

MAT 4233 — Problem Set 3

Due Tuesday 27 October 2026, at the start of the Q&A session.

This set covers the five meetings of 6 October through 22 October: cosets, Lagrange's theorem and the index (Li-Zhao §3.1), homomorphisms, their kernels and images (§3.3), normal subgroups and quotient groups (§3.4, two meetings), and the first isomorphism theorem and groups of small order (§3.4). Rings now begin on 29 October, so the problem on them has moved to Problem Set 4.

Maximum six pages. Each problem is scored on *completeness* alone, not on correctness: **2** for a nominally complete solution, **1** for a clearly partial one, **0** for nothing submitted or for filler with no substance. Any submission containing non-human-readable content, stray characters, or unproofread AI output scores 0 for that item.

Sources. AI assistance, solution keys, collaboration and the internet are all permitted, without restriction. Include one line naming what you used. Note that at the Q&A session we name the problem you are to explain; you do not choose, so be ready on every problem on this set.

Notation. We follow Li-Zhao: $(G : H)$ is the index of H in G , $\text{ord}(g)$ the order of an element g , and $U(R)$ the group of units of a ring R with unity. $\mathbb{Z}_n$ is the integers modulo n , written $[a]$ or simply a , and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the direct product. D_n is the group of symmetries of a regular n -gon, with $|D_n| = 2n$, generated by a rotation r of order n and a reflection s , with $sr s^{-1} = r^{-1}$. We compose permutations right to left, as functions: $(\sigma\tau)(x) := \sigma(\tau(x))$.

Problem 1 (Cosets, Order-Index, and Lagrange's theorem)

1. Let $H = \langle s \rangle = \{e, s\}$ in D_4 . List every left coset gH and every right coset Hg . Find all $g \in D_4$ for which $gH \neq Hg$.
 2. Let G be a finite group and $g \in G$. Using Lagrange's theorem or Order-Index, prove that $\text{ord}(g)$ divides $|G|$, and deduce that $g^{|G|} = e$. Apply this to the group $U(\mathbb{Z}_p)$, for p prime, to prove *Fermat's little theorem*: if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
 3. Let H and K be subgroups of a group G with $|H| = 12$ and $|K| = 35$. Prove that $H \cap K = \{e\}$.
-

Problem 2 (Homomorphisms)

Let $\varphi: G \rightarrow G'$ be a group homomorphism, and let e, e' be the identities of G, G' .

1. Prove that $\varphi(e) = e'$, that $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$, that $\ker \varphi$ is a subgroup of G , and that φ is injective if and only if $\ker \varphi = \{e\}$.
 2. Show that the rule $[a]_{12} \mapsto [a]_4$ gives a well-defined homomorphism $\mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$, and find its kernel and its image. Then show that the rule $[a]_{12} \mapsto [a]_5$ does *not* define a function $\mathbb{Z}_{12} \rightarrow \mathbb{Z}_5$ at all.
 3. Prove that if $g \in G$ has finite order, then $\text{ord}(\varphi(g))$ divides $\text{ord}(g)$. Deduce that the only homomorphism $\mathbb{Z}_5 \rightarrow S_3$ is the trivial one, $x \mapsto e$.
-

Problem 3 (Normal subgroups and quotient groups)

Recall that $H \leq G$ is *normal*, $H \trianglelefteq G$, if $gH = Hg$ for every $g \in G$.

1. Prove that $H \trianglelefteq G$ if and only if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
 2. In S_3 , show that $\langle (1\ 2\ 3) \rangle$ is a normal subgroup, and that $\langle (1\ 2) \rangle$ is not, by exhibiting a g with $g\langle (1\ 2) \rangle \neq \langle (1\ 2) \rangle g$.
 3. Let $N = \langle r^2 \rangle = \{e, r^2\}$ in D_4 .
 - a. Show that $N \trianglelefteq D_4$.
 - b. List the four cosets that make up D_4/N .
 - c. Show that the square of every element of D_4/N is the identity coset, and conclude that $D_4/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ rather than $\mathbb{Z}_4$.
-

Problem 4 (The first isomorphism theorem; groups of order 4)

1. Let $n \geq 1$, and let $\varphi: \mathbb{C}^* \rightarrow \mathbb{C}^*$ be $\varphi(z) := z^n$, where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers. Show that φ is a surjective homomorphism, and that its kernel is the group μ_n of n -th roots of unity. Conclude, naming the theorem, that $\mathbb{C}^*/\mu_n \cong \mathbb{C}^*$: a group can be isomorphic to one of its own proper quotients.
 2. Prove that every group of order 4 is isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and that these two are not isomorphic to each other. (*Use Lagrange's theorem to list the possible orders of elements. You may quote that a group in which $a^2 = e$ for every a is abelian.*)
 3. Decide which of the two groups of part 2 each of $U(\mathbb{Z}_8)$ and $U(\mathbb{Z}_{10})$ is isomorphic to.
-