Indeed, I'd suppose the following material has been covered up to now.

- Subgroups and their associated theorems
- Cyclic groups.
- Cosets and Lagrange theorem and its consequences.
- Normal subgroups and quotient groups ...

After the quiz, we will solve four problems.

1. An instructive theorem: $HK = KH \Leftrightarrow HK$ is a subgrp of G.
2. If G is a group in which $(a.b)^i = a^i b^i$ for three consecutive integers i and $\forall a, b \in G$, G is abelian.
3. Counter example to problem 4 of set (I).
4. Any subgrp of a cyclic grp is itself a cyclic grp.

Thm ①: $\Longrightarrow$ Let's check group axioms.

#1, Associative. ✓

#2, neutral element $\longrightarrow$ since $e \in H$, $e \in H \longrightarrow ee = e \in HK$

#3 Closed?

$$\left.\begin{aligned} \alpha &= hk \in HK \\ \beta &= h'k' \in HK \end{aligned}\right\} \quad \alpha\beta = hk\,h'k' = h(kh')k'$$

since $KH = HK \Rightarrow kh' = \bar{h}\bar{k}$ for some $\begin{cases} \bar{h} \in H \\ \bar{k} \in K \end{cases}$

$\alpha\beta = h(\bar{h}\bar{k})k' = (h\bar{h})(\bar{k}k') \in HK$ (closed ▨)

#4 inverse.

$\alpha^{-1} = k^{-1}h^{-1} \in KH$ since $KH = HK$

$k^{-1}h^{-1} = \tilde{h}\tilde{k}$ for $\begin{cases} \tilde{k} \in K \\ \tilde{h} \in H \end{cases} \Rightarrow \alpha^{-1} = \tilde{h}\tilde{k} \in HK$ ▨

$\Leftarrow$

For all $h \in H, k \in K \xrightarrow{inv} h^{-1} \in H, k^{-1} \in K \Rightarrow h^{-1}k^{-1} \in HK$

since HK itself is a grp $\Rightarrow (h^{-1}k^{-1})^{-1} = kh \in HK$

$\Rightarrow KH \subset HK \ldots (*)$

Consider any element $x \in HK$ since HK is a subgrp

so $x^{-1} \in HK$, so $x^{-1} = \tilde{h}\tilde{k}$.

$\Rightarrow x = (x^{-1})^{-1} = \tilde{k}^{-1}\tilde{h}^{-1} \in KH$.

Therefore, $(x \in HK \Rightarrow x \in KH) \Rightarrow HK \subset KH$ $(**)$

$(*), (**) \rightarrow HK = KH$.

② suppose it holds for $\{i, i+1, i+2\}$.

$$\underline{\underline{a}}(a^i \cdot b)\underline{b^i} = a^{i+1} \cdot b^{i+1}$$

$\Vert$ assumption

$$(a \cdot b)^{i+1} = (a \cdot b)(a \cdot b)^i$$
$$= \underline{\underline{a}} \cdot (b \cdot a)^i \underline{b^i}$$

Cancellation gives $a^i b = b a^i$

just take $i \to i+1$ and it gives $a^{i+1} b = b a^{i+1}$

Now, $a \cdot (a^i \cdot b) = a(b \cdot a^i) = (a \cdot b)(a^i)$

$$a^{i+1} \cdot b = b \cdot a^{i+1} = (b \cdot a)(a^i)$$

cancellation law

$\longrightarrow$ $ab = ba$ ☒

If

(i) $\exists e \in G : a \cdot e = a$ for all $a \in G$.

(ii) $\forall a \in G \; \exists y(a) \in G : y(a) \cdot a = e$.

(Right identity, left inverse) doesn't constitute a group

This (Right identity + left inverse) doesn't constitute a g...

Let G be a arbitrary set with more than two elements.

$\circ : G \times G \longrightarrow G$

$\forall a, b \in G \quad a \circ b = a$

① closed ✓

② $\begin{cases} a \circ (b \cdot c) = a \circ b = a \\ (a \circ b) \circ c = a \circ c = a \end{cases} \longrightarrow$ Associative

③ choose an arbitrary element $e \in G \rightarrow$

$\forall a \in G \quad a \cdot e = a \rightarrow$ (i) holds.

④ Given $a \in G$, take the left inverse $y(a) = e$ (the chosen element):

$y(a) \circ a = e \circ a = e \rightarrow$ (ii) holds.

But clearly $(G, \circ)$ doesn't constitute a group!

We expect that inverses in G to be two sided.

but $a \circ y(a) = a \circ e = a \neq e$ (!)

Similarly, neutral element isn't two-sided:

$e \cdot a = e \neq a$!

So (i), (ii) are not good manifestation of group axioms!

$G = \langle g \rangle$

Let i be the smallest integer such that $g^i \in H$.

For any $g^j \in H$, divide j by i = $j = ai + b$

with $0 \leq b < i$.

$$g^j = g^{ai+b} \longrightarrow g^b = g^j g^{-ai} = \underbrace{g^j}_{\in H} \underbrace{(g^i)}_{\in H}{}^{-a} \in H$$

But i was the smallest one!

$\Rightarrow b = 0 \Rightarrow g^j = (g^i)^a \longrightarrow H = \langle g^i \rangle$

Bonus (For someone OTB):

$H \subset G$, $a \in G$

show that $aHa^{-1} = \{aha^{-1} \mid h \in G\} \subset G$

i) $e \in aHa^{-1}$, since $e \in H \Rightarrow aea^{-1} = e \in aHa^{-1}$

ii) Associativity inherits.

iii) closed $x, y \in aHa^{-1} \longrightarrow \begin{cases} x = ah_1a^{-1} \\ y = ah_2a^{-1} \end{cases}$

so $xy = (ah_1 a^{-1})(ah_2 a^{-1}) = a\underbrace{h_1 h_2}_{\in H} a^{-1} \in aHa^{-1}$

(iv) Inverse : $\underset{aHa^{-1}}{\underset{\cap}{x}} = ah_1 a^{-1} \rightarrow x^{-1} = (a^{-1})^{-1} h_1^{-1} a^{-1}$

$= ah_1^{-1} a^{-1} \in aHa^{-1}$ ⊠

what's the order of aHa^{-1}?

Take $f: H \rightarrow aHa^{-1}$ $\quad f(h) = aha^{-1}$

Injective : $f(h_1) = f(h_2) \Longrightarrow h_1 = h_2$

$\Downarrow$

$ah_1 a^{-1} = a h_2 a^{-1} \longrightarrow$ multiply by $a^{-1}, a \longrightarrow$

$h_1 = h_2$ ⊠

surjective : Take an element $a\tilde{h}a^{-1} \in aHa^{-1}$,

by definition of aHa^{-1}, $\tilde{h} \in H$

so f maps $\tilde{h}$ to $f(\tilde{h}) = a\tilde{h}a^{-1}$, ⊠

$\Longrightarrow O(H) = O(aHa^{-1})$ ✓