MA419 Question answers

Tut 3 – 3
Tut 4 – 5

<u>Tutorial-1</u> : G, H are groups if $x \in G$ s.t $x^n = 1$ for some n then set

$ord(x) = \min\{m \mid x^m = 1 \text{ and } m \geq 1\}$

1. <u>given</u>: $x^r = 1$

<u>prove</u>: $ord(x) \mid r$

<u>proof</u>: as $ord(x) = \min\{m \mid x^m = 1 \text{ and } m \geq 1\}$

let $O = \{m \mid x^m = 1 \text{ and } m \geq 1\}$

then $r \in O$

now if $ord(x) = m$

then $x^m = 1$, $m \geq 1$

also as $x^r = 1$

$x^{r-m} = 1$

$x^{r-m} = x^0 = x^m = x^{2m} \ldots$

$x^{r-m} = x^{km}$

$x^r = x^{(k+1)m}$

as $x^r = x^{(k+1)m}$

$\exists K \in \mathbb{N}$ s.t

$r = (k+1)m$

so $m \mid r$

$m = ord(x) = \min\{n \geq 1 \mid x^n = 1\}$

$x^r = 1 \Rightarrow m \mid n$

$r = qm + c$ $\quad c = 0$

or $1 \leq c \leq m-1$

$1 = x^r = x^{qm+c}$

$1 = x^{qm} x^c$

$1 = x^c$

x^{c-1} $\quad c = 0$

cont.

2. $g \in G$ $\quad ord(gxg^{-1}) = ord(x)$

<u>proof</u>:

$ord(gxg^{-1}) = \min\{m \mid (gxg^{-1})^m = 1, m \geq 1\}$

$(gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1})$ m times

$= gx^mg^{-1}$

for $gx^mg^{-1} = 1$

$\Rightarrow gx^m = g$

$\Rightarrow x^m = 1$

and $x^m = 1$

$gx^mg^{-1} = 1$

$\Rightarrow (gxg^{-1})^m = 1$

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

so $\min\{m \mid (gxg^{-1})^m = 1, m \geq 1\}$

$= \min\{m \mid (x)^m = 1, m \geq 1\}$

as $(gxg^{-1})^m = 1 \Leftrightarrow x^m = 1$

$ord\ gxg^{-1} = ord\ x$

$\overset{\|}{\theta}$ $\quad ord\ x = m$

$ord\ \theta = n$

$(gxg^{-1})^m = gx^mg^{-1}$

$= g1g^{-1} = 1$

$n \leq m$

$\theta = gxg^{-1}$

$g^{-1}\theta g = x$

$ord(x) \leq ord(\theta)$

$m \leq n$

$m = n$

also if $gx = a$

$g^{-1} = b$

$gxg^{-1} = ab$

$ba = g^{-1}gx = x$ or $ab = a(ba)a^{-1}$

so $ord(ab) = ord(ba)$

3. to prove: $x^2=1, \forall x \in G$ then G is abelian.

proof: let $a, b \in G$ then:

note: as $x^2 = 1$

$x \cdot x = e$

$x = x^{-1}$

so, $\forall a \in G$, $a^{-1} = a$

$x^2=1$, $\forall x \in G$

$ab = ba$

$ab = (ab)^{-1}$

$= b^{-1}a^{-1}$

$= ba$

now let $c = ab$, for some $a, b \in G$

also note: for any group, if $a \in G$ and $b \in G$

$(ab)(x) = 1$

$x = b^{-1}a^{-1}$

so $(ab)^{-1} = b^{-1}a^{-1}$

now $ba = b^{-1}a^{-1} = (ab)^{-1} = c^{-1} = c$

as $c^{-1} = c$

$\therefore$ $ba = ab$

$\therefore$ if $x^2 = 1$ G is abelian.

4. $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic group

proof: let's suppose $\mathbb{Z} \cong \mathbb{Q}$

then, $\exists f$ s.t

$f: \mathbb{Z} \to \mathbb{Q}$ is bijective $\Rightarrow |\mathbb{Z}| = |\mathbb{Q}|$

but as $\{n\} \in \mathbb{Q}$ $\forall n \in \mathbb{Z}$

$\mathbb{Z} \subseteq \mathbb{Q}$

also as $\frac{1}{2} \in \mathbb{Q}$ but $\frac{1}{2} \notin \mathbb{Z}$

$|\mathbb{Z}| < |\mathbb{Q}|$

so $|\mathbb{Z}| = |\mathbb{Q}|$ ✱

$\therefore$ f is not bijective

$\therefore$ $\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$

not cyclic

$\mathbb{Z}$ is cyclic

$\mathbb{Q}$ is cyclic

$\mathbb{Q} = \mathbb{Z}\, p/q$ $(p,q)=1$ no common factor

$\mathbb{Q} \ni \frac{1}{q+1} = n\frac{p}{q}$

$q = (np)(q+1)$ ✗

$\frac{1}{q+1} \in \mathbb{Q} = n\frac{p}{q}$ $(q+1, q) = 1$

$q = (np)(q+1)$

$q+1 \mid q$ not possible

not possible as $q+1 > q$

5. $\psi: G \to G$

$\psi(g) = g^2$

To prove: G is abelian $\Leftrightarrow$ ψ is a group homomorphism

proof: $(\Rightarrow)$ let's suppose G is abelian, then

$\forall a, b \in G$

$ab = ba$

now for $\psi: G \to G$

$g \to g^2$

$\psi: G \to G$

$g \to g^2$

G is abelian

$\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$

$= (g_1 g_2)^2$

$= g_1 g_2 g_2 g_1$

$= g_1^2 g_2^2$

$= \psi(g_1)\psi(g_2)$

$$\psi(ab) = (ab)^2 = abab$$
$$= aabb \quad (\text{as } ba = ab)$$
$$= a^2b^2$$
$$= \psi(a)\,\psi(b)$$

$\forall\ \psi(ab) = \psi(a)\psi(b)$
$(ab)^2 = a^2b^2$
$abab = a^2b^2$
$ab = ba$

so $\psi(ab) = \psi(a)\psi(b)$
also, $\psi(e) = e.e = e$
and
$$\psi(aa^{-1}) = \psi(e) = e = \psi(a)\psi(a^{-1})$$
$$\psi(a^{-1}) = (\psi(a))^{-1}$$

$\therefore$ ψ is a group homomorphism.

($\Leftarrow$) now if ψ is a group homorphism,
then
$\forall\, a, b \in G$
$$\psi(ab) = \psi(a)\psi(b)$$
$$\Rightarrow \quad abab = aabb$$
$$\Rightarrow \quad ba = ab$$
so G is abelian

6. all subgroups of $\mathbb{Z}/_{45}\mathbb{Z}$

$\mathbb{Z}/_{45}\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ \overline{44}\}$

$H_0 = \langle \bar{0} \rangle = \{\bar{0}\}$

$H_1 = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ \overline{44}\}$

$H_3 = \langle \bar{3} \rangle = \{\bar{0}, \bar{2}, \bar{5}, \ldots\ \overline{44}\}$

$H_5 = \langle \bar{5} \rangle = \{\bar{0}, \bar{4}, \bar{9}, \ldots\ \overline{44}\}$

$H_9 = \langle \bar{9} \rangle = \{\bar{0}, \bar{8}, \overline{17}, \ldots\ \overline{44}\}$

45 factors $1, 3, 5, 9, 15 \ldots 45$
$0, G, \langle \bar{3} \rangle, \langle \bar{5} \rangle, \langle \bar{9} \rangle, \langle \overline{15} \rangle$

By lagrange's theorm
$|H| \mid |G|$

$H_{15} = \langle \overline{15} \rangle = \{\bar{0}, \overline{14}, \ldots\ \overline{44}\}$

7. <u>To prove</u>: Not cyclic

(a) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\to$ order 4 $\neq p$

if cyclic then $\exists\ (a,b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
s.t
$$\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} = \langle (a,b) \rangle$$
$$= \{(a,b)^m \mid m \in \mathbb{N}\}$$

every non-zero elt has order 2

<u>Case I</u>: $(a,b) = (0,0)$
Not true

<u>Case II</u>: $(a,b) = (1,0)$
Not true

<u>Case III</u>: $(a,b) = (0,1)$
Not true

<u>Case IV</u>: $(a,b) = (1,1)$
Not true

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ if cyclic then $\cong \mathbb{Z}$ $(\bar{1},0) \leftarrow$ finite order $\neq 0$

ψ is not one-one $(0,n)$ or $(1,n) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, $\forall n \in \mathbb{Z}$

then if for (a,b), $a=0$, $(1,n)$ element will not be made.

$\psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ vica-versa
bijective

not one-one $\therefore$ Not cyclic

$\mathbb{Z}$ has no non-zero elts of finite order

(c) $\mathbb{Z} \times \mathbb{Z} = \{(n,m) \mid \forall n,m \in \mathbb{Z}\}$

if cyclic then $\exists (a,b) \in \mathbb{Z} \times \mathbb{Z}$ s.t

$$\langle (a,b) \rangle = \mathbb{Z} \times \mathbb{Z}$$

if $(a,b)^2 = (2a, 2b)$

then $(2a, 2b-1) \notin \mathbb{Z} \times \mathbb{Z}$
but in reality
as $2b-1 \in \mathbb{Z}$
and $2a \in \mathbb{Z}$
$(2a, 2b-1) \in \mathbb{Z} \times \mathbb{Z}$ $\divideontimes$

$\therefore \mathbb{Z} \times \mathbb{Z}$ is not-cyclic

$\mathbb{Z}(a,b)$

p, q are prime

$(p,q) = n(a,b)$
$= (na, nb)$

$a \neq 0$, $b \neq 0$

$a \mid p$ $a = \pm 1$ or p

$b \mid p$ $b = \pm 1$ or q

infinity many primes
$\Rightarrow$ not p

$(1,1)$
$(1,-1)$ $(-1,1)$, $(-1,-1)$
$(0,1) \notin \mathbb{Z}(1,1)$
$\vdots$

8. $\psi : G \to H$ group homomorphism

$E \leq H$

<u>To prove</u>: $\psi^{-1}(E) = \{g \in G \mid \psi(g) \in E\}$ is a subgroup of G.

<u>proof</u>: for $e_g \in G$ $\psi(e) = e_H \in E$
so
$e_g \in \psi^{-1}(E)$

also, for $a \in \psi^{-1}(E)$ and $b \in \psi^{-1}(E)$

$\psi(a) \in E$ and
$\psi(b) \in E$

as ψ is homomorphic

$\psi(a)\psi(b) = \psi(ab) \in E$

so, $ab \in \psi^{-1}(E)$

$\therefore \psi^{-1}(E)$ is subgroup of G

$\psi : G \to H$
$E \leq H$

$\psi^{-1}(E) = \{g \in G \mid \psi(g) \in E\}$

$\psi(e_g) = e_H \in E$

$e_g \in \psi^{-1}(E)$

$x, y \in \psi^{-1}(E)$

$\psi(xy) = \psi(x)\psi(y) \in E$

$xy \in \psi^{-1}(E)$

$x \in \psi^{-1}(E)$ $\psi(x^{-1}) = \psi(x)^{-1} \in E$

$x^{-1} \in \psi^{-1}(E)$

9. $E = \mathbb{Q}/\mathbb{Z} = \{ q + \mathbb{Z} \mid \forall q \in \mathbb{Q} \}$

$= \text{left cosets of } \mathbb{Z} \text{ in } \mathbb{Q}$

$\theta = \frac{a}{b} + \mathbb{Z}$ $\quad (a, b) = 1$

$b \geq 1$

$b\theta = a + \mathbb{Z}$

$= 0 + \mathbb{Z}$

$= \bar{0}$

Tutorial 2 :

1. $H \leq G$ $g \in G$
$\exists g_1 \in G$ s.t
$Hg = g_1 H$
To prove : $Hg = gH$ or $g^{-1}Hg = H$

proof : $\exists g_1 \in G$ s.t
$Hg = g_1 H$

$gH = Hr$
then $Hr = Hg$
$gHg^{-1} = H$
$g \in gH$
$\Rightarrow g \in Hr$
$\Rightarrow g = hr$
$\Rightarrow Hg = Hhr = Hr$
$gH = Hg$
$gHg^{-1} = H$

$\exists h, h_1 \in H$
$\Rightarrow hg = g_1 h_1$
now $g^{-1}hg = g^{-1}g_1 h_1$
as $hg = g_1 h_1$
if $g^{-1}g_1 h_1 \in H$ then we are done

as $hg = g_1 h_1$
$h = g^{-1} g_1 h_1$
$\therefore g^{-1}hg = g^{-1}g_1 h_1 = h$
$\Rightarrow g^{-1}Hg = H$

$\Rightarrow Hg = gH$

2. $H \leq K \leq G$ bijection
G/H , $G/K \times K/H$

$\phi : G/K \times K/H \to G/H$
$(gK, kH) \to (gkH)$

① $(g_1 K, k_1 H) = (g_2 K, k_2 H)$
$g_1 K = g_2 K$
$k_1 H = k_2 H$

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

$G = \bigcup x_i K$
$K = \bigcup y_i H$
$G = \bigcup_{i,j} x_i y_i H$ $\quad G = \bigcup x_i y_j H$
$x_i y_j H = x_{i'} y_{j'} H$
$x_i = x_{i'}$
$y_i = y_{j'}$

$x_i y_i K = x_{i'} y_{i'} K$
$x_i K = x_{i'} K$
$x_i = x_{i'}$

doubt

$y_i H = y_{i'} H$
so $y_i = y_{i'}$

3. $A \trianglelefteq G$ $\quad B \leq G$
also A is abelian

$A \cap B \trianglelefteq AB$
$AB = \{ ab \mid a \in A, b \in B \}$

$A \cap B = \{ x \mid x \in A$ and $x \in B \}$
① $e \in A \cap B$
② if $x \in A \cap B$ and
$y \in A \cap B$ then
as $x \in A$ and $x \in B$
and $y \in A$ and $y \in B$

$xy = yx$ (as A is abelian)
an $xy \in A$ and $xy \in B$
$\Rightarrow xy \in A \cap B$

abelian
$A \trianglelefteq G$ $\quad B$
$A \cap B \trianglelefteq AB$
$x \in A \cap B$
$g = ab \in AB$
$g^{-1}xg = b^{-1}a^{-1}xab$
$= bxb^{-1} \in B$
$\in A$
$\in A \cap B$

③ $x \in A \cap B$
then $x \in A$ and $x \in B$
$\Rightarrow x^{-1} \in A$ and $x^{-1} \in B$
$\Rightarrow x^{-1} \in A \cap B$

④ $x \in A \cap B$ then
$\forall g \in AB$
let $g = ab$

$ab\,x\,(ab)^{-1}$
$= abxb^{-1}a^{-1}$
$= ab'a^{-1} \in A$
as $x \in A$ $(bxb^{-1} \in A)$
now
$abxb^{-1}a^{-1} = ab'a^{-1} \in A$
$b' \in A$
as $b' \in A$
$b'aa^{-1} = b' \in B$

$\therefore A \cap B \trianglelefteq AB$

4. $|G| < \infty$ $\left.\begin{array}{l} H \leq G \\ N \trianglelefteq G \end{array}\right\}$ $HN = NH$, $HN \leq G$

<u>TO prove</u>: $|H|$ and $|G/N|$ are rel prime
$\gcd\{|H|, |G/N|\} = 1$ then $H \subseteq N$

<u>proof</u>: $\dfrac{|HN|}{|N|} = \dfrac{|H|}{|H \cap N|}$
$|HN| = \dfrac{|H||N|}{|H \cap N|}$
$|G| = |G/HN|\,|HN|$
$= |G/HN| \dfrac{|H||N|}{|H \cap N|}$
~~$|G|$~~ $= \dfrac{|G/HN|\,|H|\,\cancel{|G|}}{|G/N|\,|H \cap N|}$

$|G/N|\,|H \cap N| = |G/HN|\,|H|$

as $\gcd(|H|, |G/N|) = 1$
$|H| \mid |H \cap N|$ so
$|H| \leq |H \cap N|$
$\Rightarrow |H| = |H \cap N|$

$|G| < \infty$ $N \trianglelefteq G$, $H \leq G$
$(|H|, |G/N|) = 1$ $\Big]$ to prove $\Rightarrow H \subseteq N$
G/N
$h \in H$, $hN \in G/N$
$\mathrm{ord}(h) = r$, $\mathrm{ord}(hN) = m$
$m \mid r$, $m \mid |G/N|$ $m \mid |G/N|$
$m \mid |H|$ $m \mid |H|$

$\Rightarrow \underline{m = 1}$, $\underline{hN = N}$
$\therefore \underline{h \in N}$

5. $N \trianglelefteq G$ $\quad |G| < \infty$

$|N| \quad |G/N|$

let $H \leq G$ s.t

$|H| = |N|$

to prove: $H = N$

proof: $\dfrac{HN}{N} \cong \dfrac{H}{H \cap N}$ (second isomorphism theorm)

$$|G| = |G/HN|\,|HN|$$
$$= |G/HN| \frac{|H||N|}{|H \cap N|}$$

$$\cancel{|G|} = |G/HN| \frac{|H|\,\cancel{|G|}}{|G/N|\,|H \cap N|}$$

$$|G/N|\,|H \cap N| = \underbrace{|G/HN|\,|N|}_{\gcd = 1}$$

$$|N| \mid |H \cap N|$$

$N \leq H \cap N$

$\Rightarrow N = H$

$\therefore$ unique

$|G| < \infty$

$N \trianglelefteq G$

$(|N|, |G/N|) = 1$

N is unique subgroup of order $|N|$ if $H \leq G$ then $H = N$

$H \leq G$ $\quad |H| = |N|$

$(|H|, |G/N|) = 1$

$\Rightarrow H \subseteq N$

$\therefore |H| = |N| \Big\} \Rightarrow H = N$

6. $H, K \trianglelefteq G$ $\quad G = HK$

$G/H \cap K \cong G/H \times G/K$

$\phi: G \longrightarrow G/H \times G/K$

$(g) \longrightarrow (gH, gK)$

① $\ker(\phi) = \{ g \in G \mid gH = e \text{ and } gK = e \}$

$= H \cap K$

② ϕ is onto as $\forall g$ st (gH, gK) there is a pre image.

③ ϕ is homomorphism:

$$\phi(g_1 g_2) = (g_1 g_2 H, g_1 g_2 K)$$
$$= (g_1 H . g_2 H, g_1 K . g_2 K)$$

as $H, K \trianglelefteq G$

$$= (g_1 H, g_1 K).(g_2 H, g_2 K)$$
$$= \phi(g_1).\phi(g_2)$$

$\therefore$ from 1st isomorphism theorm:

$$G/H \cap K \cong G/H \times G/K$$

$H, K \trianglelefteq G = HN$

$G/H \cap K \cong G/H \times G/K$

$\phi: G \longrightarrow G/H \times G/K$

$g \rightarrow (gH, gK)$

$\ker \phi = H \cap K$

$\phi: G/H \cap K \hookrightarrow G/H \times G/K$

(aH, bK)

$(aH, bK) = (aH, eK).(eH, bK)$

$\phi(\theta_1) = (aH, eK)$

$\phi(\theta_2) = (eH, bK)$

$\phi(\theta_3) = (aH, bK)$

$a \in G = HK = KH$

$a = hk \qquad aH = khH = KH$

$\Phi(\bar{k}) = (kH, kK)$

$= (aH, eK)$

7. $|G/Z(G)| = n$

then

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

$O_x = \{ g x g^{-1} \mid \forall g \in G \}$

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

$|G/Z(G)| = n \quad a \in G$

$O_a = \{ g a g^{-1} \mid g \in G \}$

$|O_a| = |G/G_a|$ (proved)

also $G_a \supseteq Z(G)$

$|G/Z| \to |G/G_a|$ so $\# |O_a| \leq n$

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

then $x \in Z(G)$ and for $g = e$ $Z(G) \leq O_x$

for some $g \in G$

$|G| = |G/O_g| |O_g|$

now, $|O_g| = |O_g / Z(G)| |Z(G)|$

$|G| = |G/O_g| |O_g / Z(G)| |Z(G)|$

$|G| = |G/Z(G)| |Z(G)|$

as $|G/Z(G)| = n = |G/O_g| |O_g / Z(G)|$

$n \geq |G/O_g|$

8. $|G| = p^n_{n \geq 1}$ let $H \leq G$

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

P primes $|G| = p^n$

$\exists H_i \leq G$, s.t $|H_i| = p^i$

$i = 0 \quad H_0 = \{e\}$

$i = n \quad H_n = G$

now $|G| = |O_e \sqcup O_{g_1} \sqcup O_{g_2} \cdots O_{g_n}|$

also $|G/O_g| |O_g| = |G| = p^n$

as $|G/O_g| |O_g| = p^n$

Pf: induction on n

$n = 1$

$n \geq 2$

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

$e \neq a \in Z(G)$

$H = (a)$ $|H| = p^{i_0}$ $\exists H_i \leq H$

$|H_i| = p^i \quad i \leq i_0$

$H \trianglelefteq G$

in G/H, $E_i \leq G/H$

s.t $|E_i| = p^j \quad 0 \leq j \leq n - i_0$

$E_i = H_i/H$, $H_i \supseteq H$

$|H_i| = p^{j + i_0}$

now $\gcd\{ |G/O_g|, p^n \} = p^r$

for $r = 0, 1, \cdots$

now $|G/O_g| = k \times p^r$

$\hookrightarrow$ any comb of primes

as $k p^r |O_g| = p^n$

$k |O_g| = p^{n-r} = p^{r'}$

as $p^{r'}$ is prime comb of P

but k does not have P

$\Rightarrow k = 1$

$|O_g| = p^{r'}$

$\therefore$ order of subg. is p^i

① prove $|Z(G)| \neq 1$

② prove $p \mid |Z(G)|$

③ prove $\langle x \rangle \leq Z(G)$

s.t $\langle x \rangle \trianglelefteq G$

④ prove $G/\langle x \rangle$ is a group of less order

⑤ prove H_i of $G/\langle x \rangle$

⑥ map $\psi : G \to G/\langle x \rangle$

then $\psi^{-1}(H_i) \leq G$

⑦ $|\psi^{-1}(H_i)| = \underbrace{p^i \times p}_{p \text{ cosets}} = p^{i+1}$

Tutorial-3 :

1. let $|G| = 2n+1$ and let $\exists x \in G$ s.t $x \neq e$ and x and x^{-1} be conjugate in G.

i.e $\quad O_x = \{gxg^{-1} \mid g \in G\}$

$x \sim x^{-1}$

$O_x = \{gxg^{-1} \mid g \in G\}$

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

$\exists\, g \in G$ s.t $x^{-1} = gxg^{-1}$

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

$\Rightarrow (gx)(gx) = 1$

$\Rightarrow (gx)^2 = 1$

$\theta \in O_x$

$\theta = gxg^{-1}$

$\theta^{-1} = gx^{-1}g^{-1}$

$\theta^{-1} \sim x^{-1} \sim x$

$\theta^{-1} \in O_x$

$\therefore \exists\, g'$ s.t $(g')^2 = 1$

$H = \{e, g'\} \leq G$

$|H| = 2$

then as index $\in \mathbb{N}$ but $|H| = 2$

$|G/H|$ even or odd

$\Rightarrow |G|$ even $*$

$O_x = \bigsqcup_{v \in O_x} \{v, v^{-1}\}$

$2 \mid \# O_x$

$\# O_x = |G/G_x| \,\big|\, |G|$

$\Rightarrow 2 \mid |G|$ $*$

2. $H \leq G$ index $= n$

let $G \times \{g_i H \mid g \in G\} = \{g_i H \mid g \in G\}$

$|G/H| = n$

$\therefore i = 1, 2, \ldots, n$

$G \times \{1, 2, \ldots n\} = \{1, 2, \ldots n\}$

$|G/H| = n$

$G/H = \{g_1H, \ldots g_nH\}$

G acts on this group like a permutation

$\eta : G \to S_n$

$\eta(g) = \sigma_g$ $\}$ prove this

$g \in G$

$\phi_g : G/H \to G/H$

$aH \to gaH$

then $\sigma_g(1, 2, \ldots n) = (\ldots)$

Note: this $\eta : G \to S_n$ is homomorphism

$aH = a'H$

$a = a'h$

$ga = ga'h$

$gaH = ga'H$

$K = \ker(\eta)$

① $|G/K| \cong |S_n|$

$\therefore |G/K| \leq n!$

also $K \trianglelefteq G$ and $K \leq H$ $\}$ prove this

① $G \times (G/H) \to (G/H)$

② $\Psi : G \to S(G/H)$

③ $G/\ker(\Psi) \to S(G/H)$

aH

$g^{-1}aH \to g.g^{-1}aH = aH$

ϕ_g is bijection

$G \to S(G/H)$

$g \to \varphi_g$

note $\varphi_g = 1 \Rightarrow H \to gH = H$

$g \in S$

$\ker(\varphi_g) \supseteq H$

$G/\ker\varphi \hookrightarrow S(G/H)$ / n! elts

3. $|G| = p^m \quad |H| = p^{m-1}$ with $H \leq G$
$\Rightarrow H \trianglelefteq G$

induction on m
$|G| = p^2$
then G is abelian
$H \trianglelefteq G$
$m \geq 3$ and $\ldots < m$
$|H| = p^{m-1}$
$H \trianglelefteq N(H) = \{g \in G \mid gHg^{-1} = H\}$

$\left| G/H \right| = p$ (index)

now if $\left| G/H \right| = p$ then

$Z(G) \subseteq N(H)$

G/H is a cyclic group
$\exists g \in G$ s.t
$G/H = \langle gH \rangle = \{ g^i H \mid i = 0, 1, \ldots p-1 \}$

if $Z(G) \not\subseteq H \Rightarrow N(H) \supsetneq H$
so $N(H) = G$
$\Rightarrow H \trianglelefteq G$

now, if G/H is cyclic.

and as $e \in H$

if $Z(G) \subseteq H$
$H/Z(G) \leq G/Z(G)$

$\Rightarrow g^{i-j} \in H$ for $i - j = np$

p^{i-j} $\quad p^i < p^m$

$\Rightarrow g^{i-j} = h'$

so by corresp. theorm

$\Rightarrow g^i = h' g^j$

$H/Z(G) \trianglelefteq G/Z(G)$

$\Rightarrow g^i = h'(h'' h''^{-1}) g^j$

$\Rightarrow H \trianglelefteq G$

$\Rightarrow g^i h_1 = h_2 g^j$

$\Rightarrow g^i H = H g^j$ when $i - j = np$

$\therefore H \trianglelefteq G$

4. $H, K \trianglelefteq G$
G/H and G/K are abelian
<u>To prove</u>: $G/H \cap K$ is abelian
<u>proof</u>:

$\dfrac{G}{H \cap K} \cong$ Abelian group then
$G/H \cap K$ is abelian group

$G \to G/H \times G/K$
$g \mapsto (gH, gK)$

now let

$\ker \varphi = H \cap K$

$\Psi : G \to G/H \times G/K$
$g \mapsto (gH, gK)$

$G/\ker\varphi \hookrightarrow \underbrace{G/H \times G/K}_{\text{Abelian}}$

so $G/H \cap K$ is abelian

$\ker(\Psi) = \{ g \mid gH = H \text{ and } gK = K \}$
$= \{ H \text{ and } K \}$
$= H \cap K$

also $\Psi(g_1 g_2) = (g_1 g_2 H, g_1 g_2 K)$
$= (g_1 H g_2 H, g_1 K g_2 K)$
$= \Psi(g_1) \Psi(g_2)$ as H, K are abelian

$\therefore \quad \dfrac{G}{H\cap K} \cong G/H \times G/K$

now lets see if $G/H \times G/K$ is abelian.

let $x \in G/H \times G/K$
then $xy = yx \ \forall y \in G/H \times G/K$

$x \in G/H \times G/K$
$y \in G/H \times G/K$

$x = (g_1 h_1, g_1' K_1)$
$y = (g_2 h_2, g_2' K_2)$

$xy = (g_1 h_1 g_2 h_2, g_1' k_1 g_2' k_2)$

$yx = (\underline{g_2 h_2} g_1 h_1, \underline{g_2' k_2} g_1' \underline{k_1})$

as abelian

$\therefore \ xy = yx, \ \forall x, y \in G/H \times G/K$

$\therefore \ G/H \times G/K$ is abelian

$\therefore \ \dfrac{G}{H\cap K} \cong G/H \times G/K$ is abelian

5. H is a cyclic group

$H \trianglelefteq G$ To prove: $K \leq H$
$\Rightarrow K \trianglelefteq G$

$\langle x^m \rangle = K \leq H = \langle x \rangle$

$|gKg^{-1}| = |K|$

$gKg^{-1} \subseteq gHg^{-1} = H$

by uniqueness of subgroup of a cyclic group

$gKg^{-1} = K$

proof: let $K \leq H$ so
① $e \in K$
② $k_1 \in K$ and $k_2 \in K$
$\Rightarrow k_1 k_2 \in K$
③ $k \in K$
$\Rightarrow k^{-1} \in K$

also $K \leq H$
let $x \in K$
then $gxg^{-1}, \forall g \in G$
$\in K$
for K to be normal
$\exists i$ s.t as $x \in H$
$x = a^i \in K$
now, $g a^i g^{-1} \in H$
as $H \trianglelefteq G$
$\Rightarrow g a^i g^{-1} = a^j$
$\exists j$ s.t this occurs.

$g a^i g^{-1} = a^j$

where $a^i \in K$

$ga^i = a^j g$

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

$a^{i-j} = e$

$i-j = n.|H|$

so $a^i = a^j$

$\therefore a^j \in K$

$\therefore K \trianglelefteq G$

6. G group H, K are only subgroups. simple

now $H = \langle a \rangle$

$K = \langle b \rangle$

$o(H) = p$

$o(k) = q$

wLog: $H = \{a^0, a^1, .. a^{p-1}\}$

now,

$g a^i g^{-1} = a^j$

$g a^i = a^j g$

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

$a^{i-j} = e$

$\therefore$ then $H \trianglelefteq G$

and $K \trianglelefteq G$

$\therefore$ G is <u>not</u> simple

7. G normal subgroups

$H, K \trianglelefteq G$ 3, 5 order

then

$HK = KH$ (as normals) also $HK \trianglelefteq G$

and also $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong H \times K$

as $(3,5) = 1$

$\therefore H \times K \cong \mathbb{Z}/15\mathbb{Z}$

now $\Psi: H \times K \to HK$

$(h,k) \to (hk)$

now,

$\Psi(x_1 x_2) = (h_1 k_1)(h_2 k_2)$

$= h_1 h_2 k_1 k_2$

$= \Psi(x_1)\,\Psi(x_2)$

$\therefore$ homomorphism

also $\ker(\Psi) = \{x \in H \times K \text{ s.t } hk = e\}$

$= \{x = e\}$

$= \{e\}$

$\therefore H \times K \cong HK \cong \mathbb{Z}/15\mathbb{Z}$

$\therefore$ HK has order 15.

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

$K = \{1, y, y^2, \dots y^4\}$

$H, K \trianglelefteq G$

$H \cap K = \{1\}$

$HK \trianglelefteq G$

$HK \cong H \times K$

$= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

so $\exists\, g \in HK$ s.t $|g| = 15$

8. $|G|=p^2q$

<u>case I</u> > $p>q$
then $n_p \equiv 1 \mod p$
$n_p = 1 + kp^2$
also $n_p | q$
$\therefore n_p < q$
$\Rightarrow n_p = 1$
$\therefore |P| = p^2$
$P \leq G$
as $|P|=p^2$; P is abelian as $n_p=1$
$\therefore P \trianglelefteq G$

<u>case II</u> > let $q>p$, then
$n_q = 1+kq \mid p^2$
if $n_q = 1$ (we are done)
if $n_q \neq 1$ then
$n_q = p$ or p^2
but as $q > p$
$n_q \neq p$
$\therefore n_q = p^2$
also if $n_q = p^2 = 1+kq$
$kq = (1-p)(1+p)$
as q is prime
$q \mid 1+p$ or $q \mid p-1$
but as $q>p$ $q \nmid p-1$
$\therefore q \mid 1+p$
$\Rightarrow q = 1+p$
only possible if
$q=3$
$p=2$

as $|G| \neq 12 \Rightarrow n_q \neq p^2$
$\therefore n_q = 1$
$\therefore |Q| = q$
which is
cyclic $\Rightarrow$ abelian
& $Q \trianglelefteq G$

<u>Note</u>: $n_q = 1$ means
$gQg^{-1} = Q, \forall g \in G$
$\therefore Q \trianglelefteq G$ (same for other)

Tutorial-4 :

1. (a) $H \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$
$K \cong \mathbb{Z}/p\mathbb{Z}$
s.t

$G = H \rtimes K$ $\quad \psi : K \to Aut(\mathbb{Z}/p^{m-1}\mathbb{Z})$

$|Aut(\mathbb{Z}/p^{m-1}\mathbb{Z})| = p^{m-2}(p-1)$

$p \mid |Aut(\mathbb{Z}/p^{m-1}\mathbb{Z})|$

$\exists\ x^p = 1$ in $Aut(\mathbb{Z}/p^{m-1}\mathbb{Z})$
when $x \neq e$

$i \to x^i \bmod p$ a non-trivial isomorphism

this means $G = H \rtimes K$
$K \ntrianglelefteq G$
$\therefore$ G is not abelian

$|G| = p^m$ $\quad$ G non-abelian
(i) $H \trianglelefteq G$, $H \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$
$Aut(H) \cong (\mathbb{Z}/p^{m-1}\mathbb{Z})^{\times}$
$|Aut(H)| = p^{m-2}(p-1)$
$x \in Aut(H)$
$ord(x) = p$
$\mathbb{Z}/p\mathbb{Z} \to Aut(H)$
$1 \to x$
non trivial
$K \ntrianglelefteq G$
$G = H \rtimes \mathbb{Z}/p\mathbb{Z} = K$
$|G| = p^m$ $\quad$ G is not ab.

(b) $H \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \mathbb{Z}/p\mathbb{Z}}_{m-1 \text{ times}}$ $\quad Aut(\underbrace{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots}_{m-1 \text{ times}})$

$\cong GL_{m-1}(\mathbb{Z}/p\mathbb{Z})$

now $|GL_{m-1}(\mathbb{Z}/p\mathbb{Z})|$
$= (p^{m-1}-1)$
$(p^{m-1}-p)$
$(p^{m-1}-p^2)$
$\vdots$
$(p^{m-1}-p^{m-2})$

$\therefore p \mid |GL_{m-1}(\mathbb{Z}/p\mathbb{Z})|$
$\therefore \exists\ \psi$ (non-trivial)
$\therefore K \ntrianglelefteq G$
$\therefore$ G is non-abelian

$H \trianglelefteq G$,
$H \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots}_{m-1 \text{ copies}}$

$Aut(\mathbb{Z}/p\mathbb{Z} \times \cdots) \cong GL_{m-1}(\mathbb{Z}/p\mathbb{Z})$

$\left[\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & 0 \\ \hline 0 & & \begin{matrix} a & b \\ c & d \end{matrix} \end{array}\right]_{m-1 \times m-1}$ $\quad GL_2(\mathbb{Z}/p\mathbb{Z}) \hookrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$
$(p^2-p)(p^2-1)$

$p \mid |Aut(H)|$
$\therefore ord(x) = p$
$\psi : \mathbb{Z}/p\mathbb{Z} \to Aut(H)$
$1 \to x$
$K \ntrianglelefteq G$, $G = H \rtimes K = \mathbb{Z}/p\mathbb{Z}$
$|G| = p^m$
G is not abelian

2. let $D_{2n} = \{\langle x, y\rangle \mid x^n = 1, y^2 = 1, xyx = y\}$ $\quad D_{2n}$ p odd
$Syl_p(G)$ is cyclic and normal in D_{2n}

now, let $S \in Syl_p(D_{2n})$
then if $x^i y \in S$ then
$(x^i y)^2 = x^i y x^i y = y^2 = 1$
$\therefore |S| = 2 \mid \{e, x^i y\}|$
$\therefore$ S is even
but as p is odd and
$|S| = p$ $\quad *$
$\therefore x^i y \notin S$
or only $x \in S$ $\quad \therefore S = \langle x \rangle$
$\therefore$ cyclic, now
for normal as S is cyclic and for $x \in S$
$gxg^{-1} = x^i y x (x^i y)^{-1}$

Note: n is not required to be odd.
$D_{2n} = \{\langle r, s\rangle \mid r^n = 1 = s^2, rs = sr^{-1}\}$
$\underline{s, rs, r^2 s, \ldots, r^{n-1}s}$
order 2

$H \cap \{s, rs, \ldots r^{n-1}s\} = \phi$
$H \leq \langle x \rangle$
so H is cyclic
by ene problem $\to 2|H| = G$
$H \trianglelefteq G$ $\quad$ then $H \trianglelefteq G$

$= x^i y\, x\, y^{-1} x^{-i}$
$= x^{i-1} y\, y^{-1} x^{-i}$
$= x^{i-1} x^{-i}$
$= x^{-1} \in S$

3. $|G| = 77 = 7 \times 11$
as $7 \nmid 10 = 11-1$
$n_p = 1; n_q = 1$

$\therefore G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/77\mathbb{Z}$
as $\gcd(7, 11) = 1$

$|G| = 77$
$77 = 7 \times 11$
$7 \nmid (11-1) = 10$
$P = Syl_7(G) \trianglelefteq G$
$Q = Syl_{11}(G) \trianglelefteq G$
$G = PQ \cong P \times Q \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$
$\cong \mathbb{Z}/77\mathbb{Z}$

4. using $G = p^r m$ $\gcd(p, m) \neq 1$
and
$H \leq G$ and let
$|H| = p^s k$
then as $n_p | m$ and $n_p = 1 \mod p$
$=1$
$\Rightarrow 1 + kp | m \Rightarrow k = 0$
now $n_H | k$ and $n_H = 1 \mod p$
$1 + sp | k$ but as $k \leq m$
$\Rightarrow 1 + sp = 1$
$\therefore n_H = 1$

now $\exists g \in G$ s.t
$gPg^{-1} \cap H = Syl(H) = H$
as only one
and $gPg^{-1} \in Syl(G) = P$
as only one

$P \cap H = Syl(H) = H$
$\therefore P \cap H \trianglelefteq H$

$P \trianglelefteq G$
normal syl p-sub
$P \cap H \trianglelefteq H$
$P \cap H$ is syl p-sub of H
Q sylow p-sub of H
$Q = gPg^{-1} \cap H = P \cap H$
$hQh^{-1} = h(P \cap H)h^{-1}$
$= (hPh^{-1}) \cap H$
$= P \cap H$
$= Q$
so $Q \trianglelefteq H$

5. $|H| = p^\alpha$ $\alpha \geq 1$
and $|P| = p^m$ for
$|G| = p^r m$ $p \times m$
now, $|H||P| = p^\alpha p^r$
and $H \trianglelefteq G$
$P \leq G$
then $\frac{|PH|}{|H|} = \frac{|P|}{|H \cap P|} \Rightarrow |PH| = \frac{|P||H|}{|H \cap P|} \leq \cancel{\frac{|P||H|}{|P|}}$
$\therefore PH$ is also a
p subgroup.
$P \leq PH$, now and $H \leq PH$
if P is sylow p subgroup
then $P = PH$ $\therefore$ $H \leq PH = P$
$\therefore H \leq P$, $\forall$
$P \in$ syl p subgroup

$P \trianglelefteq G$
P p-group
Q syl p-sub
$H \leq G$
$gQg^{-1} \cap H$ for $H = P$
$gQg^{-1} \cap P = P$
$P \leq \frac{gQg^{-1}}{H}$
$P \subseteq H$
$P = QPQ^{-1} \subseteq QHQ^{-1}$
normal
$P \subseteq QHQ^{-1}$
$P \leq$ every syl p-group

6. $|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$

$= p(p^2-1)(p-1)$

now $= p(p-1)(p-1)(p+1)$

$\uparrow$ odd / even; $(p-1)(p+1)$: even / odd

$\therefore |GL_2(\mathbb{Z}/p\mathbb{Z})| = pm$ s.t $p \nmid m$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z})$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$

$\therefore P = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$ as $|P| = p$

$P \in Syl_p(G)$

$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}/p\mathbb{Z} \right\}$

$|H| = p$

$|G| = (p^2-1)(p^2-p)$

$= p(p^2-1)(p-1)$

only p divides G

H is cyclic

Sylow p-sub is cyclic

Tutorial-5:

1. $I+J=R$
$R/IJ \cong R/I \times R/J$

as $R/I\cap J \Leftrightarrow R/I \times R/J$
as $I+J=R$
$\Rightarrow I\cap J = IJ$

Now let's show $IJ = I\cap J$

for this, let $\alpha \in I\cap J$

then $\alpha \in I$ and $\alpha \in J$

also $\alpha.1 \in I\cap J$

$\Rightarrow \alpha(x+y) \in I\cap J$

as $\exists\, x\in I,\ \exists\, y \in J$
s.t $x+y=1$

$\Rightarrow \alpha x + \alpha y \in I\cap J$

as $\alpha \in J,\ x\in I \Rightarrow \alpha x \in IJ$

and $\alpha \in I,\ y\in J \Rightarrow \alpha y \in IJ$

$\Rightarrow \alpha x + \alpha y \in IJ$

$\Rightarrow I\cap J \subseteq IJ$

now, for $\alpha \in IJ$

$\exists\, a, b \in I, J$
s.t $\alpha = ab$

as $a\in I$, $b\in R$	$a\in R$, $b\in J$
$\Rightarrow ab \in I$	$\Rightarrow ab\in J$

as $ab \in I$ and J

$\Rightarrow ab \in I\cap J$

$\Rightarrow IJ \subseteq I\cap J$

$\therefore IJ = I\cap J$

now, let $\varphi: R \longrightarrow R/I \times R/J$
$r \longmapsto (r+I,\ r+J)$

① well defined: $r_1 = r_2$

$\varphi(r_1) = (r_1+I,\ r_1+J)$
$= (r_2+I,\ r_2+J)$
$= \varphi(r_2)$

② homorphism: $\varphi(r_1)+\varphi(r_2) = (r_1+I,\ r_1+J)+(r_2+I,\ r_2+J)$
$= (r_1+r_2+I,\ r_1+r_2+J)$
$= \varphi(r_1+r_2)$

$\varphi(r_1)\varphi(r_2) = (r_1+I,\ r_1+J)(r_2+I,\ r_2+J)$
$= (r_1r_2+I,\ r_1r_2+J)$
$= \varphi(r_1r_2)$

③ Surjetive: As $\exists\, x+y=1$
$x\in I,\ y\in J$

$x = 1-y$	$y = 1-x$
$\Rightarrow x \in 1+J$	$\Rightarrow y \in 1+I$

so, $\varphi(x) = (0+I,\ 1+J)$
$\varphi(y) = (1+I,\ 0+J)$

now $\varphi(y r_2 + x r_1) = \varphi(y r_2) + \varphi(x r_1)$
$= \varphi(y)\varphi(r_2) + \varphi(x)\varphi(r_1)$
$= (r_2 + I, J) + (I, r_1 + J)$
$= (r_2 + I, r_1 + J)$

$\therefore \forall (r_2 + I, r_1 + J) \in R/I \times R/J$
$\exists\ y r_2 + x r_1 \in R$ s.t
$\varphi(y r_2 + x r_1) = (r_2 + I, r_1 + J)$
$\therefore$ surjective

④ $\ker\varphi = \left\{ r \in R \,\middle|\, \varphi(r) = 0 \right\}$
$= \left\{ r \in R \,\middle|\, (r + I, r + J) = (I, J) \right\}$

$= \left\{ r \in R \,\middle|\, r \in I \text{ and } r \in J \right\}$
$= \left\{ r \in R \,\middle|\, r \in I \cap J \right\}$
$= I \cap J$

so using first isomorphism theorem,

$R/I\cap J \cong R/I \times R/J$
$\Rightarrow R/IJ \cong R/I \times R/J$
as $IJ = I \cap J$

2. $x^n = 0$ for some $n \geq 1$

<u>To prove</u>: $1-x$ is invertible in R.

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

<u>Proof</u>: $(1-x)(1+x+x^2+\cdots x^{n-1})$
$= 1 + x + x^2 + \cdots x^{n-1}$
$- (x - x^2 - x^3 - \cdots x^{n-1})$
$= 1$

$(1-x)(1+x+x^2+\cdots x^{n-1})$
$= 1$

$\therefore \exists\ r \in R$ s.t
$(1-x)(r) = 1 = (r)(1-x)$ (as R is comm)
or $1-x$ is invertible

3. $I, J \leftarrow$ ideals
where $IJ \neq I \cap J$

Now, $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$
$4\mathbb{Z}$ is an ideal of $\mathbb{Z}$

now, $(2\mathbb{Z})(4\mathbb{Z}) = \left\{ ij \,\middle|\, i \in 2\mathbb{Z}, j \in 4\mathbb{Z} \right\}$
$= \left\{ ij \,\middle|\, i = 2n, j = 4m \text{ for some } n, m \in \mathbb{Z} \right\}$
$= \left\{ ij \,\middle|\, ij = 8nm, \text{ for some } n, m \in \mathbb{Z} \right\}$
$= \left\{ ij \,\middle|\, ij = 8r, \text{ for some } r \in \mathbb{Z} \right\}$

$(2\mathbb{Z})(4\mathbb{Z}) = \left\{ 8r \,\middle|\, r \in \mathbb{Z} \right\} = 8\mathbb{Z}$

Now, $2\mathbb{Z} \cap 4\mathbb{Z} = \left\{ r \in R \,\middle|\, r \in 2\mathbb{Z} \text{ and } r \in 4\mathbb{Z} \right\}$
$= \{ r \in R \mid r = 2m, r = 4n \}$

$= \{r \in R \mid r = 4n\}$

$= \{r \in R \mid r \in 4\mathbb{Z}\}$

$= 4\mathbb{Z}$

as $8\mathbb{Z} \neq 4\mathbb{Z}$

we have our example.

4. $IJ = I \cap J$ if $I + J = R$

let $\alpha \in I \cap J$

then $\alpha \in I$ and $\alpha \in J$

also $\alpha . 1 \in I \cap J$

$\Rightarrow \alpha(x+y) \in I \cap J$

as $\exists\, x \in I,\ \exists\, y \in J$

s.t $x + y = 1$

$\Rightarrow \alpha x + \alpha y \in I \cap J$

as $\alpha \in J,\ x \in I \Rightarrow \alpha x \in IJ$

and $\alpha \in I,\ y \in J \Rightarrow \alpha y \in IJ$

$\Rightarrow \alpha x + \alpha y \in IJ$

$\Rightarrow I \cap J \subseteq IJ$

now, for $\alpha \in IJ$

$\exists\, a, b \in I, J$

s.t $\alpha = ab$

as $a \in I$, $b \in R$ $\Rightarrow ab \in I$	$a \in R$, $b \in J$ $\Rightarrow ab \in J$

as $ab \in I$ and J

$\Rightarrow ab \in I \cap J$

$\Rightarrow IJ \subseteq I \cap J$

$\therefore IJ = I \cap J$

5. $I = \langle a_1, a_2, \dots a_m \rangle$

$= \{r_1 a_1 + r_2 a_2 + \cdots r_m a_m \mid \forall r_1, r_2, r_3, \dots r_m \in R\}$

given $a_i^{n_i} = 0$

let $n = \max\{n_1, n_2, \dots n_m\}$

then

$$I^{nm} = \sum_{r_1 + r_2 + \cdots r_m = nm} r_1 r_2 \dots r_m\, a_1^{r_1} a_2^{r_2} a_3^{r_3} \dots a_m^{r_m}$$

here $r_1 + r_2 + \dots r_m = nm$

where $r_1 \geq 1$

$r_2 \geq 1$

$\vdots$

$r_m \geq 1$

$\therefore$ there will be partitions

as there will be atleast one partition

of size more than equal to n

as max partition $\Rightarrow r_i = n\ \forall i$

multinomial theorm

$(x_1 + x_2 + \cdots x_m)^{\ell}$

$$= \sum_{\substack{\sum k_j = \ell \\ k_j \geq 0}} \binom{n}{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$$

$$= \sum \left(\frac{n!}{k_1! k_2! \dots k_m!}\right) x_1^{k_1} \dots x_m^{k_m}$$

$\ell = \sum n_i + 1$

$(r_1a_1 + r_2a_2 + \cdots r_m a_m)^e$

$= \sum \binom{n}{k_1 k_2 \ldots k_m} (r_1a_1)^{k_1} \cdots (r_m a_m)^{k_m}$

some $k_i > n_i$ for some i $= 0$

so $I^{mn} = 0$
as partition $\geq n$
$\Rightarrow a_i^n = 0$
as $a_i^{n_i} = 0$
and $n = \max\{n_1, \ldots n_m\} \geq n_i$
for $a_i^n = 0$
as $n \geq n_i$
and $a_i^{n_i} = 0$

$\therefore I^{mn} = 0$

6. $Nil(R) = \{x \mid x^n = 0 \text{ for some } n \geq 1\}$

$Nil(R)$ is an ideal as
$\forall r \in R$ and $x \in Nil(R)$
$(rx)^n = r^n x^n$
$= r^n \cdot 0$
$= r^n$
so $rx \in Nil(R)$

$\therefore Nil(R)$ is an ideal

$0 \in Nil(R)$
$Nil(R) \neq \phi$
$(-a)^n = (-1)^n a^n = 0$
$a, b \in Nil(R)$ $a^n = 0$, $b^m = 0$
$(a+b)^{n+m+1}$
$= \sum \binom{n+m+1}{\ldots} a^i b^{m+n+1-i} = 0$
$Nil(R) < (R, +)$

7. $R = \mathbb{Z}$ $S = \{7^n \mid n \geq 0\}$

Prime ideals of $S^{-1}\mathbb{Z}$ $\longleftrightarrow$ P of $\mathbb{Z}$ s.t
$P \cap S = \phi$
$P \cap (\{7^n \mid n \geq 0\}) = \phi$

$PS^{-1}\mathbb{Z}$, $0S^{-1}\mathbb{Z}$
$p \neq 7$ trivial

$P = p\mathbb{Z}$ for primes in $\mathbb{Z}$
not 7
$\therefore$ Prime ideals of $S^{-1}\mathbb{Z}$
are $(p\mathbb{Z})(S^{-1}\mathbb{Z})$
for p a prime not 7.

8. $R \leftarrow$ domain (NZD)
$P_1, P_2, \ldots P_n$ prime ideals of R

$S = R \setminus \bigcup_{i=1}^{n} P_i$ is m.c

<u>proof</u>: as $0 \in P_i$ $\forall i$
$\Rightarrow 0 \notin S$ —— ①
as $1 \notin P_i$ $\forall i$
$\Rightarrow 1 \in S$ —— ②

now if $a \in S$, $b \in S$ and $ab \notin S$ then
$a \in S \Rightarrow a \notin \bigcup_{i=1}^{n} P_i$ $b \notin \bigcup_{i=1}^{n} P_i$
and $ab \in \bigcup_{i=1}^{n} P_i$
$\Rightarrow \exists i$ s.t $a \in P_i$ or $b \in P_i$
$\Rightarrow a \in \bigcup_{i=1}^{n} P_i$ or $b \in \bigcup_{i=1}^{n} P_i$

$\Rightarrow a \notin S$, or $b \notin S$ *

$\therefore$ $a, b \in S \Rightarrow ab \in S$

$\therefore$ S is m.c

Tutorial 6:

1. $f(x) \in K[X]$ polynomial of degree 2 or 3
$\uparrow$
field

To prove: f is irreducible iff f has no root in K

proof: $(\Rightarrow)$ f is red
if $N(f) = 2$
then
$f = gh$ and $N(g) \geq 1$
$N(h) \geq 1$
$\Rightarrow N(g) = 1$
$N(h) = 1$

as $N(g) = 1$, $\exists$ a root

sim $N(f) = 3$ then
wlog $N(g) = 1$
$\exists$ a root

$(\Leftarrow)$ If a root exist then
$f = g(x - \alpha)$ so reducible

$\therefore$ f is red $\Leftrightarrow$ $\exists$ a root
$\Rightarrow$ f is irrd $\Leftrightarrow$ no root in $\mathbb{Z}[X]$

2. $x^2 + x + 1$ is irrd in $\mathbb{Z}/2\mathbb{Z}[X]$
$f(\bar{0}) = 1$
$f(\bar{1}) = 1$ so no roots in $\mathbb{Z}/2\mathbb{Z}$
$f(1) = 1$
$f(0) = 1$
$\Rightarrow$ irr in $\mathbb{Z}/2\mathbb{Z}[X]$

$x^2 + 1$ is irrd in $\mathbb{Z}/3\mathbb{Z}[X]$
as $f(\bar{0}) = 1$
same
$f(\bar{1}) = 2$
$f(\bar{2}) = 2$

so no roots in $\mathbb{Z}/3\mathbb{Z}$
$\Rightarrow x^2 + 1$ is irrd in $\mathbb{Z}/3\mathbb{Z}[X]$

3.

0	1	2	3	4	5	6
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
0	1	4	2	2	4	1

$f(\bar{0})$
$f(\bar{1})$
$\vdots$
$f(\bar{6})$

or $f(x) = x^2+1$

so $f(0)=1$
$f(1)=2$
$f(2)=5$
$f(3)=3$
$f(4)=3$
$f(5)=5$
$f(6)=1$

$\therefore x^2+1$ is irred in $\mathbb{Z}/7\mathbb{Z}[x]$

4. $\mathbb{R}, \mathbb{C}$ are <u>not</u> isomorphic as rings

if they are, then

$\exists\ \varphi : \mathbb{C} \longrightarrow \mathbb{R}$
$\alpha \longmapsto \varphi(\alpha) \in \mathbb{R}$
$\in \mathbb{C}$

φ is one-one, onto, homorphism and well defined

now $\varphi(1)=1$
then $\varphi(-1) = \varphi(1-1-1)$
$= \varphi(1)+\varphi(-1)+\varphi(-1)$
$0 = 1+\varphi(-1)$
$\Rightarrow \varphi(-1) = -1$

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

$a^2=-1$ $*$

now as $i \in \mathbb{C}$

$\varphi(i) = \alpha$ for some $\alpha \in \mathbb{R}$

$\varphi(i^2) = \alpha^2 = \varphi(-1) = -1$

$\alpha^2=-1$ $*$
as $\alpha \in \mathbb{R}$

so $\mathbb{C} \not\cong \mathbb{R}$

5. $\mathbb{Q}$, $\mathbb{R}$ are <u>not</u> isomorphic as rings

let's suppose they are, then

$\varphi : \mathbb{R} \longrightarrow \mathbb{Q}$ s.t
φ is one-one, onto, homorphism and well defined

$f: \mathbb{R} \to \mathbb{Q}$
$f(\sqrt{2}\cdot\sqrt{2}) = f(2) = 2 \Rightarrow a^2=2$ $*$
$= a\cdot a = a^2$

now $\varphi(1)=1$
$\varphi(-1)=-1$ (sim to previous calculation)

$$\varphi(1) = \varphi\Big(\underbrace{\frac{1}{m}+\frac{1}{m}+\cdots\frac{1}{m}}_{m \text{ times}}\Big)$$

$\varphi(1) = m\varphi\left(\frac{1}{m}\right)$

$\Rightarrow \quad \frac{1}{m} = \varphi\left(\frac{1}{m}\right)$

also $\varphi\left(\frac{1}{m}\right) = \frac{1}{m}$ then

$$\varphi\Big(\underbrace{\tfrac{1}{m} + \tfrac{1}{m} + \cdots \tfrac{1}{m}}_{n \text{ times}}\Big) = \frac{n}{m}$$

for $n > 0$

and if $n < 0$ then

$$\varphi\Big(\underbrace{\tfrac{1}{m} + \tfrac{1}{m} + \cdots \tfrac{1}{m}}_{-n \text{ times}}\Big) = \frac{-n}{m}$$

or $\varphi\left(\frac{-n}{m}\right) = -\frac{n}{m} \Rightarrow \varphi\left(\frac{n}{m}\right) = \frac{n}{m}$

so $\forall\, p/q \in \mathbb{Q}$, $\varphi(p/q) = p/q$

but $\exists \sqrt{2} \in \mathbb{R}$ s.t $\varphi(\sqrt{2}) \in \mathbb{Q}$ say p/q

but then $\sqrt{2} = p/q$ $\times$

6. To prove: $\mathbb{Z}[i]$ is an Euclidian domain

proof : from defination

① $\mathbb{Z}[i]$ is ID

② $\exists$ Norm s.t $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^+ \cup \{0\}$

③ $\forall a, b \in \mathbb{Z}[i]$ $\exists\, q, r \in \mathbb{Z}[i]$ $(b \neq 0)$

s.t $a = qb + r$ $\quad r = 0$ or $N(r) < N(b)$

Now $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$

if $\alpha \in \mathbb{Z}[i]$ and $\beta \in \mathbb{Z}[i]$

if

$\alpha\beta = 0$

then

$(\alpha_1 + i\alpha_2)(\beta_1 + i\beta_2) = 0$

$\Rightarrow \alpha_1\beta_1 - \alpha_2\beta_2 + i(\alpha_2\beta_1 + \beta_2\alpha_1) = 0$

$\Rightarrow \alpha_1\beta_1 = \alpha_2\beta_2$

and

$\alpha_2\beta_1 + \beta_2\alpha_1 = 0$

<u>case I</u>: $\alpha_1 \neq 0$ then

$\beta_1 = \dfrac{\alpha_2\beta_2}{\alpha_1}$

$\alpha_2\beta_2\dfrac{\alpha_2}{\alpha_1} + \beta_2\alpha_1 = 0$

$\beta_2\left(\dfrac{\alpha_2\alpha_2}{\alpha_1} + \alpha_1\right) = 0$

$\beta_2 = 0$ or $\alpha_2\alpha_2 = -\alpha_1\alpha_1$ $*$

so $\beta_2 = 0$

and also as $\beta_2 = 0$

$\Rightarrow \beta_1 = 0$

<u>case II</u>> $\alpha_2 \neq 0$, then

$\beta_2 = \dfrac{\beta_1\alpha_1}{\alpha_2}$

and agin $\beta_1 = 0$, $\beta_2 = 0$

so if $\alpha \neq 0$ then $\beta = 0$

and

wlog $\alpha = 0$ then $\beta \neq 0$

so $\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$

$\therefore$ $\mathbb{Z}[i]$ is <u>ID</u>

Now $N(\alpha) = N(\alpha_1 + i\alpha_2) = \alpha_1^2 + \alpha_2^2$

so $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^+ \cup \{0\}$

$\therefore$ N is a norm

and now

as $\alpha\bar{\alpha} = (\alpha_1 + i\alpha_2)(\alpha_1 - i\alpha_2)$

$= \alpha_1^2 + \alpha_2^2$

$\alpha\bar{\alpha} = N(\alpha)$

$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\beta}\bar{\alpha} = \alpha\bar{\alpha}\beta\bar{\beta}$

$= N(\alpha)N(\beta)$

so $N(\alpha\beta) = N(\alpha)N(\beta)$

if $N(\alpha) \neq 0$, then
$\alpha_1^2 + \alpha_2^2 \neq 0$
or
$\Rightarrow N(\alpha) \geq 1$

as $N(\alpha) \longrightarrow \mathbb{Z}^+ \cup \{0\}$
$= \{0, 1, 2, \ldots \ldots\}$

then $N(\alpha\beta) = N(\alpha)N(\beta) \geq N(\beta)$
if $N(\alpha) \neq 0$

Now if $\alpha \in \mathbb{Z}[i]$
$\beta \in \mathbb{Z}[i] \neq 0$
then

<u>To show</u>: $\exists\, q, r \in \mathbb{Z}[i]$
s.t
$\alpha = qb + r$
$N(r) < N(b)$

if $\alpha, \beta \in \mathbb{Z}[i]$ then

$$\frac{\alpha}{\beta} = p + iq \quad \text{for}$$

$p, q \in \mathbb{Q}$

now $\alpha = \beta(p + iq)$

for $a, b \in \mathbb{Z}$ s.t

$|p - a| \leq \frac{1}{2}, \quad |q - b| \leq \frac{1}{2}$

we get

$$\alpha = \beta(a + ib) + \beta((r - a) + i(s - b))$$

$\alpha = \beta\varphi + \delta$

$\varphi = a + ib \in \mathbb{Z}[i]$

$\delta = \alpha - \beta\varphi$
as $\alpha \in \mathbb{Z}[i]$
$\beta\varphi \in \mathbb{Z}[i]$

$\Rightarrow \delta \in \mathbb{Z}[i]$

so $\alpha = \beta\varphi + \delta$

now $N(\delta) = N(\alpha - \beta\varphi)$

$$= N(\beta)\, N\big((r-a) + i(s-b)\big)$$
$$= N(\beta)\left[(r-a)^2 + (s-b)^2\right]$$
$$\leq N(\beta)\left[\left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2\right]$$
$$= \tfrac{1}{2} N(\beta) \leq N(\beta)$$

so $N(\delta) \leq N(\beta)$

7. π is irred in $\mathbb{Z}[i]$

To prove: $\mathbb{Z}[i]/(\pi)$ is a finite field

proof: as π is irred in $\mathbb{Z}[i]$ and

$\mathbb{Z}[i]$ is a U.D $\Rightarrow$ $\mathbb{Z}[i]$ is a P.I.D

as π is irred in $\mathbb{Z}[i]$ $\Rightarrow$ π is prime in $\mathbb{Z}[i]$

so $\dfrac{\mathbb{Z}[i]}{(\pi)}$ = field

$\longrightarrow$ as (π) is a prime ideal and also maximal

now as (π) is prime ideal in $\mathbb{Z}[i]$ (prime in PID is maximal)

$(\pi) \cap \mathbb{Z}$ is also a prime ideal

$\Rightarrow (\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some $p \in \mathbb{Z}$

now as $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$

$p \in (\pi) \cap \mathbb{Z}$
$\Rightarrow p \in (\pi)$

now, $[\alpha] \in \dfrac{\mathbb{Z}[i]}{(\pi)}$

$\alpha = a + ib$

$a \in \{0, 1, 2 \ldots p-1\}$
$b \in \{0, 1, 2 \ldots p-1\}$

$$\left|\frac{\mathbb{Z}(i)}{(\pi)}\right| \leq p^2$$

$[\alpha] \in \dfrac{\mathbb{Z}[i]}{(\pi)}$ — the cosets will be $\leq p^2$

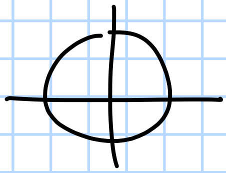
(as $\dfrac{\mathbb{Z}[i]}{(\pi)}$ is field)

$\alpha = \pi x + r$
$[\alpha] = [r]$
$r = 0$ or $N(r) < N(\pi)$
$= a^2 + b^2$

and each coset will have finite elements

$r = r_0 + i r_1$

$r_0^2 + r_1^2 < a^2 + b^2 = c$



only finitely many points possible

Here any coset has finite elements

8. $\mathbb{C}[X]$ is a PID then

$X - \alpha$ is irreducible

$\Rightarrow (X-\alpha)$ is irred

$\Rightarrow (X-\alpha)$ is prime

$\Rightarrow (X-\alpha)$ is maximal as $\mathbb{C}[X]$ is a PID

$P_i = (X - i)$

now let $S = R \setminus \bigcup_{i=1}^{n} (X - i)$

and let $A = S^{-1}R$

now $S^{-1}P_1, S^{-1}P_2, \dots\dots S^{-1}P_n$ primes in A

as $P_i \cap S = \phi$ and P_i is prime in R

as $\left\{ \text{prime ideals of } S^{-1}R \right\} \longleftrightarrow \left\{ \text{prime } P \text{ of } R \text{ s.t } P \cap S = \phi \right\}$

$\#$ prime ideals of $S^{-1}R$ $= n$

now, let $PS^{-1}R$ s.t P be a prime in R be prime in $S^{-1}R$

Note: R is P.I.D, S is m.c then $S^{-1}R$ is also P.I.D

as $J \trianglelefteq S^{-1}R$ → ideal of $S^{-1}R$

then as $S^{-1}R$ is a fraction ring

$(J \cap R)S^{-1}R = J$

$(a)S^{-1}R = J$

↑ or $S^{-1}R$ is a PID

$P \cap S = \phi$

and $P = (X - \alpha)$

$P \subseteq \bigcup_{i=1}^{n} P_i$

so (P) is prime → (P) is maximal

$x - \alpha \in P_i$

$(X - \alpha) \subseteq P_i$

maximal ideal in R $\Rightarrow (X-\alpha) = P_i$ or P_i is a maximal ideal

$\#$ maximal ideals in $S^{-1}R = n$

Tutorial - 7 :

1. T/M, T/N are noetherian

To show : $T/_{M\cap N}$ is noetherian

Prove $T/M \oplus T/N$ is noetherian

then $\psi : T \to T/M \oplus T/N$
$t \mapsto (t+M, t+N)$

as $\psi : T \longrightarrow T/M \oplus T/N$
$t \longmapsto (t+M, t+N)$

then

$$\ker(\psi) = M \cap N = \{ t \in T \mid (t+M, t+N) = (0,0) \text{ or } t \in M \,\&\, t \in N \}$$

① ψ is well-defined as for

$t_1 = t_2$
$t_1 + M = t_2 + M$
$\&$ $t_1 + N = t_2 + N$

$\frac{T}{M\cap N} \hookrightarrow T/_M \oplus T/_N$

so $T/_{M\cap N} \leq T/_M \oplus T/_N$ submodule $\Rightarrow T/_{M\cap N}$ is noetherian

② ψ is homomorphic as

$$\psi(t_1 + t_2) = (t_1 + t_2 + M, t_1 + t_2 + N)$$
$$= (t_1 + M, t_1 + N) + (t_2 + M, t_2 + N)$$
$$= \psi(t_1) + \psi(t_2)$$

$$\& \ \psi(\alpha t) = (\alpha t + M, \alpha t + N)$$
$$= (\alpha t + \alpha M, \alpha t + \alpha N)$$
$$= \alpha(t + M, t + N)$$
$$= \alpha \psi(t)$$

③ ψ is surjective : for $M, N \leq T$
if $x \in M$
then
$\psi(x) = (0, x+N)$
for $y \in N$ $\quad \psi(y) = (y+M, 0)$

$$\psi(x+y) = (y+M, x+N)$$

or

$\forall (y+M, x+N) \in T/M \oplus T/N$
$\exists \ x+y \in T$ s.t
$\psi(x+y) = (y+M, x+N)$

$\therefore \psi$ is surjective

or $\quad T/\ker\psi \cong T/M \oplus T/N$

$\Rightarrow T/M\cap N \cong T/M \oplus T/N$

as T/M, T/N are noeth
$\Rightarrow T/M \oplus T/N$ is also noeth
$\Rightarrow T/M \cap N$ is also noeth

2. $M \cong N$ both R-module

To show: $\forall I \leq R \Rightarrow M/IM \cong N/IN$

proof : $IM = \{ \text{finite sum of } a_i \in I \text{ with } m_i \in M \}$
$= \{ \alpha_1 m_1 + \dots \alpha_r m_r \mid \alpha_i \in I, m_i \in M \}$

let $\varphi : M \to N$ s.t φ is isom
$m \mapsto \varphi(m)$ $\quad$ & $M \cong N$
for this map

then $\tilde{\varphi} : M \longrightarrow N/IN$
$m \longmapsto \varphi(m) + IN$

$\ker \tilde{\varphi} = \{ m \in M \mid \varphi(m) \in IN \}$

$\forall m \in \ker \tilde{\varphi}$
as $\varphi(m) \in IN$
$\Rightarrow \varphi(m) = \alpha_1 n_1 + \cdots \alpha_s n_s$
$\Rightarrow m = \varphi^{-1}(\alpha_1 n_1 + \cdots \alpha_s n_s)$
$= \alpha_1 \varphi^{-1}(n_1) + \cdots \alpha_s \varphi^{-1}(n_s)$
$\in IM$
or $\ker \tilde{\varphi} \subseteq IM$

$\phi : M \to N$
$\psi : \phi^{-1} : N \to M$
then

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ & \searrow^{\eta\circ\phi} & \downarrow \eta \\ & & N/IN \end{array}$$

$\phi(IM) \subseteq IN$

$\bar{\phi} : M/IM \longrightarrow N/IN$
$m + IM \longmapsto \phi(m) + IN$

$\bar{\psi} : N/IN \longrightarrow M/IM$
$n + IN \longrightarrow \psi(n) + IM$

$\bar{\psi} \circ \bar{\phi}(m + IM) = \psi \circ \phi(m) + IM$
$= m + IM$

$\bar{\psi} \circ \bar{\phi} = 1_{M/IM}$
$\bar{\phi} \circ \bar{\psi} = 1_{N/IN}$

So, $M/IM \cong N/I$

now $\forall k \in IM$
$\Rightarrow k = a_1 m_1 + \cdots a_e m_e$
$\Rightarrow \varphi(k) = \alpha_1 \varphi(m_1) + \cdots a_e \varphi(m_e)$
$\Rightarrow \varphi(k) \in IN$
$\Rightarrow k \in \ker \tilde{\varphi}$
$\Rightarrow IM \subseteq \ker \tilde{\varphi}$

proving $\tilde{\varphi}$ is ① well-defined &
② homomorphic
is trivial

$\tilde{\varphi} : M \longrightarrow N/IN$
is surjective as
$m \longmapsto \varphi(m) + IN$
then $\varphi(m) = n$
then $\forall n \in N/IN$
$\exists m$ s.t
$m = \varphi^{-1}(n)$

as $M \cong N$

$\therefore M/\ker \tilde{\varphi} \cong N/IN$
$\Rightarrow M/IM \cong N/IN$

3. $\operatorname{ann}(M) = \{ r \in R \mid rm = 0 \quad \forall m \in M \}$

<u>To show</u>: $\operatorname{Ann}(M)$ is ideal in R
<u>proof</u>:
for $r_1 \in \operatorname{Ann}(M), r_2 \in \operatorname{Ann}(M)$
$(r_1 + r_2)(m) = r_1 m + r_2 m = 0$
$\Rightarrow r_1 + r_2 \in \operatorname{Ann}(M)$
$\Rightarrow (\operatorname{Ann}(M), +) \leq (R, +)$

① $0 \in \operatorname{Ann}(M)$
② $x, y \in \operatorname{Ann}(M)$
$\forall m \in M \Rightarrow (x - y)m = 0$
$\Rightarrow x - y \in \operatorname{Ann}(M)$
$(\operatorname{Ann}(M), +) \leq (R, +)$

now for $\forall a \in \operatorname{Ann}(M)$ & $r \in R$
$(r.a)m = r(am) = r.0 = 0$
$\forall m \in M$
$\Rightarrow ra \in \operatorname{Ann}(M)$
$\therefore \operatorname{Ann}(M) \leq R$

$x \in \operatorname{Ann} M$
$r \in R$
$(rx)m = r(xm)$
$= r.0$
$= 0$
$\forall m \in M$
$\operatorname{ann} M \leq R$

<u>To show</u>: M is $R/\operatorname{ann}(M)$ module
<u>proof</u>: for $(r + \operatorname{Ann}(M)).m = r.m + \operatorname{Ann}(M).m$
$= rm$

M is $R/\text{Ann}\,M$-module
$(r + \text{ann}\,M)\cdot m = rm$
$r + \text{ann}\,M = r' + \text{ann}\,M$
$\Rightarrow r = r' + x \in \text{Ann}\,M$
$\Rightarrow rm = r'm$
$\therefore$ well defined

$$s + \text{Ann}(M) = r + \text{Ann}(M)$$
$$\Rightarrow sm = rm$$
$\therefore$ well defined

also $(s_1 + s_2)m = s_1 m + s_2 m$ for $s_1, s_2 \in R/\text{Ann}(M)$

$$(s_1 \cdot s_2)m = (s_1(s_2 m))$$

as $1_{R'}(m) = m$
$r'(m_1 + m_2) = r'm_1 + r'm$
$\therefore$ M is $R/\text{Ann}(M)$-module

4. M is noeth R-module then $R/\text{ann}(M)$ is noeth ring

proof: as M is noeth R module
M is f.g
or say
$$M = \langle m_1, \dots, m_s \rangle$$
as M is noeth
$$\Rightarrow \underbrace{M \oplus M \oplus \cdots \oplus M}_{s \text{ times}} \text{ is also noeth}$$

proof:
$M = \langle m_1, \dots, m_s \rangle$
$\psi : R \to M^s$
$\ker \psi = \text{Ann}(M)$
$\therefore$
$R/\ker\psi = \psi(M^s) \leq M^s$
so $R/\ker\psi$ is noterian

$$\Rightarrow M^s \text{ is noeth}$$

if $\psi : R \longrightarrow M^s$
$1 \longmapsto (m_1, \dots, m_s)$
$r \longmapsto (rm_1, \dots, rm_s)$
as ψ is well define & Homorphic (trivial)
then $R/\ker\psi \cong \psi(M^s)$
Here $\ker\psi = \{ r \in R \mid \psi(r) = 0 \}$
as $\psi(r) = 0$
$\Leftrightarrow r.m_i = 0 \ \forall i \in \{1, 2 \dots s\}$
$\Leftrightarrow r \in \text{Ann}\,M$

or $\ker\psi = \text{Ann}\,M$

now, $R/\text{Ann}\,M \cong \psi(M^s)$

as M^s is noeterian and
$\psi(M^s) \leq M^s$ or $\psi(M^s)$ is sub-module and here also noeth

$\therefore R/\text{Ann}\,M$ is noeth ring

5. $\underset{\text{noeth}}{R} \Rightarrow \underset{\text{noeth}}{R[x]}$ (Hilbert's basis theorm)

if $R[x]$ is noeth & $R \leq R[x]$ (trivial)
$\Rightarrow R$ is noeth

$\therefore \underset{\text{noeth}}{R} \Leftrightarrow \underset{\text{noeth}}{R[x]}$

$\frac{R[x]}{(x)} \cong R$ is also noeth
$(x) \leftarrow$ ideal of $R[x]$

6. $R = k[X,Y]/(X,Y)^5$

or

$R = [k + (X,Y)^5]$

where $k \in k[X,Y]$

then

$(X,Y)^5$ is 0 in R

then

$M = (X,Y)M$

$= (X,Y)(X,Y)M$

$= \vdots$

$= (X,Y)^5 M$

$M = 0.M = 0$

$M = (X,Y)M$

$= \ldots$

$\ldots$

$M = (X,Y)^5 M$

$\Rightarrow M = 0$

7. M is R-module

To show: $\mathcal{C} = \{S \leq M \text{ s.t } S \text{ is f.g and } S \subsetneq M\}$

then

$\mathcal{C}$ has a maximal element

$\Rightarrow M$ is noeth

Proof: Now let

$S_1 \leq S_2 \leq S_3 \ldots$

then this is chain of as f.g submodules in M then

it has a maximal elemt

say S_{n_0}

after this

$S_n = S_{n_0} \quad \forall\, n \geq n_0$

doubt

$\therefore M$ is noeth

$N \leq M$

we want to show N is f.g

$\mathcal{C} = \{E \mid E \text{ is f.g submodule of } N\}$

let E_0 be maximal elemt of $\mathcal{C}$

$E_0 = \langle u_1 \ldots u_r \rangle$

If $E_0 \neq N$ then let

$n \in N \setminus E_0 \Rightarrow E_0 \subsetneq (u_1, \ldots u_r, n) \in \mathcal{C}$ *

8. for any $n \geq 1$, to make a ring with n prime ideals all of which are maximal

doubt

$$\frac{\mathbb{Z}}{(p_1 p_2 \ldots p_n)\mathbb{Z}} = R$$

p_i distinct primes

$\bar{m}$ maximal in R

$m \supseteq (p_1 \ldots p_n)$

so $p_i \in m$

$m = (p_i)$

$$\mathbb{Z}/(p_1 p_2 \ldots p_n) \cong \underbrace{\mathbb{Z}/(p_1) \oplus \mathbb{Z}/(p_2) \oplus \mathbb{Z}/(p_3) \oplus \cdots \oplus \mathbb{Z}/(p_n)}_{\text{fields}}$$

$\therefore n$ maximal fields $\to \{0\} \leftarrow$ only maximal sample Quiz-1 :

1. $|G|<\infty$, $p \mid |G|$

To prove: $\exists\, x \in G$ s.t $\operatorname{ord}(x) = p$ (Cauchy's theorem)

proof :

let $S = \left\{ (x_1, \dots x_n) \;\middle|\; \begin{array}{l} x_1 x_2 \dots x_n = e \\ \text{and } x_i \in G \ \forall i \end{array} \right\}$

then

$$|S| = \underbrace{|G| \times |G| \times \cdots |G|}_{n-1 \text{ times}}$$

(as we have to have find x_n for any combination of $x_1 x_2 \dots x_{n-1}$)

$|S| = |G|^{n-1}$

$\Rightarrow p \mid |S|$ (as $p \mid |G|$)

now, let $H = \{1, \sigma, \sigma^2, \dots \sigma^{n-1}\}$

where

$\sigma(x_1 \dots x_n) = (x_2, x_3 \dots x_n, x_1)$

Action on S legitimate

$|H| = p$

and also see that if

$x_1 x_2 x_3 \dots x_n = 1$

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

$\Rightarrow x_2 x_3 \dots x_n x_1 = 1$

now, this means that by using the class equation on S

$$|S| = |Z(S)| + \sum_{a \in G} |G/G_a|$$

we have $p \mid |S|$

$\Rightarrow p \mid |Z(G)| + \sum |G/G_a|$

as $O_a = \{ h(a) \mid \forall h \in H \}$

it can have $|O_a| = 1$ or p

if 1 then $a \in O_a$ (trivial)

$\Rightarrow \{a\} = \{ h(a) \mid \forall h \in H\}$

$\Rightarrow a = h(a) \ \forall\, h \in H$

$\Rightarrow a \in Z(G)$

as $p \mid |Z(G)| + \sum |G/G_a| = |Z(G)| + kp$

$\Rightarrow p \mid |Z(G)| \Rightarrow |Z(G)| \neq 1$

$\Rightarrow \exists\, x \in Z(G)$ s.t

$h(x) = x \ \forall\, h \in H$ & $x \neq e$

$\Rightarrow h(x_1, x_2 \dots x_n) = (x_1, x_2, \dots x_n) \ \forall h \in H$

$\Rightarrow x_2 = x_1 = \dots x_n = \bar{x}$ (say)

$\Rightarrow (\bar{x})^p = e$

$\therefore (\bar{x}) \neq e$ and $(\bar{x})^p = e$

or $\operatorname{ord}(\bar{x}) = p$

with sylow: $|H| = p^e$ (direct)

if $e = 1$, done else $\operatorname{ord}(x^{p^{(e-1)}}) = p$

2. To prove : The following groups are not cyclic :
Proof :
(a) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = G$
then $|G| = 4$

$$G = \{ (\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{1}) \}$$
ord 1 ord 2 ord 2 ord 2
as no element has ord 4
not cyclic

(b) $\mathbb{Z} \times \mathbb{Z} = G$
then if G is cyclic $G = \langle (a,b) \rangle$
$(1,0) = m(a,b)$
$\Rightarrow b = 0$
$(0,1) \neq n(a,b)$ as $b = 0$ *

3. $Z(G) = \{ x \in G \mid gxg^{-1} = x \ \forall g \in G \}$

To prove : $[x] = \{ gxg^{-1} \mid \forall g \in G \}$ ← conjugacy class (orbit of x)
$O_x = \{ gxg^{-1} \mid \forall g \in G \}$

$|O_x| \leq n$

proof :
let $\psi : O_a \longrightarrow G/G_a$ ← stabiliser of G
$gag^{-1} \longmapsto gG_a$

well defined :
for $g_1 a g_1^{-1} = g_2 a g_2^{-1}$
$G_a = \{ g \in G \mid gag^{-1} = a \}$
$\Rightarrow g_1 a g_1^{-1} = g_2 a g_2^{-1}$
$g_2^{-1} g_1 a (g_1 g_2^{-1})^{-1} = a$
$\Rightarrow g_2^{-1} g_1 \in G_a$
$\Rightarrow g_1 G_a = g_2 G_a$
$\Rightarrow \psi(g_1 a g_1^{-1}) = \psi(g_2 a g_2^{-1})$

one-one : If $g_1 G_a = g_2 G_a$
then
$\Rightarrow g_2^{-1} g_1 \in G_a$
$\Rightarrow g_2^{-1} g_1 \, a (g_2^{-1} g_1)^{-1} = a$
$\Rightarrow g_1 a g_1^{-1} = g_2 a g_2^{-1}$

onto : $\forall \ gG_a \in G/G_a$
$\exists \ gag^{-1}$ s.t $\psi(gag^{-1}) = gG_a$ (trivial)

$\therefore |[x]| = |O_x| = |G/G_x|$ (Bijection) now, as $Z(G) = \{x \in G \mid gxg^{-1} = x \ \forall g \in G\}$

and $G_x = \{g \in G \mid gxg^{-1} = x \ \forall g \in G\}$

if $\alpha \in Z(G)$ then

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

$G_x = \{g \in G \mid gxg^{-1} = x\}$

putting x here

$x\alpha x^{-1} = \alpha$

$\Rightarrow \alpha x^{-1} = x^{-1}\alpha$

$\Rightarrow \alpha x^{-1}\alpha^{-1} = x^{-1}$

$\Rightarrow \alpha^{-1} x \alpha = x$

$\Rightarrow \alpha^{-1} \in G_x$

$\Rightarrow \alpha \in G_x$ (as G_x is a subgroup)

$\Rightarrow Z(G) \subseteq G_x$

then

$$\left| G/Z(G) \right| \geq \left| G/G_x \right| = |O_x|$$

$\Rightarrow |O_x| \leq n$

as index of $Z(G) = n = \left| G/Z(G) \right|$

4. S_n is symmetric group

A_n is subgroup of even permutations

$H \leq S_n$

<u>To prove</u>: $H \subseteq A_n$ or $|H \cap A_n| = \frac{1}{2}|H|$

<u>proof</u>: $\varepsilon : S_n \longrightarrow \{\pm 1\}$

be the sign of homorphism

i.e

$f \in S_n$

Bijection, then sign of it is $+1$ or -1.

$\therefore$ $\varepsilon : S_n \longrightarrow \{\pm 1\}$

$f \longmapsto sgn(f)$

$\varepsilon(f) = sgn(f)$

<u>ε is well defined</u>: as $f_1 = f_2$

then

$sgn(f_1) = sgn(f_2$

<u>ε is homorphism</u>:

$\varepsilon(f_1) = sgn(f_1)$

$\varepsilon(f_2) = sgn(f_2)$

then

$\varepsilon(f_1 f_2) = sgn(f_1 f_2) = sgn(f_1)\, sgn(f_2)$

$= \varepsilon(f_1)\, \varepsilon(f_2)$

now $\tilde{\varepsilon} : H \longrightarrow \{\pm 1\}$

$\tilde{\varepsilon}(H) = \{1\}$ then $H \subseteq A_n$

if $\tilde{\varepsilon}(H) = \{\pm 1\}$ then
$\operatorname{Im}(\tilde{\varepsilon}) = \{\pm 1\}$ or
onto

and so $H/\ker\tilde{\varepsilon} \cong \{\pm 1\}$

$$\Rightarrow \left| H/\ker\tilde{\varepsilon} \right| = 2$$
$$\Rightarrow |H| = 2|\ker\tilde{\varepsilon}|$$
$$\Rightarrow \tfrac{1}{2}|H| = |\ker\tilde{\varepsilon}|$$

But $\ker\tilde{\varepsilon} = \left\{ f \in H \;\middle|\; \begin{array}{l} sgn(f) = 1 \\ \text{or } f \in A_n \end{array} \right\}$
$= H \cap A_n$

$$\therefore |\ker\tilde{\varepsilon}| = |H \cap A_n| = \tfrac{1}{2}|H|$$

sample midsem:

1. sylow's third theorm :

$|G| = p^k m \quad k \geq 1, \; p \nmid m$

then

n_p = no of psylow subgroups of G

① $n_p \equiv 1 \mod p$

② and $n_p \mid m$

sylows third theorm proof :

$N = \{g \in G \mid gHg^{-1} = H \;\forall g \in G\}$ where H is a sylow p G

let Ψ: sylow p subgroup $\longrightarrow G/N$

$K = gHg^{-1} \longmapsto gN$

then

① well defined and one-one

$g_1 H g_1^{-1} = g_2 H g_2^{-1}$

$\Leftrightarrow g_2^{-1} g_1 \in N$

$\Leftrightarrow g_1 N = g_2 N$

② onto as : $\forall gN = x \Rightarrow \exists\, gHg^{-1} \in$ Sylowpsubgroup s.t $K = gHg^{-1}$

$\therefore$

$|\#\text{Sylowp } G| = |G/N|$

$n_p = |G/N| = \dfrac{|G/H|}{|N/H|}$

$\Rightarrow |N/H|\, n_p = |G/H| = m$

$\Rightarrow n_p \mid m$

now, as H acts on sylowp subgroup by conjugation

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

then

$\text{Sylowp}(G) = O_{K_1} \sqcup O_{K_2} \cdots \sqcup O_{K_r}$

now if $|O_K| = 1$ then

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

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

as $K \trianglelefteq N(K)$

$\Rightarrow K \trianglelefteq H$

$\Rightarrow K = H$ as $|K| = |H|$

if $|O_K| \neq 1$ and

as $|O_K| = |H / C_H(K)| = \dfrac{|H|}{|C_H(K)|} = \dfrac{p^r}{|C_H(K)|}$

$\Rightarrow |O_K| \mid p$

$\Rightarrow |O_K| = p$ as $|O_K| \neq 1$

$\therefore \ | \# \text{sylow } p(G)| = |O_H| + \cdots$
$= 1 + p(r-1)$
or $n_p \equiv 1 \bmod p$

2. p is a prime let

$$H = \mathbb{Z}/p^2\mathbb{Z}$$
then
$$\text{Aut}(H) \cong \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times}$$

$$\text{ord}(\text{Aut}(H)) = (p)(p-1)$$
as
$$p \mid \text{ord}(\text{Aut}(H))$$
$$\Rightarrow \exists \ x \in \text{Aut}(H)$$
s.t $\text{ord}(x) = p$

now let $K = \mathbb{Z}/p\mathbb{Z}$

$$\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/p^2\mathbb{Z})$$
$$\bar{1} \longmapsto x$$
$$\bar{i} \longmapsto x^i$$
then φ is non-trivial group homomorphism

$\Rightarrow$ so $H \rtimes K \neq H \times K$
and
$G = H \rtimes K$ s.t
$|G| = p^3$,
and as $K \ncong H \rtimes K$
$\Rightarrow G$ is <u>not</u> <u>abelian</u>

3. $H, K \trianglelefteq G$
$G = HK$

<u>To prove</u>: $G/H \cap K \cong G/H \times G/K$

<u>proof</u>: let $\psi : G \longrightarrow G/H \times G/K$
$g \longmapsto (gH, gK)$
then
① <u>well defind</u>
trivial
② <u>homomorphism</u>:
as
$$\psi(g_1 g_2) = (g_1 g_2 H, g_1 g_2 K)$$
$$= (g_1 H g_2 H, g_1 K g_2 K)$$
$\because H \trianglelefteq G, K \trianglelefteq G$
$$\psi(g_1, g_2) = (g_1 H, g_1 K) \cdot (g_2 H, g_2 K)$$

③ $\ker \psi = \{g \in H, g \in K\}$
$= H \cap K$

④ <u>ψ is onto</u>:
as $H, K \trianglelefteq G$ & $G = HK$
$\Rightarrow G = KH$
now, for $x = (\alpha H, \beta K)$

$\phi(\theta_1) = (\alpha H, K)$

$\phi(\theta_2) = (H, \beta K)$

as $\alpha \in G$

$\alpha = kh$

$\alpha H = kH$

so $\theta_1 = k$

$\therefore \phi(\theta_1) = (\alpha H, K)$

now

similarly $\beta = h'k'$

$\beta K = h' K$

let $\theta_2 = h'$

then

$\phi(\theta_2) = (H, \beta K)$

$\therefore \exists\ \theta_1, \theta_2$ s.t

$\phi(\theta_1) = (\alpha H, K)$

$\phi(\theta_2) = (H, \beta K)$

so $\phi(\theta_1\theta_2) = (\alpha H, \beta K)$

$\therefore \exists\ \theta_1\theta_2 \in G$ s.t $\forall\ x = (\alpha H, \beta K)$

$\phi(\theta_1\theta_2) = x$

$\therefore G/H\cap K \cong G/H \times G/K$

4. $|G| = pq$

To show: G is not simple

proof: as $|G| = pq$

wlog $q > p$ then

$n_q \equiv 1 \bmod q$

and $n_q \mid p$

but as $p < q$

and $n_q = 1, 1+q, \ldots$

$\Rightarrow n_q = 1$

$\therefore \text{Sylow}_q(G) = 1$

or $\forall g \in G$

$gHg^{-1} = H$ $\leftarrow \text{Sylow}_q(G)$

$\Rightarrow H \trianglelefteq G$ $\quad |H| = q \therefore H \neq \{0\}, G$

$\Rightarrow G$ is not simple

5. G is a group of order 15

then

$|G| = 15 = 3 \cdot 5$

$n_5 = 1,\ n_3 = 1$ and $H \cap K = \{e\}$

$G = HK$

and $H, K \trianglelefteq G$ so $G/H\cap K \cong G/H \times G/K$

$\Rightarrow G \cong G/H \times G/K$

$\Rightarrow G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$\Rightarrow G \cong \mathbb{Z}/15\mathbb{Z}$ as $\gcd(3,5)=1$

6. H is cyclic
$H \trianglelefteq G$
and $|G| < \infty$

To prove : every subgroup of H is normal in G

proof : as $H \trianglelefteq G$ and
H is cyclic

$K \leq \langle x \rangle \trianglelefteq G$
$gKg^{-1} \leq gHg^{-1} = H$
as H is normal
and $|gKg^{-1}| = |K|$
but as H is cyclic
H contains a unique
K of order $|K|$
$\therefore$ $|gKg^{-1}| = |K|$
$\Rightarrow gKg^{-1} = K \ \forall g \in G$
$\Rightarrow K \trianglelefteq G$

7. $H \leq (\mathbb{Q}, +)$
and $|G/H| < \infty$
(finite index)

let
$G/H = \{g_1H, g_2H, \ldots g_nH\}$
for
some $g_1, g_2 \ldots g_n \in G$
$g_1 = e$
or
$G/H = \{H, g_2H, \ldots g_nH\}$
$\mathbb{Z}/H\cap\mathbb{Z} \hookrightarrow \mathbb{Q}/H$ or $|\mathbb{Z}/H\cap\mathbb{Z}|$ is finite
now $H \cap \mathbb{Z} = m\mathbb{Z}$
as $H \cap \mathbb{Z} \leq \mathbb{Z}$
now if $m=1$
then
nothing, else
if $m \neq 1$ then
$H \cap \mathbb{Z} = m\mathbb{Z}$ for some $m \in \mathbb{N}, m > 1$
now, this means
if $|\mathbb{Q}/H| = t$

then
$\frac{1}{n^i} + H \in \mathbb{Q}/H$
and as $|\mathbb{Q}/H| = t < \infty$

$\Rightarrow \frac{1}{n^i} = \frac{1}{n^j} + h$ for some $h \in H$
for $i > j$
$\Rightarrow 1 = n^{i-j} + n^i h$
as $n^{i-j} \in H$
and $n^i h \in H \Rightarrow 1 \in H \Rightarrow m \neq 1$ $*$
now this means $H \cap \mathbb{Z} = \mathbb{Z}$
and if $x \in \mathbb{Q}$ say $x = \frac{p}{q}$
as $p \in H$

$$\frac{1}{q}+H, \quad \dots \quad \frac{1}{q^{t+1}}+H$$

s.t $\frac{1}{q^i}+H = \frac{1}{q^j}+H$

$$\frac{1}{q^i} = \frac{1}{q^j} + h \text{ for } i>j$$

$$\Rightarrow \frac{1}{q} = \frac{q^{i-1}}{q^j} + h(q^{i-1})$$

$$= q^{i-1-j} + h(q^{i-1}) \in H$$

$$\Rightarrow \frac{1}{q} \in H$$

so $p/q \in H$

$\therefore H = \mathbb{Q}$

8. $|G| < \infty$, $H \leq G$ s.t $|H| = n$

$$\mathcal{C} = \{H \mid H \leq G, |H| = n\}$$

$$K = \bigcap_{H \in \mathcal{C}} H$$

let $x \in K$, $g \in G$

$gxg^{-1} \in gHg^{-1}$

as $gHg^{-1} \in \mathcal{C}$ $\forall H \in \mathcal{C}$

and $g\mathcal{C}g^{-1} = \mathcal{C}$

so $gxg^{-1} \in \bigcap_{H \in \mathcal{C}} gHg^{-1} = \bigcap_{H \in \mathcal{C}} H$

$\Rightarrow gxg^{-1} \in K$

$\Rightarrow K \trianglelefteq G$

9. p is prime <u>To find</u>: sylow p of $Gl_2(\mathbb{Z}/p\mathbb{Z})$

$$|Gl_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$$
$$= p(p^2-1)(p-1)$$

so all sylow $p(G)$ will be cyclic as $|\text{any sylow}_p G| = p$

if $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z}/p\mathbb{Z} \right\}$

then $|H| = p$

and also $H \leq G$

and H is a subgroup is trivial

$\therefore$ H is one such sylow p G

10. $R \neq 0$ **To prove**: R has a maximal ideal

proof: let $\mathcal{C} = \{ I \leq R \mid I \text{ is proper} \}$
$\hookrightarrow$ ideal of R

then
① $\mathcal{C}$ is non-zero as $\{0\} \in \mathcal{C}$
② $\mathcal{C}$ is Poset as $\forall I \in \mathcal{C}$
$I \subseteq I$
if $I \subseteq J$ and $J \subseteq I$
then $I = J$
and $I \subseteq J$, $J \subseteq K$
$\Rightarrow I \subseteq K$

③ if C = chain then

$$J = \bigcup_{I \in C} I$$

is s.t $J \in \mathcal{C}$ as $0 \in I \; \forall I \in C \Rightarrow 0 \in J$
$(J,+) \leq (R,+)$
as $(I,+) \leq (R,+)$
$\forall I \in C$
as $\forall r \in R$
and $x \in J$
$r.x \in J$
as $x \in I$ (some)
and here
as $rx \in I$
$\Rightarrow rx \in J$
so J is an ideal

now as $1_R \notin I \;\; \forall I \in C$
$\Rightarrow 1_R \notin J$
$\therefore$ J is also proper s.t $I \subseteq J \;\; \forall I \in C$
$\therefore J$ is upperbound of C
so every chain has upper bound.

$\therefore$ By Zorns lemma $\exists$ maximal element in $\mathcal{C}$.
say M
$\therefore M$ is the maximal ideal

11. $I + J = R$
To prove: $I \cap J = IJ$

proof: as $I + J = R$
$\exists x \in I$, $y \in J$
s.t
$x + y = 1$
now,
$\forall \alpha \in I \cap J$
we have $\alpha \in I$
but as $\alpha \in I$, $\alpha \in K$
$\alpha \cdot 1 = \alpha(x+y)$
$= \alpha x + \alpha y$
now $\alpha x = x\alpha \in IJ$
as $x \in I$, $\alpha \in J$
and commutative
& $\alpha y \in IJ$

$\Rightarrow \alpha(x+y) \in IJ$
$\Rightarrow \alpha \cdot 1 \in IJ$
$\Rightarrow \alpha \in IJ \Rightarrow I \cap J \subseteq IJ$

now if $\alpha \in IJ$

then $\alpha = ij$ for $i \in I$

& $j \in J$

then

as $\forall r \in R$

$ir \in I$

$\Rightarrow ij \in I$

and similarly

$ij \in J$

or

$\alpha \in I \cap J$

$\Rightarrow IJ \subseteq I \cap J$

so $IJ = I \cap J$

Sample Quiz-2:

1. I is ideal in $K[X]$

<u>To prove</u>: I is principle

<u>proof</u>: If $I = \{0\}$ then is nothing to show.

If $I \neq 0$ then let

$$e = \{\deg(f(x)) \mid f(x) \in I\}$$

let

$$r = \min e \quad (\text{By WOP})$$

let deg of $g(x) = r$

$g(x) \in I$

$\forall P(x) \in K[X]$

now let $f(x) \in I$

then

$$f(x) = g(x)\,p(x) + r(x)$$

if $r \neq 0$ then

$\deg r(x) < r = \min e$ *

$\Rightarrow r(x) = 0$

$\Rightarrow f(x) = g(x)\,p(x)$

or

$\forall f(x) \in I \Rightarrow f(x) = g(x)\,p(x) \in \langle g(x) \rangle$

$\therefore I \subseteq \langle g(x) \rangle$

now $\forall g(x) \in I$

as $p(x) \in K[X]$

$\Rightarrow$

$g(x)\,p(x) \in I$

$\Rightarrow \langle g(x) \rangle \subseteq I$

so $I = \langle g(x) \rangle$

2. R is ID

<u>To prove</u>: $R \setminus \bigcup_{i=1}^{s} P_i$ is m.c

<u>proof</u>:

as $1 \notin P_i \;\; \forall i = 1, 2 \ldots s$

$\Rightarrow$

$1 \in R \setminus \bigcup_{i=1}^{s} P_i$ —— ①

also $0 \in P_i \;\; \forall i = 1 \ldots s$

$\Rightarrow$

$0 \notin R \setminus \bigcup_{i=1}^{s} P_i$ —— ②

now if $\alpha, \beta \in R \setminus \bigcup_{i=1}^{s} P_i$

$\Rightarrow \alpha \notin P_i \;\; \forall i = 1, 2 \ldots s$

&

$\beta \notin P_i \;\; \forall i = 1, 2 \ldots s$

then $\alpha\beta \notin P_i \;\; \forall i = 1 \ldots s$

$\Rightarrow \alpha\beta \in R \setminus \bigcup P_i$

3. R is UFD , K is field of fractions

$p(x) \in R[X]$
is non-zero constant polynomial

<u>To prove</u>: $p(x)$ is reducible in $K[X] \Rightarrow p(x)$ is reducible in $R[X]$

<u>proof</u>: if $p(x)$ is reducible in $K[X]$ then

$$p(x) = A(x)B(x) \text{ for some } A(x), B(x) \in K[X]$$

now
let a = lcm of all the denominators of coef of A
b = lcm of all the denominators of coef of B

then $ab\,p(x) = a'(x)\,b'(x)$
$\in R[x] \in R[X]$

$$d\,p(x) = a'(x)\,b'(x) \quad d \in R$$

if d is a unit then we are done
as

$$p(x) = d^{-1} a'(x)\, b'(x)$$

$$a(x) = d^{-1} a'(x)$$
$$b(x) = b'(x)$$

if d is not a unit, but as $d \in R$

$$d = \underbrace{p_1 p_2 \dots p_r}_{\text{irreducibles}}$$

so $p_1 p_2 \dots p_r\, p(x) = a'(x)\, b'(x)$
taking mod p_i

$$\Rightarrow \quad 0 = \overline{a'(x)}\;\overline{b'(x)}$$
as R is ID
$$\Rightarrow \overline{a'(x)} = 0$$
or $\overline{b'(x)} = 0$

wlog $\overline{a'(x)} = 0$
then

$$a'(x) = p_i\, \tilde{a}(x)$$

then
$$p_1 \dots p_{i-1} p_{i+1} \dots p_r\, p(x) = \tilde{a}(x)\, b'(x)$$
if we repeat the process

then we get $p(x) = a(x)b(x)$
$\in R(x) \in R[X]$

$\Rightarrow p(x)$ is red in $R(x)$

4. x^4+1 is irreducible in $\mathbb{Z}[X]$

$$f(x) = x^4+1$$
$$f(x+1) = (x+1)^4+1$$
$$= (x^2+2x+1)^2+1$$
$$= x^4+4x^2+1+4x^3+4x+2x^2+1$$
$$= x^4+4x^3+6x^2+4x+2$$

as $2|4,\ 2|6,\ 2|4,\ 2|2$

but $4 \nmid 2 \Rightarrow$ By eisensie criterion

$f(x+1)$ is not reducible

$\Rightarrow f(x)$ is not reducible

5. π is prime element in $\mathbb{Z}[i]$

(i) as π is prime in $\mathbb{Z}[i]$

$\pi = a+ib \quad \pi\bar{\pi} = a^2+b^2 \in \pi \cap \mathbb{Z}$

$\pi \cap \mathbb{Z}$ is prime in $\mathbb{Z}$

or

$\pi \cap \mathbb{Z} = p\mathbb{Z}$

for some p prime in $\mathbb{Z}$

now, as $\pi \cap \mathbb{Z} = p\mathbb{Z}$

$\Rightarrow p = \pi\pi'$

for some π'

$\Rightarrow (p) \subseteq (\pi)$

$\Rightarrow \mathbb{Z}[i]/(\pi) \hookrightarrow \mathbb{Z}[i]/(p)$

$\Rightarrow \left|\mathbb{Z}[i]/(\pi)\right| \leq \left|\mathbb{Z}[i]/(p)\right|$

now, $\left|\mathbb{Z}[i]/(p)\right| = p^2$ as

$\mathbb{Z}[i] = a+ib$

then $\mathbb{Z}[i]/(p) = \bar{a}+i\bar{b}$

where $\bar{a} = 0,1 \dots p-1$

$\bar{b} = 0,1 \dots p-1$

$\Rightarrow \left|\mathbb{Z}[i]/(\pi)\right| = 1, p$ or p^2

$\left|\mathbb{Z}[i]/(\pi)\right| \neq 1$ as if 1 then $(\pi) = \mathbb{Z}[i]$ $\times$

so $\left|\mathbb{Z}[i]/(\pi)\right| = p$ or p^2

(b) If $\left|\mathbb{Z}[i]/(\pi)\right| = p^2$ then

$\left|\mathbb{Z}[i]/(\pi)\right| = \left|\mathbb{Z}[i]/(p)\right|$

or $\mathbb{Z}[i]/(\pi) \cong \mathbb{Z}[i]/(p)$

$\Rightarrow (p) = (\pi)$

$\Rightarrow p$ is prime in $\mathbb{Z}[i]$

$\Rightarrow p \in \mathbb{Z}[i]$

$N(p) = p^2 = a^2+b^2$

$\hookrightarrow$ prime as $a^2+b^2 = 0,1,2 \bmod 4$

$p^2 = 0,1,2 \bmod 4$

$\Rightarrow \; p^2 \equiv 1 \bmod 4$

$\Rightarrow \; p \equiv 3 \bmod 4$

Sample Quiz-3:

1. $\mathbb{Q}_2 = \left\{ \frac{r}{s} \,\middle|\, r, s \in \mathbb{Z},\ 2 \nmid s \right\}$

To prove: $\mathbb{Q}_2$ is local

proof: $2\mathbb{Q}_2$ is ideal (trivial)

$2\mathbb{Q}_2$ is maximal as

$$2\mathbb{Q}_2 = \left\{ \frac{r}{s} \,\middle|\, 2 \mid r,\ 2 \nmid s \right\}$$

then

if $2\mathbb{Q}_2$ is not maximal

then

$$2\mathbb{Q}_2 \subsetneq \underset{\text{some ideal}}{\underset{\uparrow}{I}} \subseteq \mathbb{Q}_2$$

then

let $\alpha \in I \setminus 2\mathbb{Q}_2$

then

α is s.t $\alpha = \frac{a}{b}$ where $2 \nmid a$, $2 \nmid b$

as $2 \nmid a$ let $\beta = \frac{b}{a} \in \mathbb{Q}_2$

then

$\alpha \cdot \beta = 1 \in I$

or $I = \mathbb{Q}_2$

$\therefore$ $2\mathbb{Q}_2$ is maximal

if $I \subsetneq \mathbb{Q}_2$ is maximal then $I = 2\mathbb{Q}_2$ as

if $I \subsetneq \mathbb{Q}_2$

as

I is maximal

$1 \notin I$

but $\alpha \in \mathbb{Q}_2 \setminus I$ then

$I + \alpha\mathbb{Q}_2 = \mathbb{Q}_2$

now

as $1 \notin I$

if $\alpha / \beta \in I$

then $\beta / \alpha \notin I$

or

$2 \mid \alpha$

so

$\alpha / \beta \in I$ of form

s.t $2\mathbb{Q}_2 \subseteq I$

$\Rightarrow 2\mathbb{Q}_2 = I$

as $2\mathbb{Q}_2$ is maximal

$\therefore$ $2\mathbb{Q}_2$ is unique, maximal ideal

2. R is noeth, S is m.c

To prove: $S^{-1}R$ is noeth

proof: As $I = (I \cap R) S^{-1}R$

for $I \cap R \leq R$

$I \cap R$ is f.g of R

$\Rightarrow I$ is f.g for $S^{-1}R$

$\therefore$ for every ideal $S \trianglelefteq R$, it is f.g $\Rightarrow$ $S \trianglelefteq R$ is noeth.

3. M is noeth-R-module
   N is R-submodule of M

as $N \leq M$, M is noeth $\Rightarrow$ N is noeth

now for E s.t
$E \leq M/N$
$\exists$ $K \leq M$ s.t
$K \geq N$ and $E = K/N$
as M is noeth,
K is f g $\Rightarrow$ E is f.g R-module
$\Rightarrow$ M/N is Noeth

4. (R, m) is noeth local ring. M, N are f.g R-modules

$f : M \to N$ is R-linear

$\tilde{f} : M/mM \to N/mN$ is surjective

To prove : f is surjective

proof : as $\tilde{f} : M/mM \to N/mN$ is surjective

$\tilde{f}(M/mM) = N/mN$

$r + mM \longmapsto f(r) + mN$

we have

$$\frac{f(M) + mN}{mN} = \frac{N}{mN}$$

$\Rightarrow$ $f(M) + mN = N$

$\Rightarrow$ $f(M) = N$ (Nakayama lemma)

$\Rightarrow$ f is onto

sample answer:

1. G is finite, P, Q are p sylow subgroups of G.

To prove: $\exists g$ s.t $gPg^{-1} = Q$

I will prove first: $K \leq G$, $p \mid |K|$, $G = p^r m$, $H \in \text{sylow}_p(G)$
$\exists g \in G$ s.t $gHg^{-1} \cap K$ is $\text{sylow}_p(K)$

Proof: $S = G/H$
$|S| = m$
let G act on S by
$G \times S \to S$
$g(aH) \mapsto gaH$

then $O_{aH} = \{ gaH \mid gaH = aH \}$
$= S$

also $\text{stab}(H) = \{ g \in G \mid g.H = H \}$
$= H$

$\text{stab}(aH) = \{ g \in G \mid gaH = aH \}$

$\forall g \in \text{stab}(aH)$
$gaH = aH$
$\Leftrightarrow ga = ah$ for some h
$\Leftrightarrow ga \in aH$
$\Leftrightarrow g \in aHa^{-1}$

$\therefore \text{stab}(aH) = aHa^{-1}$
& $\text{orbit}(aH) = S$ $\quad |S| = m$ as $p \nmid m$
$\Rightarrow p \nmid |O_{aH}|$
$\Rightarrow p \nmid |G/\text{stab}(aH)|$

now for the subgroup K $(p \mid |K|)$
$L = \text{stab}_K(aH) = aHa^{-1} \cap K$
$O(aH) = \{ kaH \mid kaH = aH \}$
$= S$ as $kaH \in S$ and $e \in K$

$\therefore |O(aH)| = |K/L| = |K/gHg^{-1} \cap K|$

now $|O(aH)| = m$

$m = |K/gHg^{-1} \cap K|$
as $p \mid |K|$
we have $p \mid |gHg^{-1} \cap K|$
and so if $|K| = p^s m$
then $|gHg^{-1} \cap K| = p^s$

$\therefore \quad gHg^{-1} \cap K$ is sylow p(K)

now putting $K = G$ we get

$$gHg^{-1} \cap G = gHg^{-1} = \text{sylow } p(G)$$

2. $H = \mathbb{Z}/p^3\mathbb{Z}$

then $|H| = p^3$

now $\text{Aut}(H) = \left(\mathbb{Z}/p^3\mathbb{Z}\right)^\times$

as H is cyclic

and also $\text{ord}(\mathbb{Z}/p^3\mathbb{Z})^\times = p^2(p-1)$

so $p \mid |\text{Aut}(H)|$

so $\exists\, x \in \text{Aut}(\mathbb{Z}/p^3\mathbb{Z})^\times$

s.t

$\text{ord}(x) = p$

now, let $K = \mathbb{Z}/p\mathbb{Z}$ then

$$\psi : K \longrightarrow \text{Aut}(\mathbb{Z}/p^3\mathbb{Z})^\times$$

$$\bar{i} \longmapsto x^i$$

ψ is non-trivial homomorphism (trivial)

$\therefore$ $G = H \rtimes K$ is s.t

$H \trianglelefteq G$ but $K \not\trianglelefteq G$

so G is not abelian

and $|G| = p^4$