Math 103A **Midterm 2** **Winter 2020**

Your Name

PID

- Do not open this exam until you are told to begin. You will have 50 minutes for the exam.
- Check that you have a complete exam. There are 4 questions for a total of 26 points.
- Each question should take up roughly 12 minutes of your time. Do not spend too much time on each question.
- You are allowed to have one single sided, handwritten note sheet.
- Cheating will result in a zero and be reported to the University.
- **Show all of your work**. You should prove your answers: for example, if a problem asks "Is ..... a group?" a yes or no answer is not enough; you must justify why it is true. If you use a main result from class, be sure to clearly state the result.
- If you need more space to answer a question, continue on the back of the page, and indicate that you have done so.
- GOOD LUCK!

Question	Points	Score
1	5	
2	6	
3	7	
4	8	
Total:	26	

1. (a) (1 point) Let A be a set. Give the definition of a permutation of A.

Solution: A permutation of A is an onto and one-to-one function $\sigma : A \to A$.

(b) (2 points) Let $A = \mathbb{Z}$. Is the function $\phi : A \to A$ given by $\phi(n) = 5n$ a permutation of A?

Solution: This is not a permutation because it is not onto. If $m = 1$, there is no solution to the equation $\phi(n) = m$, because that says $5n = 1$, so $n = 1/5 \notin \mathbb{Z}$.

(c) (2 points) Let $A = \mathbb{Z}_6$. Is the function $\phi : A \to A$ given by $\phi(n) = 5n \mod 6$ a permutation of A?

Solution: This is a permutation. We will write out the values of $\phi(n)$.

$$\phi(0) = 0$$
$$\phi(1) = 5$$
$$\phi(2) = 4$$
$$\phi(3) = 3$$
$$\phi(4) = 2$$
$$\phi(5) = 1$$

This shows that ϕ is one-to-one and onto because it uniquely matches the elements of the domain with the codomain.

As an alternative, you can say that this is a permutation because ϕ^{-1} exists: the function $\phi^{-1}(n) = 5n$ satisfies $\phi(\phi^{-1}(n)) = n$ and $\phi^{-1}(\phi(n)) = n$ (because $25 = 1 \mod 6$).

2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix}$ be permutations in S_6.

   (a) (2 points) Write σ and τ in cycle notation.

   Solution:

   $$\sigma = (123)(46)$$
   $$\tau = (15)(24)$$

   (b) (2 points) Determine if σ and/or τ is an element of A_6.

   Solution: Because $\sigma = (123)(46) = (13)(12)(46)$ is a product of an odd number of transpositions, σ is not in A_6.
   Because $\tau = (15)(24)$ is a product of an even number of transpositions, τ is in A_6.

   (c) (2 points) Compute $\sigma\tau$ and find the order of $\sigma\tau$.

   Solution: We compute $\sigma\tau = (152643)$ and because it is a cycle of length 6, the order of $\sigma\tau$ is 6.

3. (a) (1 point) If H is a subgroup of a group G, give the definition of a left coset of H.

Solution: If H is a subgroup of a group G, a left coset of H is a subset of the form $\{ah \mid h \in H\}$ for some element $a \in G$.
Alternatively, an acceptable answer is: if H is a subgroup of a group G, the left coset of H containing an element $a \in G$ is the subset $aH = \{ah \mid h \in H\}$.

(b) (3 points) Let $M_n = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. In class, we showed that $(M_n, \cdot_n)$ is a group, where $\cdot_n$ is multiplication modulo n. Prove that

$$H = \{a \in M_n \mid a \cdot_n a = 1\}$$

is a subgroup of M_n.

Solution: We check the three conditions for this to be a subgroup.

- If $a \in H$ and $b \in H$, then $a \cdot_n a = 1$ and $b \cdot_n b = 1$, so $(a \cdot_n b) \cdot_n (a \cdot_n b) = (a \cdot_n a) \cdot_n (b \cdot_n b) = 1 \cdot_n 1 = 1$, so $a \cdot_n b$ is in H. Hence, H is closed under the binary operation.
- H contains the identity because $1 \cdot_n 1 = 1$.
- H contains inverses because each element in H is its own inverse: for any $a \in H$, $a \cdot_n a = 1$, so $a = a^{-1}$.

(c) (3 points) Determine all left cosets of H in M_7, where H is the subgroup from part (b).

Solution: We can write out the relevant groups. First, $M_7 = \{1, 2, 3, 4, 5, 6\}$ and, computing $a \cdot_7 a$ for each $a \in M_7$ (denoting $a \cdot_7 a$ by a^2 for simplicity), we get $1^2 = 1$, $2^2 = 4$, $3^3 = 2$, $4^2 = 2$, $5^2 = 4$, and $6^2 = 1$, so the $H = \{1, 6\}$. Then, the cosets of H are

$$\begin{aligned} H &= \{1, 6\} \\ 2H &= \{2, 5\} \\ 3H &= \{3, 4\}. \end{aligned}$$

4. (a) (1 point) State Lagrange's Theorem.

> **Solution:** Let G be a finite group and let H be a subgroup of G. Then, $|H|$ divides $|G|$.

(b) (3 points) Let G be a group of order pq, where p and q are prime numbers. Prove that every proper subgroup of G is cyclic.

> **Solution:** Let H be a proper subgroup of G. Because H is proper, $|H| < pq$, and by Lagrange's Theorem, $|H|$ divides pq, so because p and q are prime, we must have $|H| = 1, p$ or q. If $|H| = 1$, then $H = \{e\} = \langle e \rangle$ is cyclic. If $|H| = p$ or $|H| = q$, then H is a group with a prime number of elements. By the corollary to Lagrange's Theorem from class, this implies that H is cyclic.

(c) (4 points) If G is a finite abelian group with two elements x, y of order 2 and $x \neq y$, use Lagrange's Theorem to prove that $|G|$ is a multiple of 4. (Hint: find a subgroup of order 4.)

> **Solution:** We will show that $H = \{e, x, y, xy\}$ is a subgroup of G. It contains the identity, and because x and y have order 2, $x^2 = e$ and $y^2 = e$, so $x = x^{-1}$ and $y = y^{-1}$, so it contains the inverses of x, y, and e. Because G is abelian, $xy = yx$, and $(xy)^2 = (xy)(xy) = (xy)(yx) = xy^2x = xex = x^2 = e$, so xy also has order 2 and $(xy)^{-1} = xy$. Therefore, it also contains the inverse of xy.
>
> To finish showing that H is a subgroup, we must show that H is closed, meaning the product of two elements in H is again in H. This is clear if either element is e, and each non-identity element has order 2, so $x^2 = e$, $y^2 = e$, and $(xy)^2 = e$. It is also clear that $(x)(y) = (y)(x) = xy \in H$. So, we just need to check that $x(xy) = (xy)x$ and $y(xy) = (xy)y$ are in H, but $xxy = x^2y = y$, and $xy^2 = x$, so these are in H. Therefore, H is closed. Finally, because H is a subgroup of G with exactly 4 elements, Lagrange's Theorem implies that 4 divides $|G|$.