MAT 4233 — Problem Set 2

Due Tuesday 29 September 2026, at the start of the Q&A session.

This set covers the five meetings of 10 September through 24 September: subgroups and the subgroup criterion (Li–Zhao §1.4), cyclic groups, the order of an element, and primitive roots (§1.5), generating sets and the defining relations of D_n (§1.6), permutation groups, cycle notation, and Cayley's theorem (§2.1), and the alternating group, the sign of a permutation, and the rotation group of the tetrahedron (§2.2).

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 all five.

Notation. C_n denotes the cyclic group of order n, and D_n 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 of order 2. S_n is the symmetric group on $\{1, \dots, n\}$, and $A_n \leq S_n$ its alternating subgroup. We compose permutations right to left, as functions: $(\sigma\tau)(x) := \sigma(\tau(x))$. $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ denotes the sign of σ.

Problem 1 (Subgroups)

1. State and prove the *one-step subgroup criterion*: a nonempty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for all $a, b \in H$.
2. Find all subgroups of $\mathbb{Z}_{12}$ (under addition), and give a generator for each.
3. Besides the trivial subgroup and D_4 itself, find every subgroup of D_4 of order 2 and of order 4. (*You should find five of the first kind and three of the second.*)

Problem 2 (Cyclic groups, order, and primitive roots)

1. Let g have order n in a group G, and let k be a positive integer. Prove that g^k has order $n/\gcd(n,k)$. Find a condition for g^k to generate the same subgroup as g. Deduce that a cyclic group of order n has $\varphi(n)$ generators, where φ is Euler's totient.
2. Using part 1, find the order of every element of $\mathbb{Z}_{12}$ (under addition); list all elements of order 12 (i.e., generators).
3. The group $U_{11} = (\mathbb{Z}_{11})^\times$ of units (invertible elements) modulo 11, under multiplication, has order 10.
   a. Compute the powers $2^1, 2^2, \dots, 2^{10}$ modulo 11; deduce that 2 generates $(\mathbb{Z}_{11})^\times$ —i.e., that 2 is a so-called *primitive root* modulo 11.
   b. Using part 1 (with $g = 2$), find every element of $(\mathbb{Z}_{11})^\times$ having order 5, and every primitive root modulo 11.

Problem 3 (Generating sets and the relations of D_n)

Realize D_n as symmetries of the plane: let r be rotation by $2\pi/n$ about the origin, and s reflection across the x-axis.

1. Using the rotation and reflection matrices for r and s, compute the matrix product srs^{-1} and show $srs^{-1} = r^{-1}$.
2. The three relations $r^n = e$, $s^2 = e$, $srs^{-1} = r^{-1}$ let you rewrite sr as $r^{-1}s$ — that is, moving an s past an r inverts the r. Using only this, show that *every* product of r's, s's, and their inverses can be rewritten in the form $r^i s^j$ with $0 \le i < n$ and $j \in \{0, 1\}$. (This is why D_n has at most $2n$ elements — and, since it plainly has n rotations and n reflections, exactly $2n$.)
3. Show that s and sr already generate all of D_n — that is, $\langle s, sr \rangle = D_n$ — even though neither one alone is a rotation.

Problem 4 (Permutation groups and Cayley's theorem)

Let $\sigma = (1\,3\,5)(2\,4)$ and $\tau = (1\,2)(3\,4\,5)$ in S_5.

1. Compute $\sigma\tau$ and $\tau\sigma$ in cycle notation, and confirm $\sigma\tau \ne \tau\sigma$.
2. State the order of a permutation in terms of its cycle type, and use it to find the orders of σ, τ, and $\sigma\tau$.
3. *(Cayley's theorem, concretely.)* For $g \in \mathbb{Z}_4$, let $L_g \colon \mathbb{Z}_4 \to \mathbb{Z}_4$ be left multiplication (i.e., addition) by g: $L_g(x) = x + g$.
   a. Write each of L_0, L_1, L_2, L_3 as a permutation of $\{0, 1, 2, 3\}$, in cycle notation.
   b. Verify directly that $L_{g+h} = L_g \circ L_h$ for all $g, h \in \mathbb{Z}_4$, and conclude that $g \mapsto L_g$ is an injective homomorphism $\mathbb{Z}_4 \to S_4$ — i.e., an isomorphism from $\mathbb{Z}_4$ onto its image.

Problem 5 (The alternating group and the tetrahedron)

1. Give the sign of a k-cycle in terms of k, and use it to compute $\mathrm{sgn}(\sigma)$, $\mathrm{sgn}(\tau)$, and $\mathrm{sgn}(\sigma\tau)$ for σ, τ of Problem 4. Check that your three answers are consistent with sgn being multiplicative.
2. Taking as given that every permutation has a well-defined parity (as a product of transpositions), prove that $\mathrm{sgn} \colon S_n \to \{\pm 1\}$ is a homomorphism.
3. Label the four vertices of a regular tetrahedron $1, 2, 3, 4$.
   a. Using the index of A_4 in S_4, find $|A_4|$.
   b. A rotation of the tetrahedron by $120°$ about the axis through vertex 1 and the center of the opposite face permutes $\{2, 3, 4\}$ cyclically and fixes 1. Write this permutation in cycle notation and check it lies in A_4.

c. A rotation by $180°$ about the axis through the midpoints of the (opposite) edges 12 and 34 swaps $1 \leftrightarrow 2$ and $3 \leftrightarrow 4$ simultaneously. Write this permutation in cycle notation and check it lies in A_4.

d. (No proof required.) Together with the identity, rotations of these two kinds account for all 12 rotational symmetries of the tetrahedron — so the rotation group of the tetrahedron *is* A_4, realized as permutations of its vertices.