 1$

$\varphi(x) = (1 - y + I, 1 - y + J)$

$= (I, 1 + J)$

$\varphi(y) = (1 + I, J)$

now $(r + I, s + J)$

$\varphi(rx + sy) = (r + I, s + J)$

$\therefore$ surjetive

now by I^{st} isomorphism theorm

$\frac{R}{I} \times \frac{R}{J} \cong \frac{R}{I \cap J}$

now, $I \cap J = IJ$ proof:

if $x \in IJ$

then $\exists\, a \in I, b \in J$

s.t $x = ab$

then as $ab \in IJ$

and $b \in J$

we know J is ideal so $ab \in J$

similarly $ab \in I$

$\therefore IJ \subseteq I \cap J$

now, if $x \in I \cap J$

then $x \in I$ and $x \in J$

and $I + J = R$

$1 = i + j$

$x = x \cdot i + x \cdot j \Rightarrow x \in IJ$ $\therefore IJ = I \cap J$

as $x \cdot i \in IJ$

as $i \in I$ or J and $x \cdot j \in IJ$

Lemma : P is a prime ideal, then
$P \supseteq IJ \Rightarrow P \supseteq I$ or $P \supseteq J$

proof : let $IJ \subseteq P$ and $I \not\subseteq P$, $J \not\subseteq P$
if this happens then
$\exists\, a \in I - P$
and $b \in J - P$
s.t $ab \in IJ \subseteq P$
$\Rightarrow ab \in P$
$\Rightarrow a \in P$ or $b \in P$ *
$\therefore$ if $IJ \subseteq P$
then $I \subseteq P$
or $J \subseteq P$

Now, if $I + J = R \Rightarrow I^{100} + J^{250} = R$
then if $IJ \subseteq P$
then $I \subseteq P$ or $J \subseteq P$

As if $I^{100} + J^{250} \neq R$
then $I^{100} + J^{250} \subseteq M \leftarrow$ maximal ideal (we know that maximal ideal is prime)
$\Rightarrow I^{100} \subseteq M$
and $J^{250} \subseteq M$
also as M is prime
and if $XY \subseteq M$
$\Rightarrow X \subseteq M$ or $Y \subseteq M$
here $X^2 \subseteq M$
$\Rightarrow X \subseteq M$

for us $I^{100} \subseteq M \Rightarrow I \subseteq M$
and $J^{100} \subseteq M \Rightarrow J \subseteq M$
but as $I + J = R \not\subseteq M$ *
$\therefore I^{100} + J^{250} = R$

Ring of fractions

comm ring R is always a subring of larger ring Q
$\uparrow$
every non-zero divisor of R is unit of Q
if we do this to integral domain $\Rightarrow$ Q to be a field (field of fractions/ quotient field)

$\mathbb{Z} \subseteq \mathbb{Q}$

$$\underset{\substack{\uparrow \\ \text{prime}}}{\mathbb{Z}_p} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid b \right\}$$

$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$
$p \nmid b,\ p \nmid b'$
$\Rightarrow p \nmid bb'$
$\therefore \frac{a}{b} + \frac{a'}{b'} \in \mathbb{Z}_p$
also $\frac{a}{b}\frac{a'}{b'} \in \mathbb{Z}_p$
$\therefore \mathbb{Z}_p$ is a ring

$p\mathbb{Z}_p = \left\{ \frac{a}{b} \;\middle|\; p \mid a,\ p \nmid b \right\}$
$\uparrow$
unique maximal ideal in $\mathbb{Z}_p$
$p\mathbb{Z}_p \subsetneq I \subseteq \mathbb{Z}_p$
then $\leftarrow$ ideal in $\mathbb{Z}_p$
s.t $p\mathbb{Z}_p \subsetneq I \subseteq \mathbb{Z}_p$
$\uparrow$
$p\mathbb{Z}_p$ contained in I
but not I
then $\exists\, a \in I - p\mathbb{Z}_p$

as $\alpha \in I - p\mathbb{Z}_p \in \mathbb{Z}_p$

$\alpha = \frac{a}{b}$ s.t $p \nmid a$ and $p \nmid b$

but as $\frac{b}{a}$, $p \nmid a \Rightarrow \frac{b}{a} \in \mathbb{Z}_p$

then as $\frac{b}{a} \in \mathbb{Z}_p$

$\frac{a}{b} \in I$

$\Rightarrow 1 \in I$

$\Rightarrow I = \mathbb{Z}_p$

Because of this $p\mathbb{Z}_p$ is unique maximal ideal where

$\mathbb{Z}_p = \left\{ \frac{a}{b} \middle| p \nmid b \right\}$

$p\mathbb{Z}_p = \left\{ \frac{a}{b} \middle| \begin{matrix} p \mid a \\ p \nmid b \end{matrix} \right\}$

$\therefore$ $p\mathbb{Z}_p$ is a maximal ideal.

if $I \trianglelefteq \mathbb{Z}_p$ and $I \subsetneq \mathbb{Z}_p$

then $\exists \alpha \in I$ s.t

$\alpha = \frac{a}{b}$ $p \nmid b$

as $1 \notin I$

$\frac{b}{a} \notin I \Rightarrow p \mid a$

$\therefore I = p\mathbb{Z}_p$

$\therefore$ Maximal ideal + unique

Defn: A ring is said to be local if R has a unique maximal ideal m.

Example $\mathbb{Z}_p$

as $p\mathbb{Z}_p$ is a unique maximal ideal

Ring of fractions -

$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$

$\mathbb{Z} \times \mathbb{Z}^*$ $\quad \mathbb{Z} \hookrightarrow \mathbb{Q}$

$(a,b) \sim (a',b')$ if $ab' = ba'$

$\frac{a}{b}$

$1 \in \mathbb{Z}^*$, $0 \notin \mathbb{Z}^*$, $u,v \in \mathbb{Z}^* \Rightarrow uv \in \mathbb{Z}^*$

Note - $S \subseteq R$ is m.c if

1) $1_R \in S$
2) $0_R \notin S$
3) $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$

$R \times S = \{(r,s) \mid r \in R, s \in S\}$

$(r,s) \sim (r',s')$

$\frac{r}{s} = \frac{r'}{s'}$

if $rs' = r's$

$R \times S / \sim$

$\left[\frac{r}{s}\right] + \left[\frac{r_1}{s_1}\right] = \left[\frac{rs_1 + sr_1}{ss_1}\right]$

$\left[\frac{r}{s}\right]\left[\frac{r'}{s'}\right] = \left[\frac{rr'}{ss'}\right]$

$S^{-1}R = R \times S / \sim$

$\varphi : R \longrightarrow S^{-1}R$

$r \longmapsto \left[\frac{r}{1}\right]$

φ is 1-1 ring homomorphism

12th sept :

Ring of fractions -

Note: if a is not a zero divisor and $ab = ac$ then
$\Rightarrow a(b-c)=0$
$\Rightarrow b-c=0$
$\Rightarrow b=c$

} something not being a zero divisor still enjoys some properties of a unit.

we want to show/construct a 'new' ring Q, from a commutative ring by making NZD to ideals.

so if $R \leftarrow$ integral domain $\Rightarrow Q \leftarrow$ field (units)
$\uparrow$ field of fractions/Quotient field

$\mathbb{Z} \rightarrow \mathbb{Q}$ ↪ construction of $\mathbb{Q}$ from $\mathbb{Z}$

$\frac{1}{2} = \frac{2}{4} = \cdots$

$\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$

or $(a,b) \sim (c,d) \Leftrightarrow ad = bc$

now, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

Note: we cannot do this for any R as if b is zero/zero divisor and $bd = 0$ then $d = \frac{d}{1} = \frac{db}{b} = \frac{0}{b} = 0$ (Not true)
(This is a restriction)
i.e R cannot have zero divisors or Q collapses

Second restriction - if b, d are allowed to be denominators then bd also should be a denominator.

These two restrictions are sufficient for "ring of fractions"

$\mathbb{Z}^* = \mathbb{Z}\setminus\{0\} = \mathbb{Z} - \{0\}$

$\mathbb{Z} \times \mathbb{Z}^*$

$(a,b) \sim (a',b')$
iff $ab' = ba'$
also $1 \in \mathbb{Z}^*$
$0 \notin \mathbb{Z}^*$
$u, v \in \mathbb{Z}^* \Rightarrow uv \in \mathbb{Z}^*$

$R \times \overset{\text{m.c}}{S} = \{(r,s) \mid r \in R, s \in S\}$ and $\underset{\frac{r}{s}}{(r,s)} \sim \underset{\frac{r'}{s'}}{(r',s')}$

if $s_1 r = s r_1$

$R \times S/\sim$

$\left[\frac{r}{s}\right] \leftarrow$ equivalence class of $\frac{r}{s}$

$\left[\frac{r}{s}\right] + \left[\frac{r_1}{s_1}\right] = \left[\frac{rs_1 + sr_1}{ss_1}\right]$

and $S^{-1}R = R \times S/\sim$

$\left[\frac{r}{s}\right]\left[\frac{r'}{s'}\right] = \left[\frac{rr'}{ss'}\right]$

$S^{-1}R = R \times S/\sim$

$\varphi : R \longrightarrow S^{-1}R$

$r \longmapsto \left[\frac{r}{1}\right]$

φ is 1-1 ring homomorphism as ① $\varphi(r_1+r_2)$

$= \left[\frac{r_1+r_2}{1}\right]$

$= \left[\frac{r_1}{1}\right] + \left[\frac{r_2}{1}\right]$

$= \varphi(r_1) + \varphi(r_2)$

② $\varphi(r_1 r_2) = \left[\frac{r_1 r_2}{1}\right] = \left[\frac{r_1}{1}\right] . \left[\frac{r_2}{1}\right]$

and as $\ker \varphi = \{0\}$

$\Rightarrow \varphi$ is 1-1

Now $\mathbb{Z}$, $\mathbb{Q}$

$\mathbb{Z} \times \mathbb{Z}^*$ $\quad \mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim$

$[(a,b)].[(c,d)] = [(ac, bd)]$

$[(a,b)]+[(c,d)] = [(ad+bc, bd)]$

Now if $S \subseteq R$, S is m.c and R is domain then:

$R \times S$

$(a, s_1) \sim (b, s_2)$ if $a s_2 = b s_1$

$\sim$ is an equivalence relation on $R \times S$

as ① $(a,s_1) \sim (a,s_1)$ is trivial

② $(a,s_1) \sim (b,s_2)$

then $(b,s_2) \sim (a,s_1)$ trivial

③ $(a,s_1) \sim (b,s_2) \sim (c,s_3)$

$\Rightarrow (a,s_1) \sim (c,s_3)$ trivial

now, $S^{-1}R = R \times S/\sim$

i.e $\frac{a}{s} := [(a,s)]$

where $\left[\frac{a_1}{s_1}\right] + \left[\frac{a_2}{s_2}\right] = \left[\frac{s_2 a_1 + s_1 a_2}{s_1 s_2}\right]$

$\left[\frac{a_1}{s_1}\right] . \left[\frac{a_2}{s_2}\right] = \left[\frac{a_1 a_2}{s_1 s_2}\right]$

$\varphi : R \to S^{-1}R$ $\quad \frac{s}{1} \in S^{-1}R$ and $\frac{1}{s} \in S^{-1}R$

$r \mapsto \left[\frac{r}{1}\right]$

$\therefore \forall s$ is invertible in $S^{-1}R$

ideal of R

now, $I \trianglelefteq R$

then $IS^{-1}R$ (i.e $I(R \times S/\sim)$)

$= \left\{\frac{i}{s}, i \in I, s \in S\right\}$

as $\frac{r}{s} \in S^{-1}R$ and I is ideal of R then

$\forall i \in I$ $\quad i.r \in I$

$\therefore IS^{-1}R = \left\{ \frac{i}{s} \,\middle|\, i \in I, s \in S \right\}$

$\varphi : A \to B$ $\quad \varphi$ is a ring homomorphism

$I \trianglelefteq A$ $\quad IB = \{$ finite sum $\varphi(i) b_i \mid i \in I, b_i \in B\}$

I is ideal of A $\quad \varphi(i)\, b_i \leftarrow$ from B $\quad I \rightrightarrows i \leftrightarrow B$

↑ from ideal

$U = \left\{ \frac{i}{s} \,\middle|\, i \in I, s \in S \right\}$ then $U = IS^{-1}R$

$U \subseteq IS^{-1}R$

$\varphi : R \to S$

$\left(I \subseteq R \to IS^{-1}R = \text{finite sum} \right)$

$\left(\varphi : A \to B \right.$

$I \subseteq A \to IB = \text{finite sum}$

$\swarrow B = S^{-1}R$

$\nearrow IS^{-1}R = I(B) = \text{finite sum}$

$a \in IS^{-1}R$

then $a = \frac{i_1}{1} \cdot \frac{r_1}{s_1} + \frac{i_2}{1} \frac{r_2}{s_2} + \dots \frac{i_m}{1} \cdot \frac{r_m}{s_m}$ ↙ finite sum

$= \frac{\theta}{s_1 s_2 \dots s_m}$ $\theta \in I$, $s_1 s_2 \dots s_m \in S$

$\Rightarrow a \in U$

$\Rightarrow U = IS^{-1}R$

(this is proof of $U = IS^{-1}R$ using $IB = \{\text{finite sum}\}$)

Theorem: There is a bijection

$\left\{ \begin{matrix} \text{prime ideals } P \text{ of } R \\ P \cap S = \phi \end{matrix} \right\} \longleftrightarrow \{ \text{Prime ideals of } S^{-1}R \}$

$\left(\begin{matrix} P \longrightarrow PS^{-1}R \\ \theta \cap R \longleftarrow \theta \end{matrix} \right)$ → one-one → one-one

proof: ① $PS^{-1}R \neq S^{-1}R$

as if $PS^{-1}R = S^{-1}R$

$\frac{1}{s} \in PS^{-1}R = \left\{ \frac{u}{t} \,\middle|\, u \in P, t \in S \right\}$

$\frac{1}{s} = \frac{u}{t}$

$t = us$

as $t \in S$

$us \in S$

and as $u \in P$

$us \in P$

so, $us \in S$ and P

$\Rightarrow us \in P \cap S = \phi$

$\therefore us = \phi$ $*$

$\therefore PS^{-1}R \neq S^{-1}R$

now, $PS^{-1}R = \left\{ \frac{u}{s} \,\middle|\, u \in P, s \in S \right\}$

if $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \in PS^{-1}R$

$\frac{a_1 a_2}{s_1 s_2} = \frac{u}{s}$ $u \in P, s \in S$

$\underbrace{s}_{\in S} \underbrace{a_1 a_2}_{\in P} = \underbrace{u}_{\in P} \underbrace{s_1 s_2}_{\in S} \in P$

as $S \cap P = \phi$

when $a_1 a_2 s \in P$

$\Rightarrow a_1 a_2 \in P$

$\Rightarrow a_1 \in P$ or $a_2 \in P$

$\Rightarrow \frac{a_1}{s_1} \in PS^{-1}R$ or $\frac{a_2}{s_2} \in PS^{-1}R$

this means that $\underset{\substack{\uparrow \\ \text{prime ideal}}}{P} \longrightarrow PS^{-1}R$ ↖ $PS^{-1}R$ is a prime ideal now to show $\Theta \cap R \leftarrow \Theta \swarrow$ Prime ideal in $S^{-1}R$

lemma: $J \trianglelefteq S^{-1}R$
$(J\cap R)S^{-1}R = J$

proof:
Note $(J\cap R)S^{-1}R \subseteq J$
as $x \in (J\cap R)S^{-1}R$
then $J\cap R \in J$
and $JS^{-1}R \in J$
so, $x \in J$
$\therefore (J\cap R)S^{-1}R \subseteq J$ —— ①

now if $x = \frac{j}{s} \in J$
$sx = \frac{j}{1} \in J$
$j \in J\cap R$
so $\frac{j}{s} \in (J\cap R)S^{-1}R$
$\Rightarrow x \in (J\cap R)S^{-1}R$ —— ②

$\therefore (J\cap R)S^{-1}R = J$

To show: $(PS^{-1}R)\cap R = P$

proof: Note: $P \trianglelefteq R$
and now $\underset{=J}{PS^{-1}R} \trianglelefteq S^{-1}R$
$PS^{-1}R = \left\{ \frac{u}{s} \mid u \in P, \ s \in S \right\}$
$\frac{u}{1} = s.\frac{u}{s} \in PS^{-1}R$
$u \in (PS^{-1}R)\cap R$
i.e $u \in P \Rightarrow u \in (PS^{-1}R)\cap R$
$\Rightarrow P \subseteq (PS^{-1}R)\cap R$ —— ①

now, $a \in (PS^{-1}R)\cap R$
$\frac{a}{1} = \frac{u}{s}$ $u \in P, s \in S$
$sa = u \in P$
but $s \notin P$ as $P \cap S = \phi$ (given)
$\Rightarrow a \in P$ —— ②
$\Rightarrow (PS^{-1}R)\cap R = P$
from ①, ②

now $\underset{\substack{\uparrow \\ \text{prime} \\ \text{in } S^{-1}R}}{\Theta} \longrightarrow \underset{\substack{\uparrow \\ \text{prime in} \\ R}}{\Theta \cap R}$

for this as $\Theta \trianglelefteq S^{-1}R$
$(\Theta\cap R)S^{-1}R = \Theta$ (from lemma)

and,
$\Theta\cap R = [(\Theta\cap R)S^{-1}R]\cap R$ (check for $\Theta\cap R$ is prime ideal)

as $P \trianglelefteq R \Rightarrow PS^{-1}R \cap R = P$
for $\Theta\cap R = P$ $P = (PS^{-1}R)\cap R$

$\therefore$ $\Theta \cap R$ is prime ideal for P

$$\begin{tikzcd}
\therefore \quad \Theta \arrow[r] & \Theta \cap R \\
\text{Prime in } S^{-1}R \arrow[u] & \text{Prime in } R \arrow[u]
\end{tikzcd}$$

$\therefore$ By $P \longrightarrow PS^{-1}R$
$\Theta \cap R \longleftarrow \Theta$

$\left\{ \begin{array}{l} \text{Prime ideal of } R \\ \text{s.t } P \cap S = \phi \end{array} \right\} \longleftrightarrow \{ \text{Prime ideals of } S^{-1}R \}$

<u>Examples</u>:

1) $S = \{1, f, f^2, f^3, \dots f^n \dots\}$

$S^{-1}R = R_f \longrightarrow$ Ring R with localisation with $\{1, f, f^2, \dots\}$

2) P is prime in R
$S = R \setminus P$

$0 \in P \Rightarrow 0 \notin S$
$1 \notin P \Rightarrow 1 \in S$
if $a \in S$, $b \in S$ $\Rightarrow ab \in S$ <u>proof</u>:
if $ab \notin S$ $\Rightarrow ab \in P$
$\Rightarrow a \in P$ or $b \in P$
$\Rightarrow a \notin S$ or $b \notin S$ $\quad \divideontimes$

so S is m.c
now, if $S = R \setminus P$
then
$S^{-1}R = R_P$
where $S = R \setminus P$
or $S^c = P$

now, $PR_P = P(S^{-1}R)$
$PR_P = \left\{ \frac{a}{b} \,\middle|\, a \in P,\ b \in R \setminus P \right\}$

if $I \trianglelefteq R_P$
ideal of R_P

s.t $I \not\subseteq PR_P$
then $\frac{a}{b} \in I$ with $a, b \in R \setminus P$

so $\frac{b}{a} \in R_P$

then ie $I \trianglelefteq R_P$
$\frac{a}{b} \in I$

$\frac{b}{a} \in R_P \Rightarrow \frac{b}{a} \cdot \frac{a}{b} = 1 \in I$

$\Rightarrow I = R_P$

ie if $I \trianglelefteq R_P$
and $I \not\subseteq PR_P$
$\Rightarrow I = R_P$
$\therefore$ PR_P is maximal ideal (unique)

Now, R is domain $\quad \mathrm{Frac}(R) = K$ (field)
(as domain, NZD $\rightarrow$ field) $\quad R_P \leq K \quad \forall$ prime P of R

$$\left(R_P = \left\{ \frac{a}{b} \,\middle|\, a \in R,\ b \in R \setminus S \right\} \right)$$

Theorm: $\bigcap_{P \text{ is prime in } R} R_P = R$

proof: Now as R_P is of form $\frac{a}{b}$, $b \in R \setminus P$

$1 \in R \setminus P$

so $\quad R \subset R_P$

i.e $\forall$ Prime in R

$R \subseteq R_P$

so $\quad R \subseteq \bigcap_P R_P$

now, $\alpha \in \bigcap_P R_P$, then

$\alpha = \frac{u}{v}$, $u \in R$, $v \in R \setminus P \;\forall\; P$ in R
$v \neq 0$

now $D(\alpha) = \{ t \in R \mid t\alpha \in R \}$

now, $\quad D(\alpha) \leq R$

if $D(\alpha) \neq R$

then $\quad D(\alpha) \subseteq M \leftarrow$ maximal ideal of R

$\Rightarrow$ Prime ideal of R

(maximal ideal $\Rightarrow$ Prime ideal)

$D(\alpha) \subseteq M$
$\uparrow$
prime ideal say P

then $\quad D(\alpha) \subseteq P$

now, $\quad \alpha \in R_P$

so $\quad \alpha = Q/s$, $s \notin P$

$s\alpha = Q \in R$

$s \in D(\alpha)$ *

as $\quad s \notin P$

$s \in D(\alpha) \subseteq P$

not possible

so, $D(\alpha) = R$

26th sept -

domains (ID)
→ euclidian (ED) – Have divison algorithm
→ Priciple ideal (PID) – every ideal is priciple
→ unique factorization domain (UFD) – element have prime factors

division algoritm : (for $\mathbb{Z}$)

$m, n \in \mathbb{Z}$
and $m \leq n$
$m \neq 0$
$n = q_0 m + r_0$
$m = q_1 r_0 + r_1$
$r_0 = q_2 r_1 + r_2$
$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n-1} = q_{n+1} r_n$
then $r_n = \gcd(m,n)$

Note : $0 < r_0 < |m|$
$\vdots$
$0 < r_k < r_{k-1}$
$\vdots$
$0 < r_n < r_{n-1}$
and $r_{n+1} = 0$
$r_n < \cdots < r_1 < r_0 \leq |m| - 1$

Example : K is a field, $K[X] \leftarrow$ polynomials with $a \in K$ as coefficients

$f(x) \neq 0$, $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots a_1 x + a_0$
$a_d \neq 0$
$d = \deg f(x)$, $g(x) = b_m x^m + \cdots$
$b_m \neq 0$
$\deg g(x) \leq \deg f(x)$

$b_m x^m + \cdots \overline{) a_d x^d + \cdots}$

$f(x) = q(x) g(x) + r(x)$ $r(x) = 0$ or $\deg(r(x)) < \deg g(x)$

Norm : Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on the integral domain R. If $N(a) > 0, \forall a \in R \setminus \{0\}$ then norm N is a positive norm.

(think like the distance)

Defn : (euclidian domain) The integral domain R is said to be euclidian domain (or posses a division algoritm) if there exist a norm N on R s.t for any two elements a and b of R with $b \neq 0$, $\exists q, r$ s.t

$a = qb + r$, $r = 0$ or
$N(r) < N(b)$

q = quotient
r = reminder

Note : q, r need not be unique

when divison algoritm exist on euclidian domain, it means that

$a = q_0 b + r_0$
$b = q_1 r_0 + r_1$
$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$ ← last non-zero reminder
$r_{n-1} = q_{n+1} r_n$

Note: existence of division algorithm ⇒ every ideal of R to be priciple

Prop: every ideal of a euclidean domain is principle.

Proof:

We have to show that if $I \neq \{0\}$ and $I \leq R$, then $I = (d)$ for some $d \in R$

for $I = \{0\}$ there is nothing to prove.

Let d be any non-zero element of I of minimum norm. (from well ordering priciple on $\mathbb{Z}$)

$N(d) = \min\{N(a) \mid a \in I, a \neq 0\}$

then $(d) \subseteq I$.

Now, let $a \in I$ (any element in I)

$a = qd + r$ with $r = 0$ or $N(r) < N(d)$

as $r = a - qd$ and $a \in I$, $qd \in I$

$\Rightarrow r \in I$

$\Rightarrow r = 0$ as $N(r) \geq N(d)$ because $N(d)$ is the least

so, $I \subseteq (d)$

$\therefore I = (d)$

(This means that every ideal of $\mathbb{Z}$ is priciple)

Note: This prop can be used to show that some ID are not UD by finding ideals which are not principle.

Example: ① $K[X_1, X_2]$

$(X_1, X_2) \neq (P)$

$K[X_1, X_2, \dots X_n]$ $n \geq 2$ is not E.d

② $\mathbb{Z}[X]$ is not E.d as $(2, X)$ is not priciple.

$(2, X) = \{2a_0 + 2a_1x + \dots 2a_nx^n + b_0x + b_1x^2 + \dots b_mx^{m+1} \mid a_i, b_j \in \mathbb{Z}\}$

cannot be generated by one element of $\mathbb{Z}$ as const term even, else all can be anything.

$\therefore \mathbb{Z}[X]$ is not e.d

Note: euclidean domain produces a g.c.d of two non-zero elements.

Defn: Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

(I) a is said to be a multiple of b if there exist an element $x \in R$ with $a = bx$
in this case $b \mid a$.

(II) A gcd of a, b is a non-zero element d s.t
① $d \mid a$, $d \mid b$
② if $d' \mid a$, $d' \mid b$ then $d' \mid d$ ↙ greatest of such kind

Notion: $\gcd(a, b) = (a, b)$

Note: $b \mid a$ iff $a \in (b)$ iff $(a) \subseteq (b)$
so if $d \mid a$ and $d \mid b$
then $(a, b) \subseteq (d)$

if I is ideal of R generated by a, b i.e $I = (a, b)$
then gcd of a, b is d if:

① $(a, b) \subseteq (d)$
② if $(a, b) \subseteq (d')$ then $(d) \subseteq (d')$ ↖ smallest such ideal

prop: If a, b are non-zero elements in the commutative ring of R s.t ideals generated by a, b is principle idea (d), then $(d) = $ gcd of (a, b)

proof: $(a, b) = (d)$ then $d = \gcd(a, b)$

① as $(a, b) = (d)$
$(a, b) \subseteq (d)$
or $d \mid a$ and $d \mid b$

② also if $(a, b) \subseteq (d')$
then $(d) \subseteq (d')$
$\therefore$ $d' \mid d$ for all such d'

$\therefore$ d is the gcd of (a, b)

(Here d is unique as $(a, b) = (d)$ and if $(a, b) = (g)$ then it can be shown that $g \mid d$, $d \mid g \Rightarrow d = g$)

theorm: R be UD, let a, b be non-zero elements of R. let $d = r_n$ be the last non-zero reminder of euclidean algorithm for a, b then

① d is the gcd of a, b
② d can be written as $ax + by$ or (d) is the ideal generated by (a, b).

proof: ① ideal generated by (a, b) will have a prime element s.t $(a, b) = (d)$.

as $d \mid a$, $d \mid b$ and if $d' \mid a$, $d' \mid b$ $\Rightarrow d' \mid d$

as $r_{n-1} = q_{n+1} r_n$
we see that $r_n \mid r_{n-1}$
also $r_n \mid r_n$
by induction we get $r_n \mid r_{k+1}$ and r_k

as $r_{k-1} = q_{k+1} r_k + r_{k+1}$

$r_{k-1} - r_{k+1} = q_{k+1} r_k$

$$r_k \mid r_{k-1}$$

$$\Rightarrow r_n \mid r_{k-1}$$

so, $r_n \mid b$ and $r_n \mid a$ from 1st and 0th equation.

now, this means that $(a,b) \subseteq (r_n)$ —①

Now, to show that $(r_n) \subseteq (a,b)$ we will use:

$a = q_0 b + r_0$ 0th eq $r_0 \in (a,b)$

$b = q_1 r_0 + r_1$ $r_1 \in (b, r_0) \subseteq (a,b)$

$r_0 = q_2 r_1 + r_2$ $r_2 \in (r_1, r_0) \subseteq (a,b)$

$r_1 = q_3 r_2 + r_3$ $\vdots$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$ $\vdots$

$r_{n-1} = q_{n+1} r_n$ nth eq

we get $r_{k+1} = r_{k-1} - q_{k+1} r_k$
$\in (r_{k-1}, r_k)$
$\subseteq (a,b)$

this shows $(r_n) \subseteq (a,b)$ —②

from ①, ② $(r_n) = (a,b)$

as $(d) = (a,b) \Rightarrow \gcd(a,b) = d$ is unique

$d = r_n$

$\therefore r_n = \gcd(a,b)$

② Part 2 is trivial as $(d) = (r_n) = (a,b)$
$\Rightarrow r_n = xa + yb$

Defn: (Priniple ideal domain)
A P.I.D is a I.D in which every ideal is priniple.

Note: E.D ⇒ P.I.D
but P.I.D ⇏ E.D

eg: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a P.I.D but not E.D (Proof below)

$\mathbb{Z}[X]$ $(2, X)$ is not priniple, ∴ $\mathbb{Z}[X]$ not P.I.D

$K[X,Y]$, (X,Y) is not priniple, ∴ $K[X,Y]$ not P.I.D

prop: every non-zero prime ideal in a principle ideal domain is maximal ideal.

(Here maximal ideal ⇒ prime ideal, but for P.I.D
prime ideal $(\neq 0)$ ⇒ maximal ideal)

proof: let (P) be a non-zero prime ideal in the priciple ideal domain R.

let $I = (m)$ be any ideal containing (P).

Claim: if $(P) \subseteq (m) = I$, then $I = (P)$
or $I = R$

Now if $(P) \subseteq (m)$ then $\exists\, r \in R$ s.t
$P = rm$
as P is prime ideal
$\Rightarrow rm \in (P)$
$\Rightarrow r \in (P)$ or $m \in (P)$

if $m \in (P)$ then
$(m) \subseteq (P)$
$\Rightarrow (m) = (P) = I$

if $r \in (P)$ then
$r = ps$
in this case $p = rm$
$r = rms$
$\Rightarrow 1 = m \cdot s$
or $\exists\, s \in R$ s.t
$m \cdot s = 1$
$\therefore\ 1 \in (m)$
$\Rightarrow (m) = R$

Prop: If R is any commutative ring s.t polynomial ring $R[X]$ is a P.I.D then R is a field.

proof:
given $R[X]$ is a P.I.D
as $R \subset R[X]$
and R is a domain
now, $\frac{R[X]}{(X)} \cong R$

as $f(x) = a_0 + a_1 x + \cdots a_d x^d$
$f(x) \equiv a_0 \mod (x)$

this means that $\frac{R[X]}{(X)} \cong R \leftarrow$ I.D
$\Rightarrow \frac{R[X]}{(x)}$ is an ID
$\Rightarrow (x)$ is prime ideal

now as (x) is prime $\Rightarrow (x)$ is maximal
now as (x) is maximal
$\frac{R[X]}{(x)}$ is a field
$\Rightarrow \frac{R[X]}{(x)} \cong R$ is a field
$\Rightarrow R$ is a field

Defn: let R be an integral domain

① suppose $r \in R$ is non-zero and is not a unit. Then r is called irreducible. If $r = ab$ with $a, b \in R$ atleast one of a, b must be a unit in R. otherwise R is reducible.
② x is a prime if (x) is a prime ideal
③ $a = ub$ for some unit $u \in R$, then a, b are called assosiative.

Property: R is a P.I.D where $I_1 \subset I_2 \subset I_3 \cdots\cdots \subset I_n \subset \cdots$
I_n ideals in R
then $\exists\, n_0$ st $I_n = I_{n_0}$ $\forall\, n \geq n_0$

proof:

$\cup I_n = J \leq R$

$J = (t)$ as J is an ideal of R

also $t \in I_{n_0}$ for some n_0

$\Rightarrow (t) \subseteq I_{n_0} \subseteq I_n \subseteq (t)$

$\Rightarrow \quad I_{n_0} = I_n \quad \forall\, n \geq n_0$

$\Rightarrow \quad I_n = (t) = I_{n_0} \;\forall\, n \geq n_0$

Prop: In an ID a prime element is always irreducible

proof: suppose (p) is a non zero-prime ideal.

$p = ab$

then $ab = p \in (p)$

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

wlog. $a \in (p)$ then

$a = pr$ for some $r \in R$

$\Rightarrow p = ab$

$= p(rb)$

so $rb = 1$ and $\therefore$ b is a unit

$\therefore$ p is irreducible.

Theorm: If R is a P.I.D then if $x \in R$ is irreducible
$\Rightarrow$ x is a prime

proof: $(x) \subseteq \underset{(m)}{\overset{}{M}} \leftarrow$ maximal ideal

$x = am$

m is not unit ($\because M \neq R$)

so a is a unit

now $m = \frac{1}{a} x \in (x)$

$\Rightarrow (x) = (m)$

but as (m) is maximal $\Rightarrow$ m is prime

$\Rightarrow (x) = (m)$

30th sept :

Recap : R is any domain

(i) r is irreducible if

① r is not a unit

② $r = \alpha\beta \Rightarrow \alpha$ or β is a unit

(ii) r is prime if (r) is prime ideal

Note : r is prime $\Rightarrow r$ is irreducible

r is irreducible $\Rightarrow r$ is prime for P.I.D

Also R is PID

then $I_1 \subset I_2 \subset I_3 \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$ is an ascending chain of ideals then $\exists\, n_0$ s.t $I_n = I_{n_0}\ \forall n \geq n_0$

unique factorization domain : (U.F.D)

(i) R is ID

(ii) $r \neq 0$, r not a unit then

(a) $r = p_1 p_2 \ldots p_m$ where p_i is irreducible (not distinct)

(b) $r = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$

p_i, q_i irreducible

then $m = n$

and $q_i = u_i p_i$

↖ unit

Examples : 1) $\mathbb{Z}$ is UFD

2) every PID is UFD

3) R is a UFD $\Rightarrow$ $R[X]$ is a UFD

so, $R[x_1 \ldots x_n] = \left(R[x_1 \ldots x_{n-1}]\right)[x_n]$ is also a UFD

$k[x_1, \ldots x_n]$ UFD

$\mathbb{Z}[x_1 \ldots x_n]$ UFD

Propn : In unique factorisation domain, a nonzero element is prime iff it is irreducible

proof :

($\Rightarrow$) done

($\Leftarrow$) let p be irreducible in R

$ab \in (p)$ i.e let $p \mid ab$ some $a, b \in R$

$\Rightarrow pc = ab$

let $a = p_1 p_2 \ldots p_m$

$b = q_1 q_2 \ldots q_n$

$c = c_1 c_2 \ldots c_l$

p_i, q_j, c_s are irreducible

$\Rightarrow p_1 p_2 \ldots p_m q_1 q_2 \ldots q_n = c_1 c_2 \ldots c_l p$

or $m + n = l + 1$

i.e p is either associative to Πp_i or Πq_j

$\Rightarrow$ $a = rp$ or $b = rp$

$\Rightarrow$ $p | a$ or $p | b$

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

$\therefore$ (p) is prime ideal

$\Rightarrow$ p is prime

Theorm: Every principle ideal domain is a unique factorisation domain.

proof:

let $\underset{\text{not a unit}}{\underset{\downarrow}{r}} \neq 0$ and R be PID

To show: $r = p_1 p_2 \dots p_s$ p_i are irreducible

if r is irreducible then done

otherwise $\underset{\text{reducible}}{\underset{\uparrow}{r}} = r_1 r_2 \leftarrow$ irreducibles

$r_1 = r_{11} r_{12}$

or by this process we can have r as product of irreducibles.

Now **To show:** This process terminates

$$(r) \subsetneq (r_1) \subsetneq (r_{11}) \dots \subsetneq R$$

this inclusion are proper as there is no unit in the ideals.

so, now as PID, the process terminates

(strictly increasing chain of ideals in PID terminates)

so $r = p_1 p_2 \dots p_s$ where p_i is irreducible

now to show it is unique, let $\|r\| = \min\left\{ q \,\middle|\, \begin{array}{l} r = p_1 p_2 \dots p_q \\ p_i \text{ is irreducible} \end{array} \right\}$

now if $\|r\| = 1$

then $r = p_1$ is irreducible

if $r = q_1 q_2 \dots q_s$

say q_1 is irreducible

$$p_1 = q_1 \underset{\text{unit}}{\underset{\uparrow}{(q_2 \dots q_s)}}$$

$$p = r = q_1 \underset{\text{unit}}{\underset{\uparrow}{u}}$$

lets assume this is true for $\|r\| \leq s-1$, then for $\|r\| = s$

$r = p_1 p_2 \dots p_s = q_1 q_2 \dots q_l$ ↙ some unit

we have to show $p_1 p_2 \dots p_s = u q_1 q_2 \dots q_s$

as for $\forall \|r\| \leqslant s-1$ true
were

$$q_1 q_2 \dots q_e \in (P_1)$$

wlog $q_1 \in (P_1)$ as (P_1) is prime ideal
then $\underset{\substack{\uparrow \\ \text{irreducible}}}{q_1} = \underset{\substack{\uparrow \\ \text{unit}}}{\alpha} P_1$

$$\cancel{P_1} P_2 \dots P_s = (\alpha \cancel{P_1}) q_2 \dots q_e$$

$$b = P_2 \dots P_s = \alpha q_2 \dots q_e$$

as $\|b\| \leqslant s-1$

$\Rightarrow s = e$

$\therefore$ for $\|r\| = s$
true

or unique number wise.

Note: $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$

also if $\alpha = a+ib \in \mathbb{Z}[i]$
$N(\alpha) = a^2 + b^2$ (Norm)

Exercise: which prime p are sum of two squares

$p = a^2+b^2$

if p is odd and $p \equiv 1 \bmod 4$ or $p=2$
then sum of 2 squares

$2 = 1^2+1^2$
as $p \equiv 1 \bmod 4$
$p = 5, 13, \dots$

3 ✗
$5 = 2^2+1^2$
7 ✗
11 ✗
$13 = 3^2+2^2$

Factorization in the gaussian integers :

$\mathbb{Z}[i]$ ← gaussian integers

$$\alpha = a+ib \in \mathbb{Z}[i]$$
$$N(\alpha) = a^2+b^2 = \alpha\bar{\alpha}$$
$$N(\alpha\beta) = \alpha\beta\,\overline{\alpha\beta}$$
$$= \alpha\beta\bar{\alpha}\bar{\beta}$$
$$= \alpha\bar{\alpha}\,\beta\bar{\beta}$$
$$N(\alpha\beta) = N(\alpha)\,N(\beta)$$

α is a unit in $\mathbb{Z}[i]$
then $\alpha = \pm 1, \pm i$
if $\alpha\beta = 1$
$N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$
$N(\alpha) = 1$

if $N(\alpha)=1$
as $\alpha = \pm 1, \pm i$

$\alpha = a+ib$
$a^2+b^2=1$

$$\begin{cases} a=\pm 1 \quad b=0 \;; \alpha=\pm 1 \\ a=0 \quad b=\pm i \;; \alpha=\pm i \end{cases}$$

then $\underline{\alpha \text{ is a unit}}$

now if
$\alpha = a+ib$
$N(\alpha)=p$

<u>claim</u>: α is irreducible if $N(\alpha) = p$ prime

$\alpha = \beta\gamma$
$N(\alpha) = N(\beta)N(\gamma) = p$
so
$N(\gamma) \mid p$ or $N(\beta) \mid p$
$\Rightarrow N(\gamma) = p$ or 1 $\quad N(\beta) = p$ or 1

if $N(\beta)=1 \Rightarrow \beta$ is a unit
so α is irreducib
we proved α is irreducible if $N(\alpha) = p$ prime

<u>Note</u>: we have put $p = a^2+b^2$
$= \underset{\alpha}{(a+ib)}\underset{\beta}{(a-ib)}$

$N(\alpha) = p$
$N(\beta) = p$
so α, β are irreducibles

<u>lemma</u>: if $N(\beta) = p$ then β is prime

<u>proof</u>: $\mathbb{Z} \subseteq \mathbb{Z}[i]$
let (π) be a prime ideal in $\mathbb{Z}[i]$
then
$(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ (trivial)

$N(\pi) = \pi(\bar{\pi}) \in (\pi)$
and
$\in \mathbb{Z}_{>0}$

so $N(\pi) \in (\pi) \cap \mathbb{Z}$
and
$N(\pi) > 1$
as $1 \notin (\pi)$
↑
prime ideal

now, $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ where
$\pi\pi' = p$
as $p \in (\pi)$
or $\pi \mid p \Rightarrow \pi\pi' = p$

now $N(\pi\pi') = N(p) = p^2$

$N(\pi) = p$ or $N(\pi) = p^2$
as $N(\pi) \neq 1$

case I : $N(\pi) = p^2$
we have $N(\pi') = 1$
or π' is a unit
and $p = \pi\pi'$
or p is irreducible in $\mathbb{Z}[i]$

case II : $N(\pi) = p$
then $N(\pi') = p$ (π' is irreducible)
$p = \pi\pi'$
$\pi = a + ib$
$N(\pi) = a^2 + b^2 = p$
$\overline{\pi} = a - ib \Rightarrow a^2 + b^2 = p = N(\overline{\pi})$
or $N(\overline{\pi}) = p$
$\overline{\pi} = u\pi'$
$p = \pi\overline{\pi} = \pi\pi'$
or p is product of two irreducibles
or $\mathbb{Z}[i]$ is a UFD
$\therefore \pi, \pi'$ are primes
or $N(\pi') =$ prime

special case : $p = 2 = (1+i)(1-i)$

P is odd :

$a \equiv 0, 1, 2, 3 \mod 4$
$a^2 \equiv 0, 1, 0, 1$

$a^2 + b^2 = 0, 1, 2 \mod 4$
p odd prime
so
$a^2 + b^2 \equiv 1 \mod 4$

lemma : $p \in \mathbb{Z}$ divides an integer of form n^2+1 iff p is either 2 or an odd prime congruent to 1 mod 4.

proof : Assume $p \mid n^2+1$ $(\Rightarrow)$
then
$p = 2$ as $2 \mid 1^2 + 1$
or p is odd

then $n^2 \equiv -1 \mod p$
$\Rightarrow n^4 \equiv 1 \mod p$
$\Rightarrow \operatorname{ord} n = 4$ in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$

$\Rightarrow 4 \mid p-1$ (By lagrange theorm)
$\Rightarrow p \equiv 1 \mod 4$

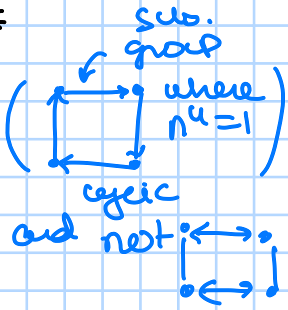
now if $p \equiv 1 \mod 4$ $(\Leftarrow)$
$p-1$ is divisible by 4

$\text{ord}(\mathbb{Z}/p\mathbb{Z})^* = p-1$ and as $4 \mid p-1$
$\uparrow$
cyclic

$\exists$ a unique n s.t
$n^4 \equiv 1 \mod p$
→ in $(\mathbb{Z}/p\mathbb{Z})^*$

$\Rightarrow n^2 = -1 \mod p$

$\Rightarrow p \mid n^2+1$



3rd oct :

Recap : if R is a P.I.D
or R is an ID and every ideal is priciple
then $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n = I_{n+1} = I_{n+2} \cdots$
or $\exists\, n_0 \in \mathbb{N}$ s.t $I_n = I_{n_0} \ \forall\, n \geq n_0$

Note : R is domain, then r is irreducible if :
(I) r is not a unit
(II) $r = ab$ then a or b are unit

r is prime : if (r) is prime ideal

Note : r is prime ⇒ r is irreducible
in PID : r is irreducible ⇒ r is prime

Note : R is U.F.D :
(I) R is domain
(II) $r \neq 0$ and if r is not a unit, then

$r = p_1 p_2 \dots p_s$ where p_i are irreducible
also if
$r = p_1 p_2 \dots p_s$
$= q_1 q_2 \dots q_l$
then
$s = l$ u is a unit
and $q_i = u p_i$

Note : R is a E.D ⇒ R is a P.I.D ⇒ R is a U.F.D ⇒ R is an ID
$ED \subseteq PID \subseteq UFD \subseteq ID$

Theorm : R is ID ⇒ R[x] is also ID

proof :

R is a domain, so R[x] is also a domain

$f(x) \neq 0$
$g(x) \neq 0 \Rightarrow f(x)g(x) \neq 0$

as $f(x) = a_n x^n + \dots a_0$
$a_n \neq 0$
$g(x) = b_m x^m + \dots b_0$
$b_m \neq 0$
then
$f(x)g(x) = a_n b_m x^{n+m} + \dots a_0 b_0$
$a_n b_m \neq 0$
as R is a domain
$\therefore f(x)g(x) \neq 0$

$\therefore$ R[x] is a domain

prop : I is an ideal of Ring R and let $(I) = I[x]$ denote ideal of R[x] generated by I (set of poly. with coeff in I) then :
$R[x]/(I) \cong (R/I)(x)$

(were if I is prime ⇒ R/I is ID ⇒ $(R/I)(x)$ is ID
or $R[x]/(I)$ is ID ⇒ (I) is prime)

proof : $\psi : R[x] \longrightarrow (R/I)[x]$

$f(x) = a_n x^n + \cdots a_0 \longmapsto \overline{f(x)} = \bar{a}_n x^n + \cdots \bar{a}_0$

$\bar{a}_i = a_i \bmod I$

<u>ψ is homomorphism :</u>

① well defined as $a_n x^n + \cdots a_0 = b_n x^n + \cdots b_0$

then

$\bar{a}_n x^n + \cdots \bar{a}_0 = \bar{b}_n x^n + \cdots \bar{b}_0$

② $\psi(f(x)+g(x)) = \overline{f(x)+g(x)} = \overline{f(x)} + \overline{g(x)}$

$= \psi(f(x)) + \psi(g(x)$

③ $\psi(f(x)g(x)) = \overline{f(x)g(x)} = \overline{f(x)}\,\overline{g(x)}$

$= \psi(f(x))\,\psi(g(x))$

<u>ψ is surjective :</u>

$\overline{f(x)} = \bar{a}_n x^n + \cdots \bar{a}_1 x + \bar{a}_0$

then

$\psi(\bar{a}_n x^n + \cdots \bar{a}_1 x + \bar{a}_0)$

$= \bar{a}_n x^n + \cdots \bar{a}_0$

or $\forall\ \overline{f(x)} \in (R/I)(x)$, $\exists\ \overline{f(x)} \in R(X)$

s.t.

$\psi(\overline{f(x)}) = \overline{f(x)}$

<u>ker ψ :</u>

$\ker\psi = \{ b_0 + b_1 x + \cdots b_m x^m \mid b_i \in I \}$

$= (I)$

or $R[X]/(I) \cong (R/I)[X]$

<u>corr</u> : P is prime in R ⇒ PR[x] is prime in R[x]

or

(P)

proof : As $R[x]/PR[x] \cong (R/P)[x]$

as

(R/P) is ID

⇒ $(R/P)[x]$ is ID

⇒ $R[x]/PR[x]$ is ID

⇒ $PR[x]$ is prime

prop: (Gauss's lemma) let R be a UFD with field of fractions F. let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$.

($p(x) = A(x)B(x)$, some non-const polynomials in $F(x)$, then there are $r, s \in F$ (not zero) s.t $rA(x) = a(x)$ and $sB(x) = b(x)$ in $R[x]$ s.t $p(x) = a(x)b(x)$. Note: $\deg A(x) = \deg a(x)$)

proof: $A(x) = \alpha_r x^r + \dots \alpha_1 x + \alpha_0$

$\alpha_r \neq 0$

$\alpha_i \in F$

$\alpha_i = \frac{c_i}{a_i}$ $a_i \neq 0$ $\forall i$ and $c_r \neq 0$

$$A(x) = \frac{c_r}{a_r} x^r + \dots \frac{c_1}{a_1} x + \frac{c_0}{a_0}$$

$a = \prod a_i$

$a(x) = a\,A(x) \in R[x]$

$\exists b$ s.t $b(x) = b\,B(x) \in R[X]$

now

$d = ab$

or $d f(x) = a'(x)\, b'(x)$

as $f(x) = A(x)B(x)$

Case I: d is a unit in R then

then

$a(x) = d^{-1} a'(x) \in R(x)$

and $b(x) = b'(x) \in R(x)$

so $f(x) = a(x)\,b(x)$

where

$d^{-1}a'(x) = a(x) \in R(x)$

$b'(x) = b(x) \in R(x$

Note: $\deg a' = \deg a = \deg A(x)$

case II: d is not a unit

then as $d \in R$

and R is a UFD

$d = p_1 p_2 \dots p_n$

s.t p_i is irreducible

$\Rightarrow (p_i)$ is prime in R

$\Rightarrow p_i R[x]$ is prime in $R[x]$

and

$(R/p_iR)[x]$ is an ID

then $\overline{d\,p(x)} = \overline{a(x)\,b(x)}$ (modulo p_i)

$\Rightarrow 0 = \overline{a'(x)}\,\overline{b'(x)}$

as $(R/p_iR)[x]$ is an ID

$\Rightarrow \overline{a'(x)} = 0$ or

$\overline{b'(x)} = 0$

wlog $\overline{a'(x)} = 0$, then $a'(x) = a'_r(x)^r + \dots a'_0$

$\forall j$ $a'_j \bmod p_i = 0$

or all coeff of $a'(x)$ divisible by p_i

$\Rightarrow p_i^{-1} a'(x) \in R[x]$

if we repeate this process for all p_i
we get

$f(x) = a(x) b(x)$, where $a(x) \in R[x]$
$b(x) \in R[x]$

where $\deg a(x) = \deg A(x)$
$\deg b(x) = \deg B(x)$

Cor: let R be a U.F.D, let F be its field of fractions and let $P(x) \in R[x]$
gcd of coeffs of $P(x)$ is 1, then:

$P(x)$ is irreducible in $R[x]$ iff $P(x)$ is irred. in $F[x]$.

(Note: if $P(x)$ is monic, gcd of coeff $= 1$ then $P(x)$ is irr in $F[x]$
and irr in $R[x]$)

proof: By gauss's lemma, if $P(x)$ is reducible in $F[x]$ then it
is reducible in $R[x]$

$(\Rightarrow)$

or $P(x)$ irr-red. in $R[x] \Rightarrow P(x)$ is irr-red. in $F[x]$

$(\Leftarrow)$

now, if gcd of coeff in $P(x) = 1$
then if $P(x)$ is red in $R[x]$ then

$P(x) = a(x) b(x)$
where $a(x) \neq$ const
$b(x) \neq$ const

so $a(x), b(x) \in F(x)$
$\therefore P(x)$ is red in $F[x]$

or $P(x)$ is red in $R[x] \Rightarrow P(x)$ is
red in $F[x]$

$\Rightarrow \sim(P(x)$ is red in $R[x]) \Leftarrow \sim(P(x)$ is red
in $F[x])$

or $P(x)$ is irr in $F[x] \Rightarrow P(x)$ is irr in $R[x]$

Theorm: R is UFD $\Leftrightarrow$ $R[x]$ is UFD

proof: $R[x]$ is a UFD then R is a UFD as R is collection of
constant polynomials of $R[x]$. And so

$(\Leftarrow)$

$\forall r \in R \Rightarrow r \in R[x]$
$\therefore r = p_1 p_2 \ldots p_n$ (irreducibles)
and if $r = q_1 q_2 \ldots q_m$
then $n = m$
and $q_i = \overset{\text{unit}}{u} p_i$

($\Rightarrow$) if R is a UFD then, let F is a field of fractions and $p(x)$ is a non-zero element of $R[X]$

let $d=$ gcd of coeff of $P(x)$ or

$$p(x)=d\ p'(x)$$

where gcd ($p'(x)$ coeff) $=1$

now as $d\in R$, d can be factored as irreducibles and also

let $p'(x)$ deg >0 i.e $p'(x)$ is not const (not unit) as if unit then trivial case.

now by induction on $p'(x)$

$$p'(x)=p_1(x)\cdots p_s(x) \text{ of irr in } R[x]$$

deg $p'(x)=1$ then $p'(x)=p'(x)$ so irr in $R[x]$

if true for deg $p'(x)<m$ then to show: true for deg $p'(x)=m$

if $p'(x)$ is irr in $R[x]$ then NTS

$p'(x)=a(x)b(x)$ gcd of coeff of a and b $=1$

as deg $a(x)<m$
deg $b(x)<m$

by induction $a(x)$, $b(x)$ are product of irred so, $p'(x)$ is product of irreducibles.

uniqueness :

$$p'(x)=p_1(x)\cdots p_s(x)$$
$$=q_1(x)\cdots q_r(x)$$

where p_i, q_j are irr in $R[x]$ $\forall\, i,j$ and gcd of coeff of $p_i, q_j=1$ $\forall\, i,j$

(Note: $F[X]$ is a UFD as F is a field $\Rightarrow F[X]$ is PID $\Rightarrow F[X]$ is a UFD)

as gcd of coeff of $p_i, q_j=1$

and p_i, q_j are irrd in $R[x]$
$\Rightarrow q_i, p_j$ are irrd in $F[X]$

or in $F[x]$, $p_i(x) = u_i q_i(x)$

u_i is unit in $F[x]$

$\Rightarrow p_i(x) = \frac{a_i}{b_i} q_i(x)$

$a_i, b_i \in R$

$\Rightarrow b_i p_i(x) = a_i q_i(x)$

let gcd of $p_i(x) = 1$ (coeff of p_i)

so gcd $b_i p_i(x) = b_i$ (coeff of p_i)

similary gcd of coeff of $a_i q_i(x) = a_i$

$\Rightarrow b_i = u a_i$ for some unit v in R

$\Rightarrow q_i(x) = u p_i(x)$

7th oct :

Recap : R is UFD $\Leftrightarrow$ $R[X]$ is a UFD

goal : To determine irreducible elements of the polynomial ring ($R[X]$)

Example : non-const monic polynomial irreducible if cannot be factord in two small degree polynomi

prop : F be a field , $P(x) \in F[X]$, $p(x)$ has a factor of degree one iff $p(x)$ root in F ($\exists\, \alpha \in F$ s.t $p(\alpha)=0$)

proof : ($\Rightarrow$) factor of degree 1 then let's assume it is monic $(x-\alpha)$ form $\alpha \in F$

$$p(\alpha)=0$$

($\Leftarrow$) if $p(\alpha)=0$ as $F[X]$ is a field $\Rightarrow$ $F[X]$ is E.D (proof is long)

or $p(x)=q(x)(x-\alpha)+r$

as r is const

$P(\alpha)=0$, r must be 0

so $r=0$ $\therefore$ $p(x)=q(x)(x-\alpha)$

or

$(x-\alpha)$ is a factor

prop : A polynomial of degree two/three over F is reducible iff it has root in F.

proof : ($\Rightarrow$) if a poynomial has deg 2 or deg 3 then

$p(x)=q(x)r(x)$

where $\deg q(x)=1$

$r(x)=1$

for $\deg P(x)=2$

and $\deg p(x)=3$

wlog $\deg q(x)=2$

$\deg r(x)=1$

(2/3 → 1 , 2 or 1)

so as degree 1 $\Rightarrow$ one root

($\Leftarrow$) if a root then

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

or reducible

prop : $p(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_0$ polynomial of degree n

(coeff $\in \mathbb{Z}$)

or

$P(x) \in \mathbb{Z}[x]$

$r/s \in \mathbb{Q}$ s.t $\gcd(r,s)=1$

and $P(r/s)=0$

then $r \mid a_0$ and $s \mid a_n$

or $p(x)$ is monic in $\mathbb{Z}[x]$ and $p(d) \neq 0$ $\forall\, d \in \mathbb{Z}$ s.t $d | a_0$ then $p(x)$ has no roots in $\mathbb{Z}$

<u>Proof</u> : $p(r/s) = 0 = a_n(r/s)^n + \cdots + a_0$

$0 = a_n r^n + \cdots \cdots a_0 s^n$

or

$a_n r^n = s(-a_{n-1} \cdots\cdots)$

$s | a_n r^n \Rightarrow s | a_n$

similary $r | a_0$

or $P(p/q) = 0$ and $P(x) \in \mathbb{Z}[x]$

$\Rightarrow p | \underset{\substack{\uparrow \\ \text{const term}}}{a_0}$ and $q | \underset{\substack{\uparrow \\ \text{highest degree term}}}{a_n}$

now if $P(x) \in \mathbb{Z}[x]$, is monic and so

$P(x) = ax + b$

now if $d | b \Rightarrow P(d) \neq 0$

then

<u>To show</u>: no root in $\mathbb{Z}$

<u>Proof</u> : $P(x) = ax + b$

now if

$P(d) = ad + b = 0$

then $d | b$ $\divideontimes$

$\therefore$ no roots in $\mathbb{Z}$

<u>Example</u> :

(1) $x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$

as if root in $\mathbb{Q}$ then

$f(p/r) = 0$ s.t $r | 1$

$p | -1 \Rightarrow p = \pm 1$

and $r \Rightarrow \pm 1$

or roots $= \pm 1$

but $(-1)^3 - 3(-1) - 1$

$= -1 + 3 - 1 = 1 \neq 0$

and $(1)^3 - 3 - 1 \neq 0$

or no roots in $\mathbb{Q} \Rightarrow$ no roots in $\mathbb{Z}$

now deg 3, no roots in $\mathbb{Z} \Rightarrow$ irreducible in $\mathbb{Z}[x]$

(2) $\left.\begin{matrix} x^2-p \\ x^3-p \end{matrix}\right\} \rightarrow$ irreducible in $\mathbb{Q}[x]$

as if r/s

then $r \mid p \Rightarrow r = p$ or 1

and as $s \mid 1 \Rightarrow s = \pm 1$

or roots will be $\pm p, \pm 1$

all not possible

$\therefore$ No roots for deg $= 2/3$

$\therefore$ irreducible

(3) x^2+1 is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$

as has root

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

$p(\bar{1}) = \bar{1} + \bar{1} = \bar{0}$

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

$\therefore$ reducible

(4) x^2+x+1 is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$

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

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

(5) x^3+x+1 is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ (same)

Techniques: ① deg $=1$ ⇔ has a root

② for deg $2/3$:

has a root ⇔ reducible

does not have any root ⇔ irreducible

③ if root in $\mathbb{Q}$ of r/s then

$s \mid a_n \quad r \mid a_0$ ← last term

④ gauss lemma:

field of fractions

$P(x)$ reducible in $F[x]$

$\Rightarrow$

$P(x)$ reducible in $R[x]$

Ring

⑤ $P(x)$ irreducible in $F[x]$

$\Leftrightarrow P(x)$ irreducible in $R[x]$

Note: only limited to low degree (factor has deg 1)

prop: I be a proper ideal in ID R.
$p(x)$ non const polynomial in $R[x]$

image of $p(x)$ in $(R/I)[x]$ is irreducible

$\Rightarrow$ $p(x)$ in $R[x]$ is irreducible

proof: suppose $p(x)$ is irreducible in $(R/I)[x]$ but reducible in $R[x]$
then
$$p(x) = q(x)r(x)$$
for $q(x), r(x) \in R[x]$
having degree ≥ 1

but $\overline{p(x)} = \overline{q(x)}\,\overline{r(x)}$ for $(R/I)[x]$
so this
means $p(x)$ is reducible
in $(R/I)[x]$ $\ast$

$\therefore$ $P(x)$ irreducible in $(R/I)[x] \Rightarrow P(x)$ is irreducible in
$R[x]$

Examples: (1) $p(x) = x^2+x+1$ in $\mathbb{Z}[x]$

$\overline{p(x)}$ for $\mathbb{Z}/2\mathbb{Z}[x]$

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

as irreducible in $\mathbb{Z}/2\mathbb{Z}[x] \Rightarrow$ irreducible in $\mathbb{Z}[x]$

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

as
$0+1 = \bar{1} \neq \bar{0}$
$1+1 = \bar{2} \neq \bar{0}$
$4+1 = \bar{2} \neq \bar{0}$

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

Note: x^2+1 is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$

Technique: ⑥ $p(x)$ is irreducible in $(R/I)[x]$
$\Rightarrow$ $p(x)$ is irreducible in $R[x]$

(3) $3(100)x^{100} + 3(99)x^{99}$
$+ \cdots\cdots 3(1)x^1 + 4$

$= 1$ in $\mathbb{Z}/3\mathbb{Z}[x]$
so irreducible
in $\mathbb{Z}[x]$

$300x^{100} + 3\times 99\, x^{99} + \cdots + 3x + 4$
irreducible in $\mathbb{Z}[x]$

propn : (Eisenstein's Criterion)
Let P be prime ideal of the ID R and let
$f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ $(n \geq 1)$
be a polynomial in $R[X]$

if $a_{n-1}, a_{n-2}, \ldots a_1, a_0 \in P$
and
$a_0 \notin P2$
then $f(x)$ is irreducible in $R[X]$

proof : if f was reducible in $R[X]$ then $f(x) = a(x)b(x)$
$a(x), b(x)$ $(n \geq 1)$
reducing modulo P we get

$$x^n = \overline{a(x)}\ \overline{b(x)} \text{ in } (R/P)[X]$$

as (R/P) is ID

for $x^n = \overline{a(x)}\ \overline{b(x)}$
where
$\overline{a(x)}, \overline{b(x)} \in (R/P)[X]$
the const term of $a(x), b(x) \in P$
or else the above not true
but then
a_0 = cost term of $a(x)$
× cost term of $b(x)$
$\in P2$ ✱

$\therefore f$ is irreducible

Corr : (Eisenstein's criteria for $\mathbb{Z}[X]$)
Let p be prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$
s.t $p \mid a_i \ \forall i \in \{0, 1, \ldots n-1\}$
but $p^2 \nmid a_0$
then
$f(x)$ is irreducible in $\mathbb{Z}[X]$
and $\mathbb{Q}[X]$

proof : Same as above, also if $f(x)$ is irr in $\mathbb{Z}[X](R)$
$\Leftrightarrow$
$f(x)$ is irr in $\mathbb{Q}[X](F)$

Examples :
(1) $x^4 + 10x + 5$ in $\mathbb{Z}[X]$
then
5 = prime
and $5 \mid 10$, $5 \mid 5$
but $25 \nmid 5$
$\therefore$ irreducible in $\mathbb{Z}[X]$

(ii) $x^n - p$ is irreducible for all $n \geq 2$

(iii) $f(x) = x^4 + 1$ now

4 $g(x) = f(x+1)$

$= (x+1)^4 + 1$

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

$= x^4 + 4x^2 + 1$

$+ 4x^3 + 4x + 2x^2 + 1$

$= x^4 + 4x^3 + 4x^2 + 4x + 2$

as $2 | 4$ and $2 | 2$

but $4 \nmid 2$

so $f(x+1)$ is irreducible

(iv) $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots\dots x + 1$

↘ cyclotomic polynomial

now $\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$

$= \frac{1}{x}\left[\cancel{1} + {}^pC_1 x^1 + {}^pC_2 x^2 + \dots {}^pC_p x^p\right]$

$= {}^pC_1 + {}^pC_2 x + {}^pC_3 x^2 + \dots {}^pC_p x^{p-1}$

$= x^{p-1} + p x^{p-1} + \frac{(p)(p-1)}{2} x^{p-2}$

$+ \dots p.$

as all factors divide p, $p^2 \nmid p$

so $\Phi(x+1)$ not reducible

$\therefore$ $\Phi(x)$ not reducible

Note: $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots\ x + 1$

$= \frac{x^p - 1}{x - 1}$ is called cyclotomic polynomial and is irreducible in $\mathbb{Z}[x]$ and also $\mathbb{Q}[x]$

Tecnique: ⑦ for $f(x) = x^n + a_{n-1}x^{n-1} + \dots\ a_1 x + a_0$ if $p | a_i$ but $p^2 \nmid a_0$ then irreducible

⑧ for $f(x)$, check $f(x+1)$ also as sometimes we can use einstinés criterion.

Note: $\overset{\leftarrow \text{field}}{R = F[x]}$

$a \in F$ then

$\eta : F[x] \longrightarrow F$

$f(x) \longmapsto f(a)$

η is a ring homomorphism

Defn: a is root of $f(x)$ if $f(a) = 0$

Prop: $a \in F$ root of $f(x) \Leftrightarrow f(x) = g(x)(x-a)$

proof:

$(\Leftarrow)$ $f(a) = g(a)(a-a) = 0$

$(\Rightarrow)$ a is a root of $f(x)$

$f(x) = g(x)(x-a) + r(x)$

and

$\deg r(x) < 1$

$\Rightarrow$

$r(x) = r \in F \setminus \{0\}$

$f(x) = g(x)(x-a) + r$

$\Rightarrow r = 0 \quad \therefore \quad f(x) = g(x)(x-a)$

lemma: $f(x) = a_n x^n + \dots a_1 x + a_0 \in \mathbb{Z}[x]$

$\gcd(r,s) = 1$, $s \geq 1$ $\quad \alpha = \frac{r}{s}$ root of $f(x)$

$\Rightarrow r \mid a_0$ and $s \mid a_n$

proof: $0 = f\left(\frac{r}{s}\right) = a_n \frac{r^n}{s^n} + \cdots a_1 \frac{r}{s} + a_0$

$0 = a_n r^n + \dots a_0 s^n$

$s \mid a_n r^n \Rightarrow s \mid a_n$

Example: $x^3 - 3x - 1 = f(x)$

no-rational-roots

$x^2 - p$, $x^3 - p$ no roots in $\mathbb{Q}[x]$

lemma: $\deg f(x) = 1 \Rightarrow f(x)$ is irreducible

$\deg f(x) = 2, 3$, if $\exists \alpha \in F$ s.t $f(\alpha) = 0 \Rightarrow f(x)$ is reducible

proof: $f(x) = g(x) h(x) \neq 0$

then

$\deg f(x) = 1 = \deg g(x) + \deg h(x)$

if $f(x) = \alpha x + \beta$

$1 = N(g) + N(h)$

$\Rightarrow$ wlog $N(g) = 0$

$\therefore g \neq c \in F^*$

or g is unit

$\therefore$ f is irreducible

ALSO for $N(f)=2$ or 3 and if it has root then wlog $N(g)=1$
so reducible

Propn: $f(x) \in \mathbb{R}[X]$, $N(f) \geq 3 \Rightarrow f$ is irreducible

proof :
if $f(x)$ real root α
then reducible
as $f(x) = g(x)(x-\alpha)$

if α not real but a root then
$\alpha \in \mathbb{C}$

$$f(x) = (x-\alpha)\, g(x) \quad \text{in} \quad \mathbb{C}[X]$$

$$z \to \bar{z}$$
$$a+bi \to a-bi$$

$$f(x) \Rightarrow \overline{f(x)} = (x-\bar{\alpha})\,\overline{g(x)} \overset{\text{as } \in \mathbb{R}[X]}{=} f(x)$$

$\bar{\alpha}$ is root of $\overline{f(x)}$

$\bar{\alpha} \neq \alpha \Rightarrow x-\alpha \quad x-\bar{\alpha}$ are both factors of $f(x)$

so $f(x) = g'(x)\,(x-\alpha)(x-\bar{\alpha})$

$$f(x) = g'(x) \underbrace{[\, x^2 - \underset{\in \mathbb{R}}{(\alpha+\bar{\alpha})}x + \underset{\in \mathbb{R}}{\alpha\bar{\alpha}} \,]}_{\mathbb{R}[X]}$$

so f is reducible

Note : $f(x)$ is irr in $\mathbb{Q}[X] \Leftrightarrow f(x)$ is irr in $\mathbb{Z}[X]$
and
$f(x)$ is irr in $\mathbb{Z}/p[X] \Rightarrow f(x)$ is irr in $\mathbb{Z}[X]$
and so $\mathbb{Q}[X]$

lemma : $\overline{f(x)}$ irr in $R/_I[X] \Rightarrow f(x)$ is irr in $R[X]$

proof : $f(x) = g(x)h(x)$
if reducible
then

$$\theta : R[X] \longrightarrow R/_I[X]$$
$$\theta(X) \longmapsto \bar{\theta}(x)$$

$$\overline{f(x)} = \overline{g(x)}\,\overline{h(x)} \;\text{\large$\lightning$}$$

Eisenstein's criterion :

R is domain   P is prime
$a_i \in P \ \forall i$
$a_0 \notin P^2$
then $f(x)$ is irr in $R[x]$

Note: $f(x)$ is irr $\Leftrightarrow$ $f(x+1)$ is irr
$f(x) = g(x)h(x)$
$f(x+1) = g(x+1)h(x+1)$

proof : $f(x) = g(x)h(x)$ (if reducible)

then

$$\overline{f(x)} = x^n = \overline{g(x)}\ \overline{h(x)}$$

or

cost of $g(x) \in P$
cost of $h(x) \in P$

$\Rightarrow a_0 \in P^2$ *

10th oct :

Defn: V is a K vetor space
if ① $(V,+)$ abelian group
② (I) $1.v = v \quad \forall v \in V$
(II) $\alpha, \beta \in K \quad (\alpha+\beta)v = \alpha v + \beta v, \ \forall v \in V$
(III) $\alpha(v_1+v_2) = \alpha v_1 + \alpha v_2, \ \alpha \in K \ v_1, v_2 \in V$
(IV) $\alpha(\beta.v) = (\alpha.\beta)v, \ \forall \alpha, \beta \in K, \ v \in V$

Note: R be a commutative ring

Defn: M is an R-module if:

$+ : M \times M \to M$
$\bullet : R \times M \to M$

s.t
(I) $(M,+)$ is an abelian group
(II) (i) $1_R.m = m \quad \forall m \in M$
(ii) $(\alpha+\beta).m = \alpha m + \beta m, \ \forall \alpha, \beta \in R, \ \forall m \in M$
(iii) $\alpha.(m_1+m_2) = \alpha.m_1 + \alpha.m_2, \ \forall \alpha \in R, \ \forall m_1, m_2 \in M$
(iv) $\alpha.(\beta.m) = (\alpha.\beta).m, \ \forall \alpha, \beta \in R, \forall m \in M$

Note: V k-vetor space
maximal lin ind set = Basis
minimal spanning/generating set = Basis
$V \cong k^n \to$ Dim of V

Example: $\mathbb{Z} \cong \mathbb{Z}^1$
or
$\{1\}$ = Basis
$n = n.1$
$\forall n \in \mathbb{Z}, \ n = n.1$
for $n \in \mathbb{Z}$

↱ not minimal spanning
$(2,3)\mathbb{Z} = \mathbb{Z}$
but
$2\mathbb{Z} \neq \mathbb{Z}$
$3\mathbb{Z} \neq \mathbb{Z}$

Example: ↙ k is the same
V is a vetorspace, so is $k[x]$
(k- vetor space)

Example: R is a comm ring

$$R^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \middle| \ a_i \in R \right\}$$

$$r.\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}$$

called: free R-module of rank = n

Note: $\mathbb{R}^n \cong \mathbb{R}^m \Rightarrow m = n$
(for comm ring)

$\mathbb{R}^n \cong \mathbb{R}^m \not\Rightarrow m = n$
(for non-comm ring)

Defn: M, N are R-modules then

$$M \oplus N = \{(m,n) \mid m \in M, n \in N\}$$

$$(m,n) + (m',n') = (m+m', n+n')$$

$$r.(m,n) = (r.m, r.n)$$

Note: $R^n = \underbrace{R \oplus R \oplus \cdots \oplus R}_{n \text{ times}}$

Defn: **Submodule**:
$M \subseteq N$
is called submodule of N
if (I) $(M,+) \leq (N,+)$
(II) $r \in R, m \in M \Rightarrow r.m \in M$

Exe: $N \leq R \Leftrightarrow N$ is an ideal of R

($\Rightarrow$) As $N \leq R$, N is the submodule of R

$(N,+) \leq (R,+)$

and

for $r \in R$, $m \in N \Rightarrow r.n \in N$

and

as R is comm

for $r \in R$, $m \in N$

$r.n = n.r \in N$

or N is ideal of R

($\Leftarrow$) Trivial

Note: $N \leq M$ (N is submodule of M)
and N, M are R-modules then

$(N,+) \leq (M,+)$

then:

$M/N = [m + N] \quad \forall m \in M$

$M/N = \{[m+N] \mid m \in M\}$

Note: $M/_N$ is a R-module:

proof: M/N satisfies:

① $(M/_N, +)$ is abelian as

for $m_1 + N \in M/N$

and

$m_2 + N \in M/N$

then

$$(m_1+N) + (m_2+N)$$
$$= m_1 + m_2 + N$$
$$= m_2 + m_1 + N$$
$$= (m_2+N) + (m_1+N)$$

② (i) $1_R.(m+N) = m + \underbrace{1_R.N}_{\in N}$

$$= m + N$$

(ii) $\alpha(m_1+N + m_2+N)$

$$= \alpha m_1 + \alpha m_2 + N$$
$$= \alpha(m_1+N) + \alpha(m_2+N)$$

(iii) $(\alpha+\beta)(m+N) = \alpha(m+N) + \beta(m+N)$

(iv) $\alpha.(\beta.(m+N)) = \alpha\beta m + N$

$$= (\alpha\beta)(m+N)$$

Note: $m + N = m' + N$

$m = m' + n \quad \exists n \in N$

$rm = rm' + rn \in N$

$rm + N = rm' + N$

Defn: $\varphi : M \to N$ is a module homorphism

if

1) $\varphi(m_1+m_2) = \varphi(m_1) + \varphi(m_2)$

2) $\varphi(r.m) = r\varphi(m)$

Note: $Hom_k(k^n, k^m) \cong M_{m,n}(k)$

$Hom_R(R^n, R^m) \cong M_{m,n}(R)$

Example: $A \in M_{m,n}(R)$

then

$$\varphi_A : R^n \longrightarrow R^m$$
$$\underline{a} \longmapsto A\underline{a}$$

$$\varphi_A(\underline{a}) = A\underline{a}$$

$$\varphi_A(\underline{a}+\underline{b}) = A(\underline{a}+\underline{b})$$
$$= A\underline{a} + A\underline{b}$$
$$= \varphi(\underline{a}) + \varphi(\underline{b})$$

and sim $\varphi_A(r\underline{a}) = r\varphi_A(\underline{a})$

Note: $\phi : R^n \to R^m$

where $e_1, e_2 \dots e_n$ are std e_i of R^n

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \} i^{th} \text{place } 1$$

$$c_i = \phi(e_i)$$

$$A = [c_1, c_2 \dots c_n]$$

$$\phi = \varphi_A$$

Example: $2\mathbb{Z} \leq \mathbb{Z}$

$\downarrow$

submodule

$\{\bar{0}, \bar{1}\} = \mathbb{Z}/_{2\mathbb{Z}}$ $\nwarrow$ Also a submodule

$\neq \mathbb{Z}^n$ for any $n \geq 1$

Defn: $\varphi : M \to N$ is a module homomorphism

$$\ker \varphi = \{m \mid \varphi(m) = 0\}$$

$$\ker \varphi \leq M$$

$$\operatorname{Im} \varphi = \{\varphi(m) \mid m \in M\} \leq N$$

$$\operatorname{coker} \varphi = N/\operatorname{Im}(\varphi)$$

Defn: $\varphi : M \to N$ is isomorphism

if $\exists\ \phi : N \to M$ s.t.

$$\phi \cdot \varphi = 1_M$$

$$\varphi \cdot \phi = 1_N$$

Defn: $\varphi : M \to N$ is bijective

then module hom $\Rightarrow \varphi^{-1} : N \to M$ is R-linear

if

$$\left\{ \begin{array}{l} \varphi \circ \varphi^{-1} = 1_N \\ \varphi^{-1} \circ \varphi = 1_M \end{array} \right.$$

(R-linear is called for Homomorphism)

Note: $\varphi^{-1}(n_1) = m_1$

$\varphi^{-1}(n_2) = m_2$

then

$$\varphi(m_1) = n_1$$

$$\varphi(m_2) = n_2$$

$$\varphi(m_1 + m_2) = n_1 + n_2$$

$$\varphi^{-1}(n_1 + n_2) = m_1 + m_2 = \varphi^{-1}(n_1) + \varphi^{-1}(n_2)$$

Note: as $\varphi(rm) = r\varphi(m)$

$= rn$

we have

$\Rightarrow rn = \varphi(rm)$

$\Rightarrow \varphi^{-1}(rn) = rm$

$\Rightarrow \varphi^{-1}(rn) = r\varphi^{-1}(n)$

First isomorphism theorm:

$\varphi : M \to N$ is surjetive R-linear map then

$$\Rightarrow M/\ker\varphi \underset{\bar\varphi}{\cong} N$$

proof : $\bar\varphi : M/\ker\varphi \longrightarrow N$

$$(m+\ker\varphi) \longmapsto \varphi(m)$$

$$\bar\varphi(m+\ker\varphi)=\varphi(m)$$

$\bar\varphi$ is ① well defined, trivial
② $\bar\varphi$ is bijetive hom of ab. group
③ $\bar\varphi(rm+\ker\varphi)=\varphi(rm)$
$=r\varphi(m)$
$=r\bar\varphi(m+\ker\varphi)$

so $M/\ker\varphi \cong N$

Note: $L, N \leq M$
then $L+N=\{l+m \mid l\in L, n\in N\}$

$L+N \leq M$
and $L\cap N \leq M$

second isomorphism theorm:

$$\frac{L+N}{L} \cong \frac{N}{L\cap N}$$

proof :

$$\begin{tikzcd}
N \arrow[r, "i"] \arrow[dr, "\phi=\pi\circ i"'] & L+N \arrow[d, "\pi"] \\
 & \frac{L+N}{L}
\end{tikzcd}$$

if $x\in \frac{L+N}{L}$ then

$x=(l+n)+L$
$=n+L$
$=\phi(n)$

$$\phi : N \longrightarrow \frac{N+L}{L}$$

$$n \longmapsto n+L$$

$\phi(n)=n+L=x$

as i, π is R-linear

so ϕ is surjetive R-linear, so

$$N/\ker\phi \cong \frac{L+N}{L}$$

let $n \in \ker \phi$ then

$$n + L = L$$

or $n \in L$

as $n \in N$ we have

$n \in N$ and L

$\Rightarrow n \in N \cap L$

now $\forall x \in N \cap L$

as $x \in N$

and $x \in L$

we have

$\phi(x) = x + L$

as $x \in L$

$\Rightarrow \phi(x) = L$

or $x \in \ker \phi$

$\therefore \ker \phi = N \cap L$

so $\dfrac{N}{N \cap L} \cong \dfrac{L + N}{L}$

17th oct :

Theorm : If R is a commutative ring and $f: R^n \to R^e$ is isomorphism then $n = e$

Now before the proof of this lemma, we will look at some more stuff:

Def^n: when M is R-module

$\text{ann}_R M$ is the anihilator of M

$$\text{ann}_R M = \{ r \in R \mid rm = 0 \ \ \forall m \in M \}$$

Note : $\text{ann}_R M \leq R$

proof :

① $0 \in \text{ann}_R M$

② if $a, b \in \text{ann}_R M$

$$(a-b)m = am - bm = 0$$
$$\Rightarrow a - b \in \text{ann}_R M$$
$$\Rightarrow (\text{ann}_R M, +) \leq (R, +)$$

③ Now if $r \in \text{ann}_R M$

$\forall t \in R$
$\& \ m \in M$

we have $(tr)m = t(rm) = t \cdot 0 = 0$

or $tr \in \text{ann}_R M$

$$\Rightarrow \text{ann}_R M \leq R$$

Note : M is an $R/\text{ann}_R M$ - module

proof :

$$(r + \text{ann}_R M) \cdot m := rm + \underbrace{r'm}$$

$r' \in \text{ann}_R M$
$\Rightarrow r'm = 0$

$$= rm$$

now $(r + \text{ann}_R M) \cdot m = rm$ is well-defined :

$$r + \text{ann}_R M = s + \text{ann}_R M$$
$\Rightarrow r = s + t$, for some $t \in \text{ann}_R M$
$$\Rightarrow rm = sm + tm$$
$$\Rightarrow rm = sm$$

$\therefore$ the action is well defined

to show M is a module over $R/\text{ann}_R M$

① $R' \times M \to M$

② M is an abelian group

③ $1_{R'}(m) = m$

④ $r_1' r_2' (m) = (r_1'(r_2' m))$

⑤ $(r_1+r_2)(m) = r_1 m + r_2 m$
& $r(m_1+m_2) = rm_1 + rm_2$

now ① is done
so is ②
if we show other as well, we are done

Note : M, L are R-modules:
$f : M \longrightarrow L$ is R-linear
then
$N \leq \ker f$

$\Rightarrow \tilde{f} : M/N \longrightarrow L$ is R-linear

proof : as $\tilde{f} : M/N \longrightarrow L$
$m+N \longmapsto f(m)$

or $\tilde{f}(m+N) = f(m)$

$m+N = m'+N$
$\Rightarrow f(m) = f(m')$ ∴ well defined

similarly others can be proved here

Note : Theorm A is true $n=e$ (for comm rings)

Note : $I \leq R$
$\hookrightarrow$ ideal of R
then

$$IM = \{\underbrace{\Sigma\, i_j m_j}_{\text{finite sum}} \mid i_j \in I, m_j \in M\}$$

Exe : $IM \leq M$
here
$$IM = \{\Sigma\, i_j m_j \mid i_j \in I, m_j \in M\}$$
then
$\forall\, m \in M$
$m(i_1 m_1 + \cdots i_m m_m)$
$\Rightarrow \underset{\in IM}{i_1 m_1 m} + \cdots \underset{\in IM}{i_m m_m m}$

so $IM \leq M$
$\hookrightarrow$ ideal of M

Note : $I \leq \operatorname{ann} M/IM$

as $\bar{m} \in M/IM$
then

$i \in I$
then $i\bar{m} = \overline{im} = \bar{0}$

Theorm : (B) $\varphi : R^n \longrightarrow R^l$ is surjetive $\Rightarrow n \geq l$

Here see that theorm B $\Rightarrow$ theorm A

as $f : R^n \longrightarrow R^l$ is iso
$\Rightarrow$ is surj
$\Rightarrow n \geq l$

sim. $f^{-1} : R^l \longrightarrow R^n$ is iso
$\Rightarrow$ is surj
$\Rightarrow l \geq n$

$\therefore \; l = n$

proof : m be a maximal ideal of R, then

$$\begin{tikzcd}
R^n \arrow[r, "\phi"] \arrow[dr, "\psi"'] & R^l \arrow[d, "\eta"] \\
& \frac{R^l}{mR^l} = \left(\frac{R}{m}\right)^l
\end{tikzcd}$$

$\psi : R^n \longrightarrow (R/m)^l$ is surj

as

① ϕ is surj
② η is surj

now $t \in mR^n$
then
$t = \alpha_1 m_1 + \cdots \alpha_s m_s \qquad \alpha_i \in R^n$
$\qquad\qquad\qquad\qquad\qquad m_i \in m$

$\phi(t) = \phi(\alpha_1) m_1 + \cdots \phi(\alpha_s) m_s \in mR^l$

as $\phi(t) \in mR^l \in \ker(\eta)$

$\Rightarrow \psi(t) = \eta \circ \phi(t) = 0$

$\therefore \forall t \in mR^n \Rightarrow t \in \ker(\psi)$

$\Rightarrow mR^n \subseteq \ker \psi$

then $R^n / mR^n \xrightarrow{\bar{\Psi}} R^l / mR^l$

$\quad \|$

$\bar{\Psi} : (R/m)^n \longrightarrow (R/m)^l$

as R/m is a field $\Rightarrow$ module is the vector space

$\Rightarrow$
$\bar{\Psi} : K^n \longrightarrow K^l$

$\Rightarrow n \geq l$

local rings:

we say R is a local ring
if R has a unique maximal ideal m

Example: R is a ID
P is prime in R
$S = R \setminus P$
$S^{-1}R$ is local with unique maximal ideal $PS^{-1}R$

Nakayama's lemma:

(R, M) is local
N is a f.g R-module (f.g is finitely generated)

if $N = mN \Rightarrow N = 0$

proof: $N = \langle n_1, \cdots n_r \rangle$

$n_r \in N = mN$
$n_r = a_1 n_1 + \alpha_2 n_2 + \cdots a_n n_r$
$\alpha_i \in m$
$(1-\alpha_1) n_r = \alpha_1 n_1 + \cdots \alpha_{r-1} n_{r-1}$

as (R, M) is local
$e \in m \Rightarrow 1 - e$ is a unit in R
as
$1 - e$ is not a unit $\Rightarrow 1 - e \in M$
$\Rightarrow 1 \in M$ *

so, $n_r = \frac{\alpha_1}{1-\alpha_r} n_1 + \frac{\alpha_2}{1-\alpha_r} n_2 + \cdots \frac{\alpha_{r-1}}{1-\alpha_r} n_{r-1}$

$\Rightarrow N = \langle n_1, \dots, n_{r-1} \rangle$

$\downarrow$

$N = \langle n_1 \rangle$

now as $N = mN \Rightarrow n_1 = \alpha n_1 \quad \alpha \in M$
$\Rightarrow (1-\alpha) n_1 = 0$
$\Rightarrow n_1 = 0$
as $1-\alpha$ is a unit

$\Rightarrow N = 0$

Note: $M = \langle m_1, \dots m_r \rangle$

f.d k-vector space $\frac{M}{mM} = \langle \bar{m}_1, \dots \bar{m}_r \rangle$
then $\{\bar{m}_1, \dots \bar{m}_s\}$ basis of M/mM

$N = \langle m_1 \dots m_s \rangle$
then $\frac{M}{mM} = \frac{N + mM}{mM} \Rightarrow M = N + mM$

If R is local: then $M = N$:

proof: $E = M/N = \langle m_{s+1}, \dots m_r \rangle$

$$mE = \frac{mM}{N} = \frac{N + mM}{N} = \frac{M}{N} = E$$

$\Rightarrow mE = E$

$\Rightarrow E = 0$

$\Rightarrow M = N$

24th oct:

Theorm: R is a PID, M is a f.g R-module then:

$$M = R^s \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_l)$$

where $a_1 | a_2 \cdots | a_l$ & $s \geq 0$

Here using this lemma, if G is a f.g abelian group then

$$G \cong \mathbb{Z}^s \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \mathbb{Z}/n_l\mathbb{Z}$$

$n_1 | n_2 | \cdots n_s$, $s \geq 0$

as if G is a f.g abelian group then it is a $\mathbb{Z}$-module

as ① $(n_1)(g_1+g_2) \in G$
② $(n_1+n_2)(g) \in G$
③ $(n_1)(n_2)(g) \in (n_1n_2)(g)$

Lemma: R is any comm ring

$\varphi : M \longrightarrow R^s$

s.t φ is surjective

then $M \cong \ker\varphi \oplus R^s$

proof: let $\{e_1, \ldots e_s\}$ be std basis of R^s

φ is surjective then

$\varphi(m_i) = e_i$ for $m_i \in M$

defin $\theta : R^s \longrightarrow M$

$a_1e_1 + \cdots a_se_s \longmapsto a_1v_1 + \cdots a_sv_s$

for $v_i \in M$

$$\begin{tikzcd} R^s \arrow[r, "\theta"] \arrow[dr, "1"'] & M \arrow[d, "\varphi"] \\ & R^s \end{tikzcd}$$

(as $R^s \xrightarrow{1} R^s$
$\varphi(\theta(w)) = w$)

now $\pi : \ker\varphi \oplus R^s \longrightarrow M$

$(u, w) \longrightarrow u + \theta(w)$

as $\ker\varphi \leq M$

& $\theta(w) \in M$

then $\pi(u,w) = 0$

$\Rightarrow u + \theta(w) = 0$

$\Rightarrow \theta(w) = -u$ ← ker of φ

$\Rightarrow w = \varphi(\theta(w)) = -\varphi(u)$
$= 0$

$\Rightarrow w = 0$

$\Rightarrow \theta(w) = 0$

$\Rightarrow u = 0$

$\Rightarrow \ker\pi = \{0\}$ (π is 1-1)

$\Rightarrow \ker(\varphi) \oplus R^s \cong M$

Note: $m \in M$, $w = \varphi(m) \in R^s$

then $\varphi(\theta(w)) = w = \varphi(m)$

$\theta(w) - m \in \ker\varphi$

$\theta(w) - m = u \in \ker\varphi$

$m = \theta(w) + (-u)$ ← from $\ker\varphi$

↖ from R^s

Prop^n: R be a PID and M be a finitely generated free module over R of rank n. Then every submodule of M is also free of rank $\leq n$.

or (Prof proved this)

R is PID and $N \subseteq R^s$ then N is also free s.t $N = R^a$ where $a \leq s$

proof: for $N = \{0\}$, this is the trivial case where our lemma is true. For $N \neq \{0\}$

let $s = 1$ then:

$N \subseteq R$

as R is a PID

$\Rightarrow N = \langle \alpha \rangle$

or N is also free s.t

$$N = \langle \alpha \rangle \cong R^1$$

as $\varphi : R \longrightarrow \langle \alpha \rangle$

$s \longmapsto s\alpha$

① φ is well-defined
② φ is Homomorphism
③ φ is one-one
④ φ is onto

} all trivial

now, let's suppose for $s \leq n-1$ the lemma is true. Then

let $\pi_i : R^n \longrightarrow R$

↑ projection linear maps

then

as $N \neq 0$ $\exists\, n \in N$ s.t $n = (n_1, \dots, n_n)$ where $n_i \neq 0$

for that i

$$\pi_i(n) = (n_i) \neq 0$$

$\therefore \pi_i(N) \neq 0$

$\Rightarrow \pi_i(N) \leq R$

$\Rightarrow \pi_i(N) = \langle \alpha \rangle \cong R$ (Already proved)

now as $\pi_i(N) = \langle \alpha \rangle$, $\exists\, v \in N$ s.t $\pi_i(v) = \alpha$

also $\ker(\pi_i) \cap N < \ker(\pi_i)$ where rank $\ker(\pi_i) = n-1$

$\Rightarrow$ rank $\ker(\pi_i) \cap N \leq n-1$

$$N = (\ker \pi_i \cap N) \oplus Rv$$

($\because \tilde{\pi}_i : N \xrightarrow{\sim} Rv$
$N = \ker \tilde{\pi}_i \oplus Rv$)
from prev

then as Rank $[\ker \pi_i \cap N] \leq n-1$ we have Basis of $\ker \pi_i \cap N = \{e_1 \dots e_m\}$

where $m \leq n-1$
& Basis of $Rv = \{v\}$

or Basis of $N = \{\underbrace{e_1 \dots e_m, v}_{m+1 \leq n-1+1 = n}\}$

$\therefore$ for n also true

$\therefore N \cong R^k$ where $k \leq s$

Theorm: (structure theorm)
let R be a PID, M be a f.g free module over R of rank n ($M \cong R^n$) and
$0 \neq N \leq M$ (N is a submodule of M)
then $\exists$ basis
$\{e_1, e_2, \dots e_n\}$ of M and $a_i \neq 0$ s.t
$\{a_1 e_1, \dots a_r e_r\}$ is a basis for N
&
$a_1 | a_2 | a_3 \dots | a_r$

Proof: let $\mathcal{F} = \{T(N) ; T \in Hom_R(M, R)\}$
then
let (α) be maximal of $\mathcal{F}$
as $N \neq 0$
$N \ni n = (n_1 \dots n_n)$
$n_i \neq 0$ (there will be atleast one i s.t $n_i \neq 0$)

$$\Rightarrow \underset{\overset{\uparrow}{\text{Projection}}}{\pi_i} : M \longrightarrow R \qquad \pi_i \in Hom(M, R)$$

$\Rightarrow \pi_i(N) \in \mathcal{F}$
where
$\pi_i(N) \neq 0$

$\Rightarrow (\alpha) \neq 0$

now, as $\mathcal{F}$ has maximal element α
$\exists T_0(N) \in \mathcal{F}$
s.t $T_0(N) = (\alpha)$
$\exists v \in N$ s.t
$T_0(v) = \alpha$

now, as $T_0(v) = \alpha$

$\forall T(N) \in \mathcal{F}$
we have
$T \in Hom(M, R)$
let $d = gcd(\alpha, T(v))$
then
as $d \in R$ (which is a PID)

$d = x\alpha + y T(v)$
$= x T_0(v) + y T(v)$
$d = (x T_0 + y T)(v) \in \mathcal{F}$

$\Rightarrow d \in \mathcal{F} \Rightarrow (d) \subseteq (\alpha)$
also as $d = gcd(\alpha, T(v))$

we have
$(\alpha) \subseteq (d)$

$\therefore (\alpha) = (d)$
$\Rightarrow \alpha = a$

or $\alpha \mid T(v) \quad \forall\, T \in \mathrm{Hom}(M,R)$

then let $\pi_i : M \longrightarrow R$
be a projection
then $\pi_i \in \mathrm{Hom}(M,R)$
$\therefore \alpha \mid \pi_i(v)$
$= \alpha \mid v_i \quad \forall\, i = 1,2....n$

or $v = (v_1, ...v_n)$
$= (\alpha \omega_1. ....\alpha \omega_n)$
$v = \alpha(\omega_1....\omega_n)$
$\Rightarrow v = \alpha \omega$
where $\omega = (\omega_1 .... \omega_n)$

now, as $v = \alpha \omega$
$T_0(v) = T_0(\alpha \omega)$
$\alpha = \alpha T_0(\omega)$
$\Rightarrow T_0(\omega) = 1$

now, $T_0 : M \longrightarrow R$
is sujetive as $T_0(\omega) = 1$
$T_0(\gamma \omega) = \gamma$
$\forall\, \gamma \in R$
$\therefore \forall\, \gamma \in R, \exists\, \gamma \omega \in M$ s.t
$T_0(\gamma \omega) = \gamma$

then $M \cong \mathrm{Ker}(T_0) \oplus R\omega$ ← as $T_0 : M \to R\omega$ is surjetive
$\Rightarrow M \cong \mathrm{Ker}(T_0) \oplus R\omega$

similarly $\tilde{T}_0 : N \longrightarrow Rv$
then $\mathrm{Ker}(\tilde{T}_0) = \mathrm{Ker}\, T_0 \cap N$
$\therefore N \cong \mathrm{Ker}(\tilde{T}_0) \oplus Rv$
$N \cong [\mathrm{Ker}\, T_0 \cap N] \oplus Rv$ ← as $T_0 : N \to Rv$ is sujetive (see the above proof for surj)

now by induction, $\mathrm{Ker}\, T_0$ has bases $\{e_2, ... e_n\}$
s.t $\{a_2 e_2, ... a_r e_r\}$ is basis for $\mathrm{Ker}\, T_0 \cap N$

then $\{e_1 = \omega, e_2, ... e_n\}$ basis for M
$\{a_1 e_1 = \alpha \omega, \alpha_2 e_2, ... \alpha_r e_r\}$ basis for N
where $a_2 \mid a_3 \mid a_4 ... \mid a_r$

now for $a_1 | a_2$ i.e $\alpha | a_2$

let $T(e_1) = 1 = T(e_2)$
or else 0

then as $\alpha | T(v)$

$g \in Hom(M, R)$

and $g(e_1 a_1) = a_1 = \alpha$

here $(\alpha) \subseteq g(R^n)$

but as (α) is maximal

$\Rightarrow (\alpha) = g(R^n)$

$\Rightarrow g(a_2 e_2) = a_2 \in (\alpha)$

$\Rightarrow (a_2) \subseteq (a_1) = (\alpha)$

$\Rightarrow a_1 | a_2$

Applications of Structure theorm :

propn : R is a PID, M is a f.g R-module, then

$$M \cong R^s \oplus R/(a_1) \oplus R/(a_2) \oplus R/(a_3) \cdots \oplus R/(a_r)$$

where $a_1 | a_2 | \cdots a_r$

proof : $M = \langle m_1, \ldots m_n \rangle$

then $\varphi : R^n \longrightarrow M$

s.t φ is surjective

$$\varphi : R^n \longrightarrow M$$
$$(a_1, \ldots a_n) \longmapsto a_1 m_1 + \cdots a_n m_n$$

where $\ker\varphi \leq R^n$

then $\exists$ Basis $\{e_1 \ldots e_n\}$ of R^n s.t

$\{a_1 e_1 \ldots a_r e_r\}$ are basis of $\ker\varphi$

where $a_1 | a_2 | \ldots a_r$

$$\ker\varphi = N = R(a_1 e_1) \oplus R(a_2 e_2) \oplus R(a_3 e_3) \oplus \cdots R(a_r e_r)$$

$R^n / \ker\varphi \cong M$ (isomorphism theorm)

$$R^{n-r} \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots R/(a_r)$$

where $a_1 | a_2 \cdots | a_r$

Note : If $N \subseteq R^n \Rightarrow N = R^s$ where $s \leq n$
$\hookrightarrow$ PID

also if $\psi : R^r \longrightarrow R^n$

then ψ can be represented as $n \times r$ matrix

Basis of R^r $\{e_1 \ldots e_r\}$

Basis of R^n $\{n_1 \ldots n_n\}$

then ψ is $[\psi(e_1) \ldots \psi(e_r)]_{n \times r}$

lemma : (R,π) be a local PID where π is the irreducible element

then $\varphi : R^r \longrightarrow R^n$ be a linear map
then $\exists$ basis of R^r and R^n s.t
wrt this Basis

$$\varphi = \left(\begin{array}{cccc|c} \pi^{a_1} & & & & \\ & \pi^{a_2} & & & \\ & & \ddots & & \\ & & & \pi^{a_e} & 0 \\ \hline & & 0 & & 0 \end{array}\right)_{n\times r}$$

where $a_1 \leq a_2 \leq \cdots\cdots a_e$

proof : for $r=1$ φ is $n\times 1$ matrix

e_1 is a basis then

$$\varphi(e_1) = v_1 = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

where $\alpha_i = \pi^{r_i} u_i$

then $$v_1 = \begin{pmatrix} \pi^{r_1}u_1 \\ \vdots \\ \pi^{r_n}u_n \end{pmatrix} \rightarrow \begin{pmatrix} \pi^{r_0}u_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$ where $r_0 = \min\{r_1 \ldots r_n\}$

as By row transformation

$$R_i - \pi^{r_i - r_0} R_1$$

$$\varphi = \begin{pmatrix} \pi^{r_0}u_1 \\ \vdots \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} \pi^{r_0} \\ \vdots \\ 0 \end{pmatrix}$$ as u_1 is a unit

now for $$\varphi = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{r1} & \cdots & \cdots & a_{rn} \end{pmatrix}_{n\times r}$$

where $a_{ij} = \underset{\substack{\uparrow \\ \text{unit}}}{u_{ij}} \pi^{r_{ij}}$

let $a_{11} = u_{11}\pi^{r_{11}}$ where $r_{11} = \min\{r_{ij}\}$

then $R_i - \frac{u_{j1}}{u_{11}} \pi^{r_{j1}-r_{11}} R_1$

to get $\swarrow$ column transformation

$$\begin{pmatrix} a_{11} & \begin{array}{c|ccc} \end{array} 0 \; . \; . \; . \; 0 \\ \hline 0 & \varphi' \end{pmatrix} \qquad C_i - \frac{u_{1j}}{u_{11}} \pi^{r_{1j}-r_{11}}$$

as $\varphi' : R^{r-1} \longrightarrow R^{n-1}$ By induction true

now as $N \subseteq F = R^n$
$\{e_1 \dots e_n\}$ of R^n

at last $\left(\begin{array}{ccc|c} \pi^{c_1} & & & \\ & \pi^{c_2} & & 0 \\ & & \ddots \pi^{c_l} & \\ \hline & 0 & & 0 \end{array}\right)_{n \times r}$

(we can reduce matrices like this as we were asked to find bases not use particular basis)

as $\{\pi^{c_1} e_1, \pi^{c_2} e_2, \dots \pi^{c_l} e_l\}$
Basis of N we get
$\pi^{c_1} \mid \pi^{c_2} \mid \dots \mid \pi^{c_l}$
$\Rightarrow c_1 \leq c_2 \leq \dots \leq c_l$

28th oct :

Recap: R is a PID , M is a f.g R module

$$M \cong R^s \oplus R/(a_1) \oplus \cdots\cdots R/(a_r)$$

where

$$a_1 | a_2 | a_3 \cdots | a_r$$

now, if G is a f.g abelian group then

$$G \cong \mathbb{Z}^s \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}_{n_r}\mathbb{Z}$$

$$n = p_1^{a_1} \cdots p_l^{a_l}$$

where $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l^{a_l}$

Rational canonical form :

If K is a field s.t V is a vector-space & $V \cong K^m$

let $T : V \to V$

Be a linear transformation

now, V is a K[X] module (can be proved)

where

$$X . v = T(v)$$

i.e V is a f.g K[X] module

then

$$V = (K[X])^s \oplus \frac{K[X]}{(f_1)} \oplus \cdots \frac{K[X]}{(f_r)}$$

but as $V \cong K^m$ ← finitely generated

$K[X] \cong K^\infty$ ← infinity generated

we have

$$s = 0$$

or $$V \cong \frac{K[X]}{(f_1(x))} \oplus \cdots \oplus \frac{K[X]}{(f_r(x))}$$

$$\underset{\uparrow}{W} = \frac{K[X]}{f(X)}$$

W is a vector space then if

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0$$

then basis of W are :

$$\{1, X, X^2, \ldots X^{n-1}\}$$

Matrix representation of T_V will be :

$$T_V : W \to W$$

$X . X^i = X^{i+1}$ for $i \leq n-2$

or what we get here is :

$T_V(1) = X.(1)$

$T_V(X^k) = X(X^k)$ $k \leq n-1$

then $T_v(1) = x = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$T_v(x) = x^2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$T_v(x^{n-2}) = x^{n-1} \quad \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

$T_v(x^{n-1}) = x^n = -a_{n-1}x^{n-1} - a_{n-2}x^{n-2} \cdots - a_0 x^0$

or

$\begin{pmatrix} -a_0 \\ -a_1 \\ \vdots \\ -a_{n-1} \end{pmatrix}$

$$\therefore \quad T_v := \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & & 0 & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{bmatrix}$$

Rational canonical form

Note : $K[x]/f(x)$ as rational canonical form then

$$G = \mathbb{Z}^s \oplus \cdots \oplus \mathbb{Z}/p^{r_p}\mathbb{Z}$$

$\uparrow$ Rational canonical form $\quad \uparrow$ Rational canonical form $\quad \uparrow$ Rational canonical form

$$T_v = \left[\begin{array}{c|c|c} (\downarrow) & 0 & 0 \\ \hline 0 & (\swarrow) & 0 \\ \hline 0 & 0 & (\leftarrow) \end{array}\right]$$

Jordan canonical form :

k is a field $V \cong k^m$

$T : V \longrightarrow V$

linear trasformation

$f(x) = \prod (x-\alpha_i)^{r_i}$

then

$$\frac{k[x]}{(f(x))} = \frac{k[x]}{(x-\alpha_1)^{r_1}} \oplus \frac{k[x]}{(x-\alpha_2)^{r_2}} \oplus \cdots \oplus \frac{k[x]}{(x-\alpha_l)^{r_l}}$$

(only 1)

now if $W = \frac{k[x]}{(x-\alpha)^n}$

then Basis : $\{w_0, w_1, \ldots, w_{n-1}\}$

$\{(x-\alpha)^0, (x-\alpha)^1, \ldots (x-\alpha)^{n-1}\}$

$= \{1, (x-\alpha)^1, \ldots (x-\alpha)^{n-1}\}$

$x \cdot w_i = T(w_i)$ for $i \leq n-2$

or $T(w_i) = x(x-\alpha)^i$

$T(w_i) = (x-\alpha+\alpha)(x-\alpha)^i$

$= (x-\alpha)^{i+1} + \alpha(x-\alpha)^i$

or $T(w_i) = w_{i+1} + \alpha w_i$

& $T(w_{n-1}) = 0 + \alpha w_{n-1}$

then $T := \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 1 & \alpha & & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & 1 & \alpha \end{bmatrix}_{n \times n}$ also called Jordan canonical form

Noetherian rings and modules :

R - comm ring, M is R-module

Def^n : M is Noetherian if for any $N_1 \leq N_2 \leq \cdots$ $N_i \leq M$

$\exists i_0$ s.t

$N_i = N_{i_0}$ $\forall i \geq i_0$

Def^n : R is Noetherian ring if R as an R-module is Noetherian.

Theorm : R is noetherian ring $\Leftrightarrow$ every ideal in R is f.g

proof :

(⇒) suppose if possible $\exists\, I \leq R$ s.t I is not finitely generated, then

$a_1 \neq 0$, $a_1 \in I$
where
$I_1 = (a_1)$
take $a_2 \in I \setminus I_1$
s.t $I_2 = (a_1, a_2)$
Note : $I_1 \subsetneq I_2$
$a_3 \in I \setminus I_2$

then $I_3 = (a_1, a_2, a_3)$
$I_2 \subsetneq I_3$

sim, $I_n = (a_1, \ldots a_n)$
if $I_n \neq I$
then
$\exists\, a_{n+1} \in I \setminus I_n$
s.t
$I_{n+1} = (a_1 \ldots a_n, a_{n+1})$

so, $I_1 \subsetneq I_2 \subsetneq I_3 \ldots \subsetneq I_n \subsetneq I_{n+1} \subseteq \ldots\ldots I$

as R is noterian,
chain terminates at some no
then
$I_1 \subsetneq I_2 \ldots \subsetneq I_{n_0} = \ldots\ldots I_n \ldots\ldots = I$
s.t
$\forall n \geq n_0 \quad I_{n_0} = I_n$
or $I = I_{n_0}$
$= (a_1, \ldots a_{n_0})$
$\therefore$ I is finitely generated

(⇐) suppose every ideal in R is f.g then
$I_1 \subseteq I_2 \subseteq \ldots\ldots \leftarrow$ chain

where $J = \bigcup_{n \geq 1} I_n \leq R$

as $I_1 \subseteq I_2 \subseteq \ldots\ldots \leftarrow$ chain terminates
we have $n_0 \in \mathbb{N}$
s.t
$I_{n_0} = I_n \;\forall n \geq n_0$

if $J = \bigcup_{n \geq 1} I_n \leq R$
also
as $J \leq R \Rightarrow J = (j_1, \ldots j_l)$
$\uparrow$
ideal so finitely generated

or $\exists\, m_i \in \mathbb{N}$ s.t
$j_i \in I_{m_i}$, let $n_0 = \max\{m_1, \ldots m_l\}$
then $J \leq I_{n_0} \leq I_n \leq J$
or $\forall n \geq n_0 \quad I_{n_0} = I_n$
so R is noetherian

Exaple: $k[X,Y]$ is noeterian as

$$I = (X,Y)^n = (X^n, X^{n-1}Y, \dots XY^{n-1}, Y^n)$$

↙ some ideal of $k[X,Y]$

↑ finitey gerated

∀ Ideal of R is finity gerated ⇒ R is noeterian

Theorm: M is R-module then

M is Noeterian ⇔ every submodule N of M is f.g

proof: very similar to above

lemma: R is a R-module & $I \leq R$ then

R is noetherian ⇒ R/I is also neotherian

proof:

let $E \leq R/I$

then $\exists\ K \leq R$

s.t $I \leq K$ & $E = K/I$

as R is noetrian ⇒ K is neotrian

and so K is f.g & so is I

∴ E is finitely gerated R-module

as E is finitely gerated R module we have

$\forall E \leq R/I$

↑

every ideal of R/I is finety gerated

⇒ R/I is Noeterian

(R is noetrian ⇔ $\forall I \leq R$, I is f.g)

lemma: R is a noetherian ring also a domain then for S to be m.c $S^{-1}R$ is also noetherian.

proof: For $J \leq S^{-1}R$

$J = (J \cap R) S^{-1}R$ (already proved)

⇒ $J = (a_1 \dots a_l) S^{-1}R$

as $J \cap R \leq R$

↑

ideal of R (a noetrian ring)

⇒ $J = \left(\frac{a_1}{1} \dots \frac{a_l}{1}\right)$

∴ J is finety gerated

⇒ $S^{-1}R$ is noetherian

Note: $R = k[x_1 \dots x_n \dots]$ is not noeterian as

$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \dots$ ← chain does not terminate

Theorm: R is Noeth ring, M is f.g R-module
$\Rightarrow$ M is noetherian

lemma-1: If M is noet R-module & $N \leq M$ then
M/N is Noetherian

proof: For $E \leq M/N$

$L \leq M$, $L \geq N$

or

$E = L/N$

as $\underset{\uparrow}{L} \leq M$

L is f.g $\Rightarrow$ E is f.g $\Rightarrow$ M/N is noetherian

Remark: For M be f.g $\Rightarrow$ M is notherian it is suff to prove
as $M \cong R^s / \ker \phi$

R^s is noetrian, $\ker \phi \leq R^s$ is also noet $\Rightarrow$ $R^s/\ker \phi$ is noet (above)

As $M = \langle m_1, \dots m_s \rangle \leftarrow$ f.g

$\phi : R^s \longrightarrow M$

s.t $(a_1 \dots a_s) \longmapsto (a_1 m_1 + \dots \dots a_s m_s)$
(surjective maps)

$M \cong R^s / \ker \phi$

lemma-2: M, N is Noeth $\Rightarrow$ $M \oplus N$ is Noeth

proof:

$\pi : M \oplus N \longrightarrow M$
$(m, n) \longmapsto m$

then $N = \ker \pi$

let

$K \leq M \oplus N$

then

$\pi(K) \leq M$

or $\pi(K) = (\bar{u}_1, \dots \bar{u}_r)$

& as $K \cap N \leq N \Rightarrow (v_1 \dots v_s) = K \cap N$

let $u_i \in K$ s.t $\pi(u_i) = \bar{u}_i$

claim: $K = (u_1 \dots u_r, v_1 \dots v_s)$

as $\alpha \in K \Rightarrow \pi(\alpha) \in \pi(K)$

$\Rightarrow \pi(\alpha) = a_1 \bar{u}_1 + \dots a_r \bar{u}_r$
for $a_i \in R$

let

$\tilde{\alpha} = a_1 u_1 + \dots a_r u_r$
$\in K$

then

$\pi(\tilde{\alpha}) = a_1 \bar{u}_1 + \dots a_r \bar{u}_r$
$= \pi(\alpha)$

$\Rightarrow \pi(\tilde{\alpha} - \alpha) = 0$

$\Rightarrow \tilde{\alpha} - \alpha \in \ker \pi \cap K$
as $\alpha, \tilde{\alpha} \in K$

$\Rightarrow \alpha - \tilde{\alpha} = d_1 v_1 + \dots d_s v_s$

$\Rightarrow \alpha = \tilde{\alpha} + d_1 v_1 + \dots d_s v_s$

$\Rightarrow K = (u_1, \dots u_e, v_1 \dots v_s)$

Cor : R is noeth $\Rightarrow R^n$ is noeth

proof :

as R is noeth $\Rightarrow R \oplus R$ is noeth
$\Rightarrow R^2$ is noeth

By induction

$$R^n = \underset{\substack{\uparrow \\ \text{noeth}}}{R^{n-1}} \oplus \underset{\substack{\uparrow \\ \text{noeth}}}{R} \Rightarrow R^n \text{ is noeth}$$

$T : V \to V$
T is surjective $\Rightarrow$ T is iso
T is 1-1 $\Rightarrow$ T is iso
} Basic Rank – nullity

Note : as $M \cong R^s / \ker \phi$
where R^s is noetherian
$\ker \phi \leq R^s \Rightarrow \ker \phi$ is noeth

$\Rightarrow R^s / \ker \phi \cong M$ is noeth

Theorem : M is noeth R-module then if

$f : M \to M$ is surjective
$\Rightarrow f : M \to M$ is injective ($\ker f = \{0\}$)

proof : Here

$\ker(f) \subseteq \ker(f^2) \leq . . . .$
then $\exists n_0 \in \mathbb{N}$ s.t
$\forall n_0 \geq n$

$$\ker(f)^{n_0} = \ker(f)^n$$

then, if $m \in \ker f$
$\Rightarrow f(m) = 0$

f^{n_0} is surjective

as

$$\begin{tikzcd} M \arrow[r, "f"] & M \arrow[r, "f"] & M \arrow[r, dashed] & M \arrow[r, dashed, "f"] & M \end{tikzcd} \leftarrow n_0 \text{ times}$$

f is surjective
$\Rightarrow f^{n_0}$ is surjective

$\therefore \exists t \in M$ s.t $m = f^{n_0}(t)$
$\Rightarrow f(m) = f^{n_0+1}(t)$
$\Rightarrow 0 = f^{n_0+1}(t)$
$\Rightarrow t \in \ker f^{n_0+1} = \ker f^{n_0}$
$\Rightarrow f^{n_0}(t) = 0$
$\Rightarrow m = 0$
$\Rightarrow \ker(f) = \{0\}$
$\Rightarrow$ f is injective

29th oct :

Theorm : (Hilbert Basis theorm)
let R be Noeth ring then $R[X]$ is noeth

(Here $R[X, Y] = (R[X])[Y]$
is also noeth)

proof : let $I \neq 0$ be an ideal in $R[X]$
$0 \neq f \in R[X]$
then
$f = a_n x^n + \cdots a_1 x + a_0$
leading term
$LT(f) = a_n$
Note : $LT(0) = 0$

then $\underset{\substack{\uparrow \\ \text{ideal of } R}}{J} = \langle LT(f) \mid \forall f \in I \rangle \leq R \Rightarrow J = \langle LT(f_1), \ldots LT(f_s) \rangle$
s.t $f_i \in I$

now, if $\deg f_i = r_i$
& $r = \max\{r_i\}$

if
$E = A \oplus Ax \oplus \cdots \oplus Ax^{r-1}$
then
$E \cap I$ is f.g A-module
as $\underset{\substack{\uparrow \\ \text{sub} \\ \text{module}}}{E \cap I} \leq \underset{\substack{\uparrow \\ \text{fg A module}}}{E}$
$\Rightarrow$ f.g

let $E \cap I = \langle v_1 \ldots v_e \rangle$

claim : $K = I$ then for $K = \langle v_1 \ldots v_e, f_1 \ldots f_s \rangle$

using induction for $f \in I$ case ① $\deg f \leq r-1$
then
$f \in E \cap I = \langle v_1 \ldots v_e \rangle$
$\Rightarrow f \in K$

② $\deg f \geq r$
if for $\deg f = m-1$ true
then
for $\deg f = m$
we have
$f = a x^m +$ lower terms
$a = LT(f) \in \langle LT(f_1), \ldots LT(f_s) \rangle$

$\Rightarrow a = \sum \alpha_i LT(f_i)$

If $h = \sum \alpha_i x^{m - r_i} f_i$
then
$\deg$ of $h = m$
&
$f - h \in I$ by induction
as $\deg f - h < m$

as $h \in I \Rightarrow f \in I$
or $K = I = \langle v_1 \ldots\ldots v_e, f_1 \ldots f_s \rangle$
$\Rightarrow I$ is f.g for $I \leq R[X]$
$\Rightarrow R[X]$ is noeth

Invariant theory :

$R = \mathbb{C}[x_1 \dots x_n]$

for $G \leq GL_n(\mathbb{C})$

$|G| < \infty$

s.t $\sigma \in G$

$\uparrow$

a matrix then

$$\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix}$$

or for $f \in R$

$$\sigma(f(x_1 \dots x_n)) = f(\sigma(x_1), \dots \sigma(x_n))$$

Defn: $R^G = \{ f \in R \mid \sigma(f) = f, \forall \sigma \in G \}$

Here $\sigma(f) = f$ or f is invariant wrt σ.

What we want to see/find is that if R^G is noetherian or not as if yes then $\exists f_1 \dots f_r \in R^G$ s.t

$$R^G = \mathbb{C}[f_1 \dots f_r]$$

Example: $\mathbb{C}[x,y]$: $\sigma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

then

$$\langle \sigma \rangle = G \cong \mathbb{Z}/2\mathbb{Z}$$

also, $\sigma(f(x,y)) = f(\sigma(x), \sigma(y))$

where

$\sigma(x) = -x$

$\sigma(y) = -y$

$$\Rightarrow \sigma(f(x,y)) = f(-x,-y)$$

then

① $\sigma(x^2) = (-x)^2 = x^2$

② $\sigma(y^2) = y^2$

③ $\sigma(xy) = xy$

} some eg of f for $\sigma(f) = f$

If $f = \sum a_{ij} x^i y^j$ then for $a_{ij} \neq 0$

$$\sigma(f) = \sum a_{ij} (-1)^{i+j} x^i y^j$$

if $\sigma(f) = f$ then ① as $a_{ij} \neq 0 \Rightarrow i+j$ is even

② i is even $\Rightarrow j$ is even

for this

$$x^i y^j = (x^2)^{i/2} (y^2)^{j/2}$$

③ i is odd $\Rightarrow j$ is odd

$$x^i y^j = (x^2)^{i-1/2} (y^2)^{j-1/2} (xy)$$

or $\mathbb{C}[x^2, y^2, xy] = R^G$

where $G = \langle \sigma \rangle$

Theorm : R^G is noetu ring

lemma : $e : R \to R^G$ s.t $e(r) = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(r)$ (also called reynolds op.)

then ① $\forall a \in R^G$, $e(a) = a$

② $\forall \tau \in G$, $\tau(e(a)) = e(a)$
or $e(a) \in R^G$

③ $e(r)$ is homosphic

proof : ① as $e : R \to R^G$
$r \mapsto \frac{1}{|G|}\sum_{\sigma\in G}\sigma(r)$

we have for $a \in R^G$

$\forall \sigma \in G$ we have
$\sigma(a) = a$

or
$$e(a) = \frac{1}{|G|}\sum_{\sigma\in G} a = \frac{\cancel{|G|}}{\cancel{|G|}} a = a$$

② $\forall \tau \in G$ we have

$$\tau(e(r)) = \frac{1}{|G|}\sum_{\sigma\in G}\tau(\sigma(r))$$
$$= \frac{1}{|G|}\sum_{\sigma\in G}\sigma(r)$$
$$= e(r)$$
as $\tau(\sigma(r)) = \sigma(r)$
as $\sigma(r) \in R^G$
or $a \in R^G$

so $e(r) \in R^G$

③ Now as $e(r) \in R^G$
we have
$e(r_1 + r_2) = e(r_1) + e(r_2)$

& if $a \in R^G$ then

$$e(ar) = \frac{1}{|G|}\sum \sigma(ar)$$
$$= \frac{1}{|G|}\sum \sigma(a)\sigma(r)$$
$$e(ar) = a\,e(r)$$

lemma : $I \leq R^G$ then $(IR) \cap R^G = I$

proof :

as $I \subseteq IR$ & $I \subseteq R^G$

$\Rightarrow I \subseteq IR \cap R^G$,

now $\forall \alpha \in IR \cap R^G$
as $\alpha \in IR$ & $\alpha \in R^G$

$\Rightarrow \alpha = \alpha_1 r_1 + \cdots \alpha_m r_m$ ← finite sum $\in IR$
where $a_i \in I$, $r_i \in R$

as $\alpha \in R^G$
$\Rightarrow e(\alpha) = \alpha$

then $\alpha = e(\alpha) = \alpha_1 e(r_1) + \cdots \alpha_m e(r_m)$

as $\alpha_i \in I$ & $e(r_i) \in R^G$
$\Rightarrow \alpha_i e(r_i) \in I$
$\Rightarrow \alpha \in I$

or $(IR) \cap R^G \subseteq I \Rightarrow I = (IR) \cap R^G$

Theorm : R^G is Noetherian

proof :

Here $I_1 \subseteq I_2 \cdots$ ← chain of ascending ideals of R^G

then

$I_1 R \subseteq I_2 R \cdots$
is chain of ascending ideals in $R = \mathbb{C}[x_1 \ldots x_n]$

then as $\mathbb{C}[x_1 \ldots x_n]$ is noeth
$\exists n_0 \in \mathbb{N}$ s.t
$I_{n_0} R = I_n R \ \forall n \geq n_0$

$\Rightarrow (I_{n_0} R) \cap R^G = (I_n R) \cap R^G$
$\forall n \geq n_0$

$\Rightarrow I_{n_0} = I_n \ \forall n \geq n_0$

$\therefore R^G$ is noeth