Midterm 2 Practice: Solutions

1. (a) 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) Let $A = \mathbb{Z}$. Which of the following are permutations of A?

i. The function $\sigma : A \to A$ given by $\sigma(n) = 3n - 2$

Solution. This is not a permutation because it is not onto. If $m = 0$, there is no value of n such that $\sigma(n) = 3n - 2 = 0$ has a solution, because $n = 2/3$ is not an integer.

ii. The function $\tau : A \to A$ given by $\tau(n) = |n|$

Solution. This is not a permutation because it is not one-to-one: $\tau(1) = \tau(-1) = 1$, but $1 \neq -1$.

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

(a) Write σ and τ in cycle notation.

Solution. $\sigma = (134562)$ and $\tau = (1243)(56)$.

(b) Determine if σ and τ are elements of A_6.

Solution. We can write $\sigma = (12)(16)(15)(14)(13)$, so σ is odd and thus not an element of A_6. We can write $\tau = (13)(14)(12)(56)$, so τ is even and therefore is an element of A_6.

(c) Find $\sigma\tau$ and $|\langle \sigma\tau \rangle|$.

Solution. Multiplying in cycle notation, we find that $\sigma\tau = (25)$ so $|\langle \sigma\tau \rangle| = 2$.

3. (a) Show that the set $H = \{\sigma \in S_5 \mid \sigma(5) = 5\}$ is a subgroup of S_5.

Solution. We check the three conditions.

- If $\sigma, \tau \in H$, then $\sigma(5) = 5$ and $\tau(5) = 5$, so $\sigma(\tau(5)) = \sigma(5) = 5$, so $\sigma\tau \in H$. Therefore, H is closed under composition.
- The identity permutation satisfies $\iota(5) = 5$ so $\iota \in H$.
- If $\sigma \in H$, the inverse of σ is defined to be the permutation σ^{-1} such that $\sigma^{-1}(a) = a'$ where a' is the unique element such that $\sigma(a') = a$. Because $\sigma(5) = 5$, we must have $\sigma^{-1}(5) = 5$. Hence, $\sigma^{-1} \in H$ and therefore H is a subgroup of S_5.

(b) Show that $H \cong S_4$.

Solution. We first need to define a function and then show it is a homomorphism. Given a permutation $\sigma \in H$, we must have $\sigma(5) = 5$ and, for any $i \in \{1, 2, 3, 4\}, \sigma(i) \in \{1, 2, 3, 4\}$, hence we can define a permutation $\lambda \in S_4$ by $\lambda(i) = \sigma(i)$. This is a permutation because σ was onto and one-to-one, hence so is λ. Let $\phi : H \to S_4$ be the function such that $\phi(\sigma) = \lambda$, as defined above. Now, we check that this is an isomorphism.

- For any $\sigma_1, \sigma_2 \in H$, $\phi(\sigma_1\sigma_2) = \lambda_1\lambda_2 = \phi(\lambda_1)\phi(\lambda_2)$, hence ϕ is a homomorphism.
- If $\phi(\sigma_1) = \phi(\sigma_2)$, then $\sigma_1(i) = \sigma_2(i)$ for any $i \in \{1, 2, 3, 4\}$ and $\sigma_1(5) = \sigma_2(5) = 5$ by definition, hence $\sigma_1 = \sigma_2$, so ϕ is one-to-one.

- If λ is any permutation in S_4, we can define a function $\sigma \in H$ by $\sigma(i) = \lambda(i)$ for $i \in \{1, 2, 3, 4\}$ and $\sigma(5) = 5$. Then, by definition of ϕ, $\phi(\sigma) = \lambda$, hence ϕ is onto. Therefore, ϕ is an isomorphism.

(c) 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 $a \in G$.

(d) Show that $H' = \{\sigma \in S_5 \mid \sigma(5) = 1\}$ is a left coset of H.

Solution. Let $\tau = (15)$. Then, we will show that $H' = (15)H$. Indeed, given any element $\sigma \in H$, $\tau\sigma \in H'$ because $\tau(\sigma(5)) = \tau(5) = 1$, so $(15)H$ is contained in H'. Also, given any element $\sigma \in H'$, $\tau\sigma(5) = \tau(1) = 5$, so $\tau\sigma \in H$. Because $\tau^{-1} = \tau$, this shows that $\sigma = \tau(\tau\sigma)$, and $\tau(\tau\sigma) \in (15)H$, hence $\sigma \in (15)H$. Therefore, H' is contained in $(15)H$. Because $(15)H \subset H'$ and $H' \subset (15)H$, $H' = (15)H$ and hence H' is a left coset of H.

4. (a) State Lagrange's Theorem.

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

(b) If G is a group with p elements and p is a prime number, prove that G is abelian.

Solution. We will prove something stronger and prove that G is cyclic! Any cyclic group is abelian, so this will prove the desired statement. To prove that G is cyclic, let $a \in G$ be any non-identity element and let $H = \langle a \rangle$. By Lagrange's Theorem, we must have $|H| = 1$ or $|H| = p$. However, $|H| > 1$ because a was a non-identity element, so $H = \{e, a, \dots\}$, so we must have $|H| = p$. Therefore, $\langle a \rangle = H$ contains p elements and is a subgroup of a group with p elements, hence $\langle a \rangle = G$ and G is cyclic (hence abelian).

(c) 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. Prove that, for $n \geq 3$, $|M_n|$ is even.

Solution. First we claim that $H = \{1, n-1\}$ is a subgroup of G. Indeed, it contains the identity and contains inverses because $(n-1)^2 = n^2 - 2n + 1 = 1 \mod n$, hence $(n-1)^{-1} = n - 1$, and is closed because $(1)(1) = 1$, $(1)(n-1) = n-1$ and $(n-1)(n-1) = 1 \mod n$. Therefore, it is a subgroup, and because $n \geq 3$, $n - 1 \neq 1$, so H contains two elements. By Lagrange's Theorem, $|H|$ divides $|M_n|$, so $|M_n|$ must be even.