SOLUTIONS TO MIDSEM EXAM MA ①

(1) (a).

GIVEN : $K \trianglelefteq G$, $H < G$.

TST: $HK < G$ & $K \trianglelefteq HK$.

PROOF: Let $h_1 k_1, h_2 k_2 \in HK$.

Then. $(h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$

Now let $k_1 k_2^{-1} = k_3 \in K$.

Since $K \trianglelefteq G$. $K h_2^{-1} = h_2^{-1} K$.

$\Rightarrow k_3 h_2^{-1} = h_2^{-1} k_3'$ for some $k_3' \in K$.

$\Rightarrow (h_1 k_1)(h_2 k_2)^{-1} = h_1 h_2^{-1} k_3' \in HK$

Since $H < G \Rightarrow h_1 h_2^{-1} \in H$ & $k_3' \in K$.

$\therefore HK = \{hk \mid h \in H \ k \in K\} < G$. ②

Moreover for $e \in H$. $e.k \in HK \ \forall k \in K$

$\Rightarrow K \subseteq HK. \Rightarrow K < HK$. ①

Since $K \trianglelefteq G$, for any $hk \in HK \subseteq G$

$hk K (hk)^{-1} \subseteq K$.

①

$\Rightarrow K \trianglelefteq HK$.

1(b). $K \trianglelefteq HK \Rightarrow HK/K$ is a group. (2)

(4)

Define $\psi : H \longrightarrow HK/K$.

as $\psi(h) = h e K$.

ψ is well defined as $h_1 = h_2 \Rightarrow h_1 \cdot e = h_2 \cdot e$

$\Rightarrow h_1 \cdot eK = h_2 \cdot eK$.

$\Rightarrow \psi(h_1) = \psi(h_2)$

Claim ψ is a onto group homomorphism.

For any $h_1, h_2 \in H$ $\quad \psi(h_1 h_2) = (h_1 h_2) \cdot e K$

$= (h_1 \cdot e)(h_2 \cdot e) K$

$= h_1 \cdot eK \; h_2 \cdot eK$

(Since $K \trianglelefteq HK$)

$= \psi(h_1) \, \psi(h_2)$.

Moreover, for any $hk \in HK$ $\quad hkK$

$= hK$ as $k \in K$

$= \psi(h)$.

$\Rightarrow$. ψ is onto.

$$\text{Ker}\,\psi = \{h \in H \,/\, \psi(h) = e\}$$
$$= \{h \in H \,/\, \psi(h) = K \text{ i.e } hK = K\}$$
$$= \{h \in H \,/\, h \in K\} = K \cap H.$$

By 1^{st} iso thm

$$H/\text{Ker}\,\psi \cong \psi(H) = HK/K.$$

$$\Rightarrow H/H \cap K \cong HK/K. \quad \square$$

1(c) Define $\phi : k\mathbb{Z} \to \mathbb{Z}_{\ell/k}$.

5

$$\phi(x) = [x]_d \in \mathbb{Z}_{\ell/k = d}$$

where $[\,]_d$ denotes equiv class of x in $\mathbb{Z}_d$

Denote $\ell/k = d$ then we are given

$(k, d) = 1$.

For any $x, y \in k\mathbb{Z}$ $\quad x = y \Rightarrow [x]_d = [y]_d$

$\Rightarrow \phi(x) = \phi(y)$

$\therefore \phi$ is well defined.

<u>Claim</u>: ϕ is a onto group homomorphism

<u>Proof</u>:

Let. $x, y \in k\mathbb{Z}$ then

$$\phi(x+y) = [x+y]_d = [x]_d + [y]_d \quad \text{by defn.}$$

$$= \phi(x) + \phi(y).$$

Let $w \in \mathbb{Z}_d$.

Now. $(k, d) = 1 \Rightarrow$ For some $a, b \in \mathbb{Z}$

$$ak + bd = 1$$

$$\Rightarrow \quad wak + wbd = w$$

$$\Rightarrow \quad wak = w \mod (d)$$

$$\Rightarrow \quad [w]_d = [kwa]_d = \phi(kwa).$$

where $kwa \in k\mathbb{Z}$.

$\therefore$ ϕ is onto.

~~Ema~~ By 1^{st} iso $k\mathbb{Z}/\ker\phi \cong \phi(k\mathbb{Z}) = \mathbb{Z}_d$

$\ker\phi = \{ka \in k\mathbb{Z} \mid [ka]_d = 0\}$

ie. $= \{ka \in k\mathbb{Z} \mid d \mid ka\}$

$= \{ka \in k\mathbb{Z} \mid d \mid a.\}$ since $(k,d)=1$

$= \{ka \in k\mathbb{Z} \mid a = d.b,\ b \in \mathbb{Z}\}$

$= \{kdb \mid b \in \mathbb{Z}\} = \{lb \mid b \in \mathbb{Z}\}$

$= l\mathbb{Z}$

$\therefore\ k\mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}_d = \mathbb{Z}_{l/k}$.

1(d). (3) $m\mathbb{Z}/n\mathbb{Z}/n\mathbb{Z}$ here. the group structure is additive

$m\mathbb{Z}+n\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z}$

$m\mathbb{Z} \cap n\mathbb{Z} = \{a \in \mathbb{Z} \mid \cancel{m/k}\ \&\ n/k\}$

$= \{a \in \mathbb{Z} \mid lcm(m,n) \mid k\}$

$= lcm(m,n)\mathbb{Z}$

$m\mathbb{Z}+n\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/lcm(m,n)\mathbb{Z} \cong \mathbb{Z}_{\frac{lcm(m,n)}{m}}$ (by part c)

$\cong \mathbb{Z}_{\frac{n}{gcd(m,n)}}$ as $mn = lcm \cdot gcd$.

Altemately $\dfrac{m\mathbb{Z}+n\mathbb{Z}}{n\mathbb{Z}} \cong \gcd(m,n)\mathbb{Z}/n\mathbb{Z}$

$\cong \mathbb{Z}_{n/\gcd(m,n)}$

Q2: (a) 4 Let $x, y \in G$. Since every element of G has order 2, every element is a self inverse.

$\Rightarrow \quad x = x^{-1} \quad y = y^{-1}$

& $(xy) = (xy)^{-1} = y^{-1}x^{-1} = yx$.
$\forall\, x,y \in G$.

$\therefore$ G is abelian

(b). Let $x \in G$ For any $h \in H$

$x h x^{-1} = xh(x x^{-1}).x^{-1} = xhxh\, h^{-1}(x^{-1})^{2}$

$= (xh)^{2} h^{-1} x^{-2}$

But $xh, x^{-1} \in G \Rightarrow (xh)^{2}, x^{-2} \in H$

& $h^{-1} \in H$

$\Rightarrow xhx^{-1} \in H \Rightarrow xHx^{-1} \subseteq H$
$\forall x$

3 $\therefore H \trianglelefteq G$.

$\therefore$ G/H is a group.

$x \in G \Rightarrow x^2 \in H \Rightarrow x^2 H = H \quad \forall x \in G$

1. ie $(xH)^2 = H \quad \forall x \in G$

$\therefore$ Every element of G/H has order 2

$\Rightarrow G/H$ is abelian by 2(a).

3(a). 5

Let G be a group order pq and $Z(G) \neq \{e\}$

Then. $\exists\, e \neq a \in Z(G)$. if $o(a) = pq$ then G is cyclic. else $o(a) / pq \Rightarrow$

$o(a) = p$ or q.

In either case $H = \langle a \rangle \trianglelefteq G$. since $a \in Z(G)$ & $o(G/H.)$ is prime and hence cyclic

$\Rightarrow G$ is abelian.

$\therefore$ G has an element x of order p & element y of order q.

$H = \langle x \rangle$, $K = \langle y \rangle$, clearly $H, K \trianglelefteq G$ as G is ab.

$(xy)^{pq} = x^{pq} y^{pq} = e.$ since G is abelian. (8)

$(xy)^p = x^p y^p = y^p \neq e.$

& since $o(y) = q$ $o(y^p) = q$.

~~case~~. Similarly $(xy)^q = x^q \neq e$

$\therefore$ $o(xy) = pq$ & G is cyclic as it has an element of order(G).

3(b). Since G is non-abelian it is not cyclic.

Let $a \in G$ then $o(a) / 6 \Rightarrow o(a) = 1, 2, 3$ or 6

$o(a) \neq 6$ since G is not cyclic

$\Rightarrow o(a) = 2$ or 3 if $a \neq e$.

Now ~~&~~ since G has even order.

By pair every element with its inverse we see that $\exists$ at least one element with self inverse.

~~&~~ $A = \{\{x, x^{-1}\} / x \in G, x \neq x^{-1}\}$

Then if $|G| = |A| + \{e\}$. $\Rightarrow$ G is odd.

$\therefore$ $\exists$ $y \in G$ s.t $y \notin A$.

$\therefore$ G has an element of order 2. 2

If all elements have order 2 then G is abelian from 2(a). $\therefore$ G has an element of order 3. $\square$. 2

3 (c) 5 From 3(b) G has an element a of order 2 & b of order 3.

let $H = \langle b \rangle$ then $[G : H] = 2$

$\Rightarrow H \trianglelefteq G$.

Now $a \notin H$ as $o(a) \nmid 3$.

$\Rightarrow aH \neq H \Rightarrow G = aH \cup H$

$= \{ e, b, b^2, a, ab, ab^2 \}$

Further $H \trianglelefteq G \Rightarrow aH = Ha$.

$ab = a$. not possible as $a \neq e$.

$\Rightarrow ab = ba$.

or $ab = b^2 a$.

if $ab = ba$

then $a^i b^j a^k b^l = a^k b^l a^i b^j \quad \forall k, l, i, j$

$\Rightarrow G$ is abelian.

$\therefore$ $ab \neq ba$. $\Rightarrow$ $ab = b^2a$.

$\therefore G = \{e, b, b^2, a, ab, ab^2 \mid ab = b^2a\}$.

3(d). Then. If $o(G) = 6 = 2 \times 3$ ~~we know~~ if G has a nontrivial

2

by 3(a) G is cyclic $\Rightarrow$ $G \cong \mathbb{Z}_6$,

If $Z(G) = e$ then G is nonabelian and

by 3(c) $G \cong \{e, b, b^2, a, ab, ab^2 \mid ab = b^2a\}$

But $o(S_3) = 6$ & S_3 is nonabelian

$\therefore$ $S_3 \xrightarrow{\psi} G$.

$\psi(123) = b$

$\psi(12) = a$. gives an iso.

$\therefore$ $G \cong S_3$ or $\mathbb{Z}_6$. $\square$.

4(a) False.

4

$(\mathbb{Q}^*, \times)$ is an infinite group

and. $\{+1, -1\} < \mathbb{Q}^* : \times$

as $(-1)^2 = 1$.

$\therefore$ Infinite grps can have finite subgrps.

4(b). True. $\mathbb{Z}$ is cyclic & generated by

4 1. Every grp hom is determined by the image of 1.

Let $G = \{a_1, \dots, a_8\}$

Then define $\varphi_{a_i} : \mathbb{Z} \to G$

as $\varphi_{a_i}(k) = a_i^k$.

then this well defn

& $\varphi_{a_i}(k+l) = a_i^{k+l} = a_i^k \cdot a_i^l = \varphi_{a_i}(k) \cdot \varphi_{a_i}(l)$

Further $\varphi_{a_i}(1) = a_i \neq a_j = \varphi_{a_j}(1)$

if $i \neq j$

$\Rightarrow$ we have 8 distinct grp homomorphisms

4(c) False

4 Let $(\mathbb{Q}, +)$ be cyclic. Then $\exists\, a \in \mathbb{Q}$

s.t $\mathbb{Q} = \langle a \rangle$. $a = \cancel{\frac{p}{q}}\ \frac{m}{n}$ where $(m,n) = 1$.

~~$a \in \mathbb{Q} \Rightarrow a$~~

Let. p be a prime s.t $(p, m) = 1$

Then. $\frac{m}{np} \in \mathbb{Q} \Rightarrow \frac{m}{np} = ka$. for some $k \in \mathbb{Z}$

$\Rightarrow k = \frac{1}{p}$.

But $\frac{1}{p} \notin \mathbb{Z}$.

$\therefore (\mathbb{Q}, +)$ is not cyclic

4(d). FALSE.

4 ~~Delote~~ Note $Aut\, \mathbb{Z} = \{\pm 1\} \cong \mathbb{Z}_2$ where $+1$ is id & -1 is $k \to -k$.

$$Aut\, \mathbb{Z}_3 \cong \mathbb{Z}_3^{*} \cong \mathbb{Z}_2.$$

$Aut\, \mathbb{Z} \cong Aut\, \mathbb{Z}_3$ but $\mathbb{Z} \not\cong \mathbb{Z}_3$.

4(e). TRUE. If $\exists$ an action of $\mathbb{Z}_5$ on

4 $\{a, b, c\}$ then we have a grp hom. $\psi : \mathbb{Z}_5 \to S_{\{a,b,c\}} \cong S_3$

Then any $e \neq a \in \mathbb{Z}_5$. $O(a) = 5 \Rightarrow$ ~~$\psi(a)$~~ $O(\psi(a)) \mid 5$. But this $\Rightarrow$ $O(\psi(a)) = 1$ as no element of S_3 has order 5.

$\Rightarrow \psi$ is trivial.