Final Solutions

1. State whether the following statements are true or false. Please justify your answers.

   (a) A group cannot be isomorphic to any of its proper subgroups.

   (b) If every proper subgroup of a group is cyclic, then the group is abelian.

   Solution. (a) This statement is **false.** The additive group of integers $\mathbb{Z}$ is isomorphic to each of its proper subgroups of the form $k\mathbb{Z}$, for $k \geq 2$. It can be easily verified that the map

   $$\mathbb{Z} \to k\mathbb{Z} : x \mapsto kx, \forall x \in \mathbb{Z}$$

   is an isomorphism.

   (b) This statement is **false**. A counterexample to the statement is the nonabelian group $D_6 = S_3$. We know that a proper subgroups of D_6 is either of order 2 or 3. Thus, every proper subgroup of D_6 is cyclic.

2. Given a group G, let $S = \{aba^{-1}b^{-1} : a, b \in G\}$. We define the subgroup

   $$[G, G] := \langle S \rangle$$

   to be the *commutator subgroup or the derived group* of G.

   (a) Show that $[G, G] \lhd G$.

   (b) If $N \lhd G$, then show that G/N is abelian if and only if $[G, G] < N$.

   Solution. (a) Let $H = [G, G]$, and denote the product $aba^{-1}b^{-1}$ by $[a, b]$. First, we observe that for $g \in G$, we have

   $$g[a,b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}].$$

   Moreover, given $h \in H$, we have $h = \prod_{i=1}^{k}[a_i, b_i]$, where $a_i, b_i \in G$. Thus, for any $g \in G$, we have

   $$ghg^{-1} = \prod_{i=1}^{k}[ga_ig^{-1}, gb_ig^{-1}] \in H,$$

   from which it follows that $H \lhd G$.

   (b) This follows from the following arguments.

   $$\begin{array}{rcll} G \text{ is abelian} & \iff & aNbN = bNaN, \forall a, b \in G & \text{(By definition of abelian property.)} \\ & \iff & abN = baN, \forall a, b \in G & \text{(By definition of product in } G/N.) \\ & \iff & (ab)(ba)^{-1} = [a,b] \in N, \forall a, b \in G & \text{(By 2.2 (ii) of Lesson Plan.)} \\ & \iff & [G, G] < N, & \text{(By definition of the derived group.)} \end{array}$$

   and the assertion follows.

3. Given groups G, H, consider the set

   $$\mathrm{Hom}(G, H) = \{\varphi : G \to H : \varphi \text{ is a homomorphism.}\}$$

   (a) When H is abelian, show that $\mathrm{Hom}(G, H)$ forms an abelian group.

   (b) Show that $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$ and for $n \geq 2$, show that $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z})$ is trivial.

(c) For $m, n \geq 2$, show that $\text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_d$, where $d = \gcd(m, n)$.

Solution. (a) Without loss of generality, let us denote the operation on H by $+$ and the identity on H by 0. Given arbitrary $\varphi_1, \varphi_2 \in \text{Hom}(G, H)$, consider the natural binary operation $\cdot$ on $\text{Hom}(G, H)$ defined by

$$(\varphi_1 \cdot \varphi_2)(g) = \varphi_1(g) + \varphi_2(g), \; \forall g \in G.$$

Under the operation $\cdot$, $\text{Hom}(G, H)$ forms an abelian group with the trivial homomorphism $\varphi_0 : G \to H$ (i.e., $\varphi_0(g) = 0$, $\forall g \in G$) as the identity. The inverse of each $\varphi \in \text{Hom}(G, H)$ is the map $-\varphi : G \to H$ defined by $(-\varphi)(g) = -\varphi(g)$, for all $g \in G$. The detailed verification of all group axioms is left as an exercise.

(b) We know from the discussions in class that given $\varphi \in \text{Hom}(G, H)$ and $g \in G$ with $o(g) < \infty$, we have $o(\varphi(g)) \mid o(g)$. Thus, since the order of each nontrivial element in $\mathbb{Z}$ is infinite, we can infer that $\text{Hom}(\mathbb{Z}_n, \mathbb{Z})$ is trivial.

Now, given a $\varphi \in \text{Hom}(\mathbb{Z}, \mathbb{Z})$, if $\varphi(1) = k$ for some $k \in \mathbb{Z}$, then for each $z \in \mathbb{Z}$, we have

$$\varphi(z) = z\varphi(1) = zk.$$

So, any $\varphi \in \text{Hom}(\mathbb{Z}, \mathbb{Z})$ is uniquely determined by the value $\varphi(1)$. Therefore, we have $\text{Hom}(\mathbb{Z}, \mathbb{Z}) = \{\varphi_k : k \in \mathbb{Z}\}$, where $\varphi_k(1) = k \in \mathbb{Z}$. It is a straightforward exercise to verify that the map $\text{Hom}(\mathbb{Z}, \mathbb{Z}) \to \mathbb{Z} : \varphi_k \mapsto k$ is an isomorphism. (Verify this!)

(c) Let $[k]_\ell$ denote the residue class $\ell\mathbb{Z} + k$. Since $\mathbb{Z}_m = \langle [1]_m \rangle$, any homomorphism $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ is uniquely determined by $\varphi([1]_m)$. Again, we recall the fact that given $\varphi \in \text{Hom}(G, H)$ and $g \in G$ with $o(g) < \infty$, we have $o(\varphi(g)) \mid o(g)$. So, it follows that $o(\varphi([1])) \mid o([1]_m) = m$. Now let $\varphi_k \in \text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$ be such that $\varphi([1]_m) = [k]_n$. Consider the map

$$\Psi : \text{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_d : \varphi_k \overset{\Psi}{\mapsto} [k]_d.$$

Since $d \mid n$, $[k]_n = [k']_n \implies [k]_d = [k']_d$, it is a straightforward exercise to check that Ψ is a well-defined epimorphism. (Verify this!)

It remains to be shown that Ψ is injective. First, we observe that:

$$\begin{aligned} \varphi_k([m]_m) &= \varphi_k([0]_m) && (\text{Since } m \equiv 0 \pmod{m}.) \\ &= [0]_n && (\varphi_k \text{ is a homomorphism.}) \\ &= m\varphi_k([1]_m) && (\varphi_k \text{ is a homomorphism.}) \\ &= m[k]_n && (\text{By definition of } \varphi_k.) \end{aligned} \tag{*}$$

Thus, we have that $mk \equiv 0 \pmod{n}$, and so $mk = n\ell$, for some integer ℓ. Setting $m' = m/d$ and $n' = n/d$, (*) would imply that:

$$k(m'd) = \ell(n'd) \implies k = \ell n'/m'. \tag{**}$$

Since $\gcd(m', n') = 1$, we see that $m' \mid \ell$, and so it follows that

$$\ell \in \{m', 2m', \ldots, dm'\},$$

and by (**), we have

$$k \in \{n', 2n', \ldots, dn'\}.$$

Since there are exactly d distinct choices for k, we see that Ψ is injective.

4. Consider the map $\varphi : \mathrm{O}(2,\mathbb{R}) \to \mathrm{SO}(3,\mathbb{R})$ defined by

$$\varphi(A) = \begin{bmatrix} A & 0 \\ 0 & \det(A) \end{bmatrix},$$

for all $A \in \mathrm{O}(2,\mathbb{R})$.

(a) Show that φ is a monomorphism.

(b) Show that $\operatorname{Im}\varphi = \{A \in \mathrm{SO}(3,\mathbb{R}) : A(e_3) = \pm e_3\}$, where $e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

Solution. (a) φ is clearly well-defined since given matrices $A, B \in \mathrm{O}(2,\mathbb{R})$ such that $A = B$, we have

$$\varphi(A) = \begin{bmatrix} A & 0 \\ 0 & \det(A) \end{bmatrix} = \begin{bmatrix} B & 0 \\ 0 & \det(B) \end{bmatrix} = \varphi(B).$$

φ is a homomoprhism: Consider $\varphi(AB)$ for arbitrary $A, B \in \mathrm{O}(2,\mathbb{R})$. Then we have:

$$\begin{aligned}
\varphi(AB) &= \begin{bmatrix} AB & 0 \\ 0 & \det(AB) \end{bmatrix} && \text{(By definition of } \varphi.\text{)} \\
&= \begin{bmatrix} AB & 0 \\ 0 & \det(A)\det(B) \end{bmatrix} && \text{(det is a homomorphism.)} \\
&= \begin{bmatrix} A & 0 \\ 0 & \det(A) \end{bmatrix} \begin{bmatrix} B & 0 \\ 0 & \det(B) \end{bmatrix} && \text{(By properties of matrix product.)} \\
&= \varphi(A)\varphi(B) && \text{(By definition of } \varphi.\text{),}
\end{aligned}$$

which shows that φ is a homomorphism.

φ is injective: Let I_k be the $k \times k$ identity matrix. We have

$$\begin{aligned}
\ker \varphi &= \{A \in \mathrm{O}(2,\mathbb{R}) : \varphi(A) = I_3\} && \text{(By definition of } \ker \varphi.\text{)} \\
&= \{A \in \mathrm{O}(2,\mathbb{R}) : \varphi(A) = \begin{bmatrix} I_2 & 0 \\ 0 & 1 \end{bmatrix}\} && \text{(By definition of } I_3.\text{)} \\
&= \{A \in \mathrm{O}(2,\mathbb{R}) : A = I_2\} && \text{(By definition of } \varphi.\text{)} \\
&= \{I_2\},
\end{aligned}$$

which shows that φ is injective.

(b) We see that:

$$\begin{aligned}
\operatorname{Im}\varphi &= \{\varphi(A) : A \in \mathrm{O}(2,\mathbb{R})\} && \text{(By definition of Im.)} \\
&= \{\begin{bmatrix} A & 0 \\ 0 & \det(A) \end{bmatrix} : A \in \mathrm{O}(2,\mathbb{R})\} && \text{(By definition of } \varphi.\text{)} \\
&= \{\begin{bmatrix} A & 0 \\ 0 & \pm 1 \end{bmatrix} : A \in \mathrm{O}(2,\mathbb{R})\}. && \text{(Since } A \in \mathrm{O}(2,\mathbb{R}).\text{)}
\end{aligned} \tag{\dagger}$$

Now let $S = \{A \in \mathrm{O}(2, \mathbb{R}) : A(e_3) = \pm e_3\}$. By (†) it is apparent that given any $A \in \operatorname{Im}\varphi$, we have $A(e_3) = \pm e_3$. Thus, it follows that $\operatorname{Im}\varphi \subset S$.

Now consider any matrix $A \in S$. If $A(e_3) = e_3$, then since $A \in \mathrm{SO}(3, \mathbb{R})$, from the discussions in class, it follows A is a rotation about the vector e_3 (along the z-axis) by θ. Thus, A has form

$$A = \begin{bmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix}, \tag{\$}$$

which implies that $A \in \operatorname{Im}\varphi$. Suppose that $A(e_3) = -e_3$. Since $A \in \mathrm{SO}(3, \mathbb{R})$ represents a rotation about a vector on the unit sphere S^2 centered at origin in $\mathbb{R}^3$, A has to be the counterclockwise rotation about the vector $e_2 = (0, 1, 0)$ (along the y-axis) by π. Thus, $A(e_2) = e_2$, and furthermore, this rotation maps $e_1 = (1, 0, 0)$ (along the x-axis) to -e_1 (i.e, $A(e_1) = -e_1$). Finally, since A is also linear map, it is completely determined by where it maps the basis elements e_1, e_2, e_3, and so we have

$$A = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \in \operatorname{Im}\varphi.$$

5. **(Bonus.)** Show that $\mathrm{SO}(3, \mathbb{R})$ has no proper normal subgroups.

   Solution. Let $R(v, \theta)$ represent the counterclockwise rotation about a vector $v \in S^2$ by an angle θ. It is easy to see any two distinct points x, y (or vectors) in the unit sphere S^2 lie on a unique diameter $D_{x,y} \subset S^2$. Now $D_{x,y}$ cuts S^2 into two hemispheres. Let the vector representing the north pole northern hemisphere be denoted by $V_{x,y}$. Now consider the rotation $R(V_{x,y}, \theta_{x,y})$, where $\theta_{x,y}$ is shorter distance in radians between x and y along the circle $D_{x,y}$. Then it is easy to visualize that

   $$R(V_{x,y}, \theta_{x,y}) \circ R_{x,\theta} \circ R(V_{x,y}, \theta_{x,y})^{-1} = R_{x,\theta}.$$

   (Here we are assuming without loss of generality that $R(V_{x,y}, \theta_{x,y})(x) = y$.) In other words, the rotation by a fixed angle about any two distinct vectors in S^2 are conjugate. Therefore, any subgroup H of $\mathrm{SO}(3, \mathbb{R})$ has to contain rotations about all possible points in S^2, and the assertion follows.