# HW 7 Due: 28 May 2025

As always, your answer will be graded on the quality of presentation as well as the correct answer. To get a good score: write your answer neatly, use complete sentences, and *justify your work.*

## Computations

1. For any group $G$ and element $g \in G$, define the homomorphism

$$\begin{aligned} e_{G,g} &: \mathbb{Z} \to G \\ n &\mapsto g^n. \end{aligned}$$

(No need to prove that $e_{G,g}$ is a homomorphism.) Let's write $e_{G,g}(\mathbb{Z}) = \{e_{G,g}(n) \mid n \in \mathbb{Z}\}$. Enumerate elements of $e_{G,g}(\mathbb{Z})$ and find $\ker(e_{G,g})$ in the following situations:

(a) $G = D_4, g = R$,

(b) $G = \mathbb{Z}_{20}, g = 15$,

(c) $G = D_4, g = F$.

(d) $G = S_9, g = \mathrm{id}_{\{1,2,3,4,5,6,7,8,9\}}$.

*Solution.* (a) $e_G, g(\mathbb{Z}) = \{I, R, R^2, R^3\}$, $\ker(e_G, g) = 4\mathbb{Z}$,

(b) $e_G, g(\mathbb{Z}) = \{0, 5, 10, 15\}$, $\ker(e_G, g) = 4\mathbb{Z}$,

(c) $e_G, g(\mathbb{Z}) = \{I, F\}$, $\ker(e_G, g) = 2\mathbb{Z}$, and

(d) $e_G, g(\mathbb{Z}) = \{\mathrm{id}_{\{1,2,3,4,5,6,7,8,9\}}\}$, $\ker(e_G, g) = \mathbb{Z}$.

□

2. If $G$ is a subgroup with a subgroup $H$, let's write $G/H$ for the set $\{Hg \mid g \in G\}$. Recall that $G/H$ is a partition of $G$.

(a) Enumerate all elements of $4\mathbb{Z}/8\mathbb{Z}$.

(b) Enumerate all elements of $D_5/\langle R\rangle$.

*Solution.* (a) $4\mathbb{Z}/8\mathbb{Z} = \{4\mathbb{Z}+0, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}$.

(b) $D_5/\langle R\rangle = \{D_5 I, D_5 F\}$.

□

## Proofs

(I) Suppose that $G, H$ are groups and $\psi: G \to H$ is a homomorphism.

(a) Let's write $\psi(G) = \{\psi(g) \mid g \in G\}$. Prove that $\psi(G)$ is a subgroup of $H$.

(b) For $J$ a subgroup of $H$, let's write $\psi^{-1}(J) = \{g \in G \mid \psi(g) \in J\}$. Prove that $\psi^{-1}(J)$ is a subgroup of $G$.

*Proof.* Let's write $e_G, e_H$ for the identities of $G, H$, respectively.

(a) We must show three things.

- From class we know that $\psi(e_G) = e_H$, so that $e_H \in \psi(G)$ and $\psi(G) \neq \varnothing$.
- Suppose that $h_1, h_2 \in \psi(G)$. Then there are $g_1, g_2 \in G$ with $\psi(g_1) = h_1$ and $\psi(g_2) = h_2$. Since $\psi$ is a homomorphism, we know that $h_1 h_2 = \psi(g_1)\psi(g_2) = \psi(g_1 g_2) \in \psi(G)$.
- Finally, choose any $h \in \psi(G)$, so there is some $g \in G$ with $\psi(g) = h$. From class, we know that $h^{-1} = (\psi(g))^{-1} = \psi(g^{-1}) \in \psi(G)$.

(b) We must show three things.

- From class we know that $\psi(e_G) = e_H \in J$, so that $e_G \in \psi^{-1}(J)$ and $\psi^{-1}(J) \neq \varnothing$.
- Suppose that $g_1, g_2 \in \psi^{-1}(J)$. Since $\psi$ is a homomorphism and $J$ is a subgroup, we know that $\psi(g_1 g_2) = \psi(g_1)\psi(g_2) \in J$, so that $g_1 g_2 \in \psi^{-1}(J)$.
- Finally, choose any $g \in \psi^{-1}(J)$. From class, and since $J$ is a subgroup, we know that $\psi\left(g^{-1}\right) = (\psi(g))^{-1} \in J$, so that $g^{-1} \in \psi^{-1}(J)$.

□

(II) Suppose that $G$ is a commutative group, and let $n$ be a positive integer. Define

$$\begin{aligned} \phi\colon G &\to G \\ g &\mapsto g^n. \end{aligned}$$

(a) Prove that $\phi$ is a homomorphism of groups.

(b) Prove that $\ker(\phi) = \{g \in G \mid \operatorname{ord}(g) \text{ is a divisor of } n\}$.

(c) Suppose that $G$ is finite. Suppose further that $|G|$ and $n$ have no common factors greater than 1. Prove that $\phi$ is an isomorphism.

*Proof.* Let's write $e$ for the identity of $G$.

(a) Choose any $g, h \in G$, and note that

$$\begin{aligned} \phi(gh) &= (gh)^n \\ &= g^n h^h && \text{(since } G \text{ is commutative)} \\ &= \phi(g)\phi(h), \end{aligned}$$

so we see that $\phi$ is a homomorphism.

(b) We must show two inclusions.

- Suppose that $g \in \ker(\phi)$, so that $g^n = \phi(g) = e$. By fact from class, we know that $\operatorname{ord}(g)$ is a divisor of $n$.
- Now suppose that $g \in G$ and $\operatorname{ord}(g)$ is a divisor of $n$: let's say there's some $m \in \mathbb{Z}_{>0}$ with $n = \operatorname{ord}(g) \cdot m$. Then $\phi(g) = g^n = \left(g^{\operatorname{ord}(g)}\right)^m = e^m = e$, so $g \in \ker(\phi)$.

(c) Since $G$ is finite, we need only show that $\phi$ is injective to deduce that it is bijective; the result will then follow from part (a). Well, from class we know we can show $\phi$ is injective by showing $\ker(\phi) = \{e\}$; to this end, suppose that $g \in \ker(\phi)$. Then $g^n = \phi(g) = e$, so that $\operatorname{ord}(g)$ is a divisor of $n$. But by Lagrange's theorem, we know that $\operatorname{ord}(g)$ is *also* a divisor of $|G|$. By hypothesis, we see that $\operatorname{ord}(g) = 1$; that is, we see that $g = e$, as desired.

□

(III) Suppose that $G_1, G_2$ are groups, and define

$$\begin{aligned} \phi\colon G_1 \times G_2 &\to G_2 \\ (g_1, g_2) &\mapsto g_2. \end{aligned}$$

(a) Prove that $\phi$ is a homomorphism of groups.

(b) Prove that $\ker(\phi)$ is isomorphic to $G_1$.

*Proof.* (a) Choose any $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$ and note that

$$\phi((g_1, g_2)(h_1, h_2)) = \phi(g_1 h_1, g_2 h_2) = g_2 h_2 = \phi(g_1, g_2)\phi(g_1, g_2).$$

(b) Let's write $e_1, e_2$ for the identities of $G_1, G_2$, respectively. I claim that for any $g_1 \in G_1$, the element $(g_1, e_2)$ is in $\ker(\phi)$; indeed, note that $\phi(g_1, e_2) = e_2$ by the definition of $\phi$. Thus, we may define

$$\begin{aligned} \psi\colon G_1 &\to \ker(\phi) \\ g_1 &\mapsto (g_1, e_2). \end{aligned}$$

- To see that $\psi$ is a homomorphism, choose any $g_1, h_1 \in G_1$ and note that

$$\psi(g_1 h_1) = (g_1 h_1, e_2) = (g_1, e_2)(h_1, e_2) = \psi(g_1)\psi(h_1).$$

- To see that $\psi$ is injective, choose any $g_1 \in \ker(\psi)$. Then $(e_1, e_2) = \psi(g_1) = (g_1, e_2)$, so we see $g_1 = e_1$. By fact from class, this means that $\psi$ is injective.
- Finally, to see that $\psi$ is surjective, choose any $(g_1, g_2) \in \ker(\phi)$. This means that $e_2 = \phi(g_1, g_2) = g_2$, so that

$$\psi(g_1) = (g_1, e_2) = (g_1, g_2).$$

□