Homework: Add 2.5 #64. Add 2.6 #67, 68, 76

Let $H = \{(1), (13)\} \le S_3$. Is $H \lhd S_3$? No.

Two reasons: (1) $(123)(13)(132) = (12) \neq H$.

(2) Since (23) has same cycle structure and $(23) \notin H$, then not all conjugates of (12) are in H.

Example $H = \{1, -1\}$. $Q_8/H = \{H, iH, jH, kH\}$.
$Q_8/H \cong$ either Klein 4 or a cyclic group.

In the Klein 4 group, all elements have order 2.
$(iH)^2 = i^2H = -1H = H$.
$(jH)^2 = (kH)^2 = H$.

Definition The *center* of a group, $Z(G) = \{a \in G \mid ag = ga\ \forall\ g \in G\}$.

Example If G is Abelian, then $Z(G) = G$.

Example Let $n \ge 3$. Then $Z(S_n) = \{(1)\}$.

Proposition $Z(G) \lhd G$.

Proof:

First show $Z(G) \le G$. You do this as an exercise.

We know $e \in G$ and $eg = ge\ \forall\ g \in G$. $\therefore$ $e \in Z(G)$, so $Z(G) \neq \emptyset$.

Let $a, b, c \in Z(G)$. Then $abc = acb = cab$.

$\therefore$ $ab \in$ Z(G); and we have closure.

And since $ab = ba$, then $a = abb^{-1} = bab^{-1}$. Hence $b^{-1}a = b^{-1}bab^{-1} = ab^{-1}$, which gives us that $b^{-1} \in Z(G)$; and we have inverses.

$\therefore$ $Z(G) \le G$.

Show all conjugates are in $Z(G)$.

Let $z \in Z(G)$, $g \in G$. Then $gzg^{-1} = zgg^{-1} = ze = z \in Z(G)$.

Other way: $gzg^{-1}a = agzg^{-1}$, so $gzg^{-1} \in Z(G)$.

$\therefore$ $Z(G) \lhd G$.

Homomorphism: Preserves group structure.
Isomorphism: Is 1-1.
Automorphism: $G \to G$.

Definition An *automophism* of a group, G, is an isomorphism $f: G \to G$.

Example Prove $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.
Proof: Define $\phi: \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$ by
$\phi([1], [1]) = [1]$,
$\phi([0], [1]) = [4]$,
$\phi([0], [0]) = [0]$,
$\phi([1], [0]) = [3]$,
$\phi([0], [2]) = [2]$,
$\phi([1], [2]) = [5]$. (Just take powers of $([1], [1])$ to determine all others.)

Example $\mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_8$? No.
$[1] \in \mathbb{Z}_8$ has order 8. But no element in $\mathbb{Z}_2 \times \mathbb{Z}_4$ has order 8.

Definition: Every conjugation $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is called an *inner automorphism*.

Proposition Let $a \in G$. Prove ϕ_a is an automorphism.

Proof:
We first show ϕ_a is a homomorphism.
If $x, y \in G$, then $\phi_a(x)\, \phi_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \phi_a(xy)$.
$\therefore$ ϕ_a is a homomorphism.
We next show ϕ_a is injective.
Let $g, h \in G$ such that $\phi_a(g) = \phi_a(h)$. Then $aga^{-1} = aha^{-1}$.
So, by cancellation, $g = h$.
Hence ϕ_a is injective.
And, finally we show ϕ_a is surjective. Let $z \in G$.
Since $a^{-1}za \in G$ and $\phi_a(a^{-1}za) = a(a^{-1}za)a^{-1} = z$, then ϕ_a is surjective.

Definition Aut $(G) = \{\phi \mid \phi$ is an automorphism on $G\}$.

Proposition (1) Aut (G) is a group with respect to composition, $\langle \text{Aut}\,(G), \circ \rangle$.

Proof:
$\forall f \in$ Aut (G), $i \circ f = f \circ i$, where $i: G \to G$ is defined by $i(g) = g$, $\forall\, g \in G$.
$\therefore$ i, the identity map is the identity for Aut (G).
$\forall f \in$ Aut (G), $f^{-1} \circ f = f \circ f^{-1} = i$ (since f is a bijection).
$\therefore$ f^{-1} is the inverse of f.
$\forall f, g \in$ Aut (G),
$f \circ g \in$ Aut (G) (since f, g each are bijections from G to G).
$\therefore$ We have closure.

Definition Inn $(G) = \{\phi_a \mid a \in G\}$.

Proposition (2) Inn $(G) \lhd$ Aut (G).

Proof:

We first show Inn $(G) \leq$ Aut (G).

Since $\forall\, x \in G$, $\phi_e = exe^{-1} = x$, then $\phi_e = i$, the identity of Aut (G) and $\phi_e \in$ Inn (G), hence Inn $(G) \neq \varnothing$. Let $\phi_a, \phi_b \in$ Inn (G) where $a, b \in G$.

Since $b, b^{-1}, x \in G$, then $b^{-1}xb \in G$ and $\phi_b(b^{-1}xb) = bb^{-1}xbb^{-1} = x$.

Thus, $\phi_b^{-1}(x) = b^{-1}xb$.

$$\text{So } \forall\, x \in G,\ \phi_a\,\phi_b^{-1}(x) = \phi_a\,(b^{-1}xb) = a(b^{-1}xb)a^{-1} = (ab^{-1})\,x(ba^{-1}) = (ab^{-1})\,x(ab^{-1})^{-1} = \phi_{ab^{-1}}\,(x).$$

And $\phi_{ab^{-1}}\,(x) \in$ Inn (G) (since $ab^{-1} \in G$). $\therefore$ Inn$(G) \leq$ Aut(G).

We next show Inn $(G) \lhd$ Aut (G).

Let $a, g \in G$, $\phi_a \in$ Inn (G), $\psi \in$ Aut(G).

$$\text{Then}\quad \psi\phi_a(\psi^{-1}(\mathrm{g})) = \psi(a\psi^{-1}(g)a^{-1}) = \psi(a)\psi\psi^{-1}(g)\psi(a^{-1}) = \psi(a)g\psi(a^{-1}) = bgb^{-1},\ b = \psi(a) = \phi_b(g).$$

$\therefore$ $\psi\phi_a\psi^{-1} \in$ Inn (G). $\therefore$ Inn $(G) \lhd$ Aut (G).

Proposition (3) $\psi : G \to$ Aut (G) defined by $\psi(g) = \phi_g$ is a homomorphism. Moreover, ker $\psi = Z(G)$ and im $\psi =$ Inn (G).

Proof:

We first show ψ is a homomorphism.

Let $a, b \in G$.

$$\text{Then}\quad \forall\, x \in G,\ \phi_a\phi_b(x) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x).$$

$\therefore$ $\psi(a)\psi(b) = \phi_a\phi_b = \phi_{ab} = \psi(ab)$.

We know im $\psi =$ Inn (G) by definition.

We next show ker $\psi = Z(G)$.

$$z \in \ker\psi \Leftrightarrow \psi(z) = i, \text{ the identity map} \Leftrightarrow \phi_z = i \Leftrightarrow \phi_z(g) = i(g),\ \forall\, g \in G \Leftrightarrow zgz^{-1} = g\ \forall\, g \in G \Leftrightarrow zg = gz,\ \forall\, g \in G \Leftrightarrow z \in Z(G).$$

Recall: If G and G' are groups such that $\phi: G \to G'$ is a homomorphism, then $\ker \phi \lhd G$.

Definition The natural homomorphism is the map $\pi : G \to G/K$ where $K \lhd G$ and $\pi(g) = gK$.

Proposition $\pi : G \to G/K$ where $K \lhd G$ and $\pi(g) = gK$ is a homomorphism.

Proof:

Let $g, h \in G$. Then $\pi(g)\pi(h) = gKhK = ghK = \pi(gh)$ (since $K \lhd G$).

$\therefore$ π is a homomorphism.

Proposition $\ker \pi = K$.

Proof:

$\pi(f) = fK \Leftrightarrow f \in K$, so $\ker \pi = K$.

In more detail: Let $f \in \ker \pi$. Then $f \in \{g \in G \mid gK = K\}$. $\therefore$ $\ker \pi \subseteq K$.

Let $k \in K$. Then $k \in \{g \in G \mid gK = K\}$. $\therefore$ $K \subseteq \ker \pi$.

Kernels and normal subgroups are the same.

Theorem First Isomorphism Theorem (on Handout)

If $\phi : G \to G'$ is a homomorphism with $K = \ker \phi$, then $\phi(G) \cong G/K$.

Proof: See handout.

Example (1) $GL_n(\mathbb{R}) / SL_n(\mathbb{R}) \cong \mathbb{R}^*$

Define $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$ by $\phi(A) = \det A$.

$\ker f = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = SL_n(\mathbb{R})$

Example (2) $G_1 \times G_2 / \{e\} \times G_2 \cong G_1$

Define $\phi: G_1 \times G_2 \to G_1$ by $\phi((a, b)) = a$.

$\ker f = \{(a, b) \in G_1 \times G_2 \mid a = e\} = \{e\} \times G_2$.

Example (3) $G / Z(G) \cong \text{Inn}(G)$

Define $f : G \to \text{Inn}(G)$ by $f(g) = \phi_g$.

$$\begin{aligned} \ker f &= \{g \in G \mid gxg^{-1} = x, \forall x \in G\} \\ &= \{g \in G \mid gx = gx, \forall x \in G\} \\ &= Z(G). \end{aligned}$$

Example (4) $\mathbb{C}^+/S^1 \cong \langle \mathbb{R}^+, \bullet \rangle$

Define $f : \mathbb{C}^+ \to \langle \mathbb{R}^+, \bullet \rangle$ by $f(z) = |z|$.

$\ker f = \{z \in \mathbb{C}^+ \mid |z| = 1\} = S^1$.

Example (5) $\mathbb{R}/\mathbb{Z} \cong S^1$

Define $f : \mathbb{R} \to S^1$ by $f(r) = e^{2\pi ir}$.

$\ker f = \{r \in \mathbb{R} \mid e^{2\pi ir} = 1\} = \mathbb{Z}$.

Theorem If gcd $(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Proof:

Define $\phi: \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $\phi(a) = ([a]_m, [a]_n)$

We first show that ϕ is a homomorphism.

$\phi(h) + \phi(k) = ([h]_m, [k]_n) + ([k]_m, [k]_n) = ([h + k]_m, [h + k]_n) = \phi(h + k)$.

$\therefore$ ϕ is a homomorphism.

Note $\mathbb{Z}/\langle mn\rangle = \mathbb{Z}_{mn}$.

We now show $\langle mn\rangle = \ker\phi$ by showing containment in both directions.

Let $w \in \langle mn\rangle$. Then $w = mnp$ for some integer p.

$\therefore$ $\phi(w) = ([mnp]_m, [mnp]_n) = ([0]_m, [0]_n)$.

$\therefore$ $w \in \{x \in \mathbb{Z} \mid \phi(x) = ([0]_m, [0]_n)\} = \ker\phi$.

$\therefore$ $\langle mn\rangle \subseteq \ker\phi$.

For the reverse containment, let $z \in \ker\phi$. Then $\phi(z) = ([0]_m, [0]_n)$.

$\therefore$ $m \mid z$ and $n \mid z$. Since $(m, n) = 1$, then $mn \mid z$. $\therefore$ z is a multiple of mn.

So $z \in \langle mn\rangle$. Hence $\langle mn\rangle \supseteq \ker\phi$.

And we have $\langle mn\rangle = \ker\phi$.

So far, we have $\mathbb{Z}/\langle mn\rangle \cong \operatorname{im}\phi$.

We still need to show $\operatorname{im}\phi$ is all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

We will use order of groups to show $\operatorname{im}\phi = \mathbb{Z}_m \times \mathbb{Z}_n$.

Number of elements of $\mathbb{Z}/\langle mn\rangle = \mathbb{Z}_{mn}$ is mn.

Number of elements of $\operatorname{im}\phi$ is mn.

Number of elements of $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn.

$\therefore \operatorname{im}\phi = \mathbb{Z}_m \times \mathbb{Z}_n$.

$\therefore \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.