MAT 5173 — Problem Set 1

Due Wednesday 9 September 2026, at the start of the Q&A session.

This set covers Segment A in its entirety — the five meetings of 19 August through 2 September, that is, Ash Ch. 1: groups and subgroups (§1.1), permutation groups (§1.2), cosets, normal subgroups and homomorphisms (§1.3), the isomorphism theorems (§1.4), and direct products (§1.5). (Li–Zhao §1.3–1.5, §2.1 and §3.1–3.4 carry the same material at a gentler pace, should you want a second exposition.)

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 (Ash prints them at the back), 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 all six.

Notation. We follow Ash throughout. In particular $|a|$ denotes the order of the element a and $|G|$ the order of the group; $H \leq G$ means H is a subgroup and $H \trianglelefteq G$ that it is normal; $[G : H]$ is the index; U_n is the group of units modulo n, of order $\varphi(n)$; and D_{2n} is the dihedral group of order $2n$, i.e. the symmetry group of the regular n-gon. (The subscript in D_{2n} is the order of the group, not the number of vertices —Ash's convention, and the opposite of the one used in MAT 4233. We shall not mix the two.)

Problem 1 (order of group elements) — §1.1

Let G be a group and let $a \in G$ have finite order n.

1. Prove that $a^k = 1$ if and only if $n \mid k$. (This is the fact that makes every later computation with orders possible; prove it from the division algorithm, not by citing it.)
2. Prove that
$$|a^k| = \frac{n}{\gcd(n,k)} \qquad \text{for every } k \in \mathbb{Z}$$
3. Deduce that a cyclic group of order n has exactly $\varphi(n)$ generators (Euler's function φ). Deduce further that, if p is prime then every element of a group of order p is a generator; hence any a group of order $|G| = p$ (a prime) is cyclic.

Problem 2 (permutations, and the dihedral relations) — §1.2

1. Let $\sigma = (1,3,5)(2,4)(6,7) \in S_7$. Compute σ^{-1}; also, the orders of σ and σ^{-1}, and determine if each σ is even or odd.
2. Prove that the order of an arbitrary permutation is the least common multiple of the lengths of the cycles in its disjoint cycle decomposition.
3. Let the dihedral group $D_{2n} = \langle R, F \rangle$ be presented by generators R, F subject to
$$R^n = I, \qquad F^2 = I, \qquad RF = FR^{-1}.$$

Prove that $FR^i = R^{-i}F$ for all $i \in \mathbb{Z}$; deduce that every $D_{2n} = \{R^i 0 \le i < n\} \cup \{R^i F : 0 \le i < n\}$ with $0 \le i < n$, and that all $2n$ such elements are distinct. Finally, show that $(R^i F)^2 = I$ for every i (all such elements $R^i F$ are an *involutions*.)

Problem 3 (counting with cosets) — §1.3

1. Prove that if $[G : H] = 2$ then $H \trianglelefteq G$.
2. Let H and K be finite subgroups of a group G, and put $HK := \{hk : h \in H,\ k \in K\}$. ($HK$ is a subset of G which need *not* be a sugbroup.) Prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

3. Use Lagrange's "Order-Index" Theorem to prove *Euler's Theorem*: *If* $\gcd(a, n) = 1$ *and* $n \ge 2$, *then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Problem 4 (using the the isomorphism theorems) — §1.4

Each part asks for an application; in each, name the theorem you invoke and identify the homomorphism, its kernel and its image explicitly.

1. Let $\mathrm{GL}(n, \mathbb{R})$ be the multiplicative group of invertible $n \times n$ real matrices and $\mathrm{SL}(n, \mathbb{R})$ the subset (subgroup) of those of determinant 1. Prove that $\mathrm{SL}(n, \mathbb{R}) \trianglelefteq \mathrm{GL}(n, \mathbb{R})$ and

$$\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R}) \;\cong\; \mathbb{R}^*$$

(the multiplicative group of nonzero reals).

2. Let m and n be positive integers ($n \ge 2$) such that $m \mid n$. Identify the subgroup $m\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$. Next, prove that

$$(\mathbb{Z}/n\mathbb{Z})\big/(m\mathbb{Z}/n\mathbb{Z}) \;\cong\; \mathbb{Z}/m\mathbb{Z}.$$

Prove this twice: once directly, by exhibiting a homomorphism and applying the first isomorphism theorem, and a second time as immediate corollary of the third. (The second proof should be one sentence. That is the point of the third theorem.)

Problem 5 (direct products & counterexamples) — §1.5

1. Let C_m and C_n be cyclic of orders m and n. Prove that $C_m \times C_n$ is cyclic if and only if $\gcd(m, n) = 1$. (Both directions are about the order of an element of the product; Problem 1 does most of the work.)
2. Prove that S_3 is *not* the internal direct product of two proper nontrivial subgroups. Do so by listing every subgroup of S_3, deciding which are normal, and then showing that no admissible pair of orders survives. Conclude that a group of order 6 need not decompose, even though $6 = 2 \cdot 3$ with 2 and 3 coprime; compare part 1 and say precisely where the hypothesis of part 1 fails here.

3. Prove that the set Aff(2) consisting of all affine maps $f_{A,b}$ of the form

$$\mathbb{R}^2 \to \mathbb{R}^2 : x \mapsto f_{A,b}(x) := Ax + b$$

for some invertible $A \in \mathbb{R}^{2\times 2}$ and translation $v \in \mathbb{R}^2$ is a group under composition. Show that Aff(2) has two subgroups:

- L consisting of linear maps $x \mapsto Ax$,
- T consisting of translations $x \mapsto x + b$,

which, taken together, generate Aff. Is Aff(2) the internal direct product of the groups L and T?