MTH101: Symmetry

Solutions for Mid-semester examination

Total points: 25

Problem 1. (1 point each) Write the statements of the following theorems:

(a) Lagrange's theorem

(b) First Isomorphism Theorem of group theory.

Solution.
Part (a): Lagrange's Theorem: Let G be a finite group and let H be a subgroup of G. Then, the order of H divides the order of G.

Remark: A special case of this theorem is the statement that $ord(x)$ divides the order of G for any element $x \in G$. This special case will be treated as an acceptable answer since I may have referred to it as "Lagrange's Theorem" during my lectures.

Part (b): First Isomorphism Theorem: Let $\phi : G \to H$ be a group homomorphism. Let K be the kernel of ϕ. Then, the function $G/K \to Im(\phi)$ given by $gK \to \phi(g)$ is a group isomorphism.

□

Problem 2. (1 point each) Define the following terms:

(a) Group homomorphism

(a) Normal subgroup

Solution.
Part (a): Group homomorphism: Let G and H be groups. A group homomorphism from G to H is a function $\phi : G \to H$ such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for any $g_1, g_2 \in G$.

Part (b): Normal subgroup: Let G be a group. A normal subgroup of G is a subgroup $H \leqslant G$ such that for any $g \in G$, $gHg^{-1} \subset H$.

The following answers would also be acceptable:

- Let G be a group. A normal subgroup of G is a subgroup $H \leqslant G$ such that for any $g \in G$, $gHg^{-1} = H$.
- Let G be a group. A normal subgroup of G is a subgroup $H \leqslant G$ such that every left coset of H is also a right coset of H.
- Let G be a group. A normal subgroup of G is a subgroup $H \leqslant G$ such that for any $g \in G$, we have $gH = Hg$.

□

Problem 3. (2 points each)

(a) What is the order of $\langle \overline{6} \rangle$ in $\mathbb{Z}/111\mathbb{Z}$?

(b) What is the order of the group $U(36)$?

(c) Use the Euclidean algorithm to find the greatest common divisor of 10532 and 2324.

Solution.
Part (a): $ord(\overline{6}) = ord(6 \cdot \overline{1}) = \frac{ord(\overline{1})}{gcd(6, ord(\overline{1}))} = \frac{111}{3} = 37.$

Part (b): $|U(36)| = \phi(36) = \phi(2^2 \cdot 3^2) = (2^2 - 2) \cdot (3^2 - 3) = 2 \times 6 = 12.$

Part (c):

$$\begin{aligned} 10532 &= 2324 \times 4 + 1236 \\ 2324 &= 1236 \times 1 + 1088 \\ 1246 &= 1088 \times 1 + 148 \\ 1088 &= 128 \times 7 + 52 \\ 128 &= 52 \times 2 + 44 \\ 52 &= 44 \times 1 + 8 \\ 44 &= 8 \times 5 + 4 \\ 8 &= 4 \times 2 + 0 \end{aligned}$$

So, $gcd(10532, 2324) = 4$. □

Problem 4. (3 points) In the group S_8, consider the elements $\sigma = (3, 2, 4)(5, 1, 8, 7)$ and $\tau = (2, 1, 7)(5, 4, 6, 3)$. Compute the order of the element $\tau\sigma\tau^{-1}$.

Solution. There are two ways to solve this problem. The first method involves simply calculating the cycle decomposition of the permutation $\tau\sigma\tau^{-1}$.

As

$$\tau = (2, 1, 7)(5, 4, 6, 3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 5 & 6 & 4 & 3 & 2 & 8 \end{bmatrix}$$

we see that

$$\tau^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 7 & 6 & 5 & 3 & 4 & 1 & 8 \end{bmatrix}.$$

So,

$$\tau\sigma\tau^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 3 & 7 & 1 & 5 & 8 & 2 \end{bmatrix} = (1, 6, 5)(2, 4, 7, 8).$$

Thus, $ord(\tau\sigma\tau^{-1}) = gcd(3, 4) = 12$.

Another way to solve this problem is to observe that if $\phi : S_8 \to S_8$ is the function $\phi(x) = \tau x \tau^{-1}$, then ϕ is an isomorphism of S_8. (We saw this in Problem set 1, Problem 3.) Thus, $ord(\tau\sigma\tau^{-1}) = ord(\phi(\sigma)) = ord(\sigma)$. Since we have already been given the cycle decomposition of σ, we see that $ord(\sigma) = gcd(3, 4) = 12$. □

Problem 5. (3 points) Let $\mathbb{Q}$ denote the group of rational numbers under addition and let $\mathbb{Z}$ denote the group of integers under addition. Let G denote the quotient group $\mathbb{Q}/\mathbb{Z}$. Prove that every element of G has finite order.

Solution. Let $\phi : \mathbb{Q} \to G$ denote the quotient homomorphism. Let $x \in G$. Then, x is of the form $p/q + \mathbb{Z}$ for some rational number p/q where p and q are integers. Thus, $x = \phi(p/q)$. Then

$$qx = q\phi(p/q) = \phi(q \times (p/q)) = \phi(p) = p + \mathbb{Z} = \mathbb{Z} = 0_G.$$

Thus, we see that $ord(x)$ is finite. This shows that every element of G has finite order. □

Problem 6. (3 points) Let G be an abelian group. Let S be the set of all elements of G having finite order. Prove that S is a subgroup of G.

Solution. Clearly the identity element 1_G has finite order and so $1_G \in S$.

Let $x \in S$. Then $x^n = 1_G$ for some positive integer n. Then $(x^{-1})^n = x^{-n}$ is the inverse of $x^n = 1_G$. Thus, $(x^{-1})^n = 1_G$. Thus, x^{-1} has finite order and so $x^{-1} \in S$.

Let $x, y \in S$. We want to show that $xy \in S$. As $x, y \in S$, there exist positive integers m, n such that $x^m = y^n = 1_G$. As G is abelian, $(xy)^k = x^k y^k$ for any integer k. So $(xy)^{mn} = x^{mn}y^{mn}$. But $x^{mn} = (x^m)^n = 1_G$ and similarly $y^{mn} = (y^n)^m = 1_G$. Thus, we see that $(xy)^{mn} = 1_G$. This shows that xy has finite order and is hence in S.

Thus, we see that S is a subgroup of G. □

Problem 7. (3 points) Let $\phi : S_6 \to S_6$ be the function defined by $\phi(x) = x^2$. Is ϕ a group homomorphism? Justify your answer. (Do not just answer "yes" or "no". You must prove your claim.)

Solution. For ϕ to be a group homomorphism, we must have $\phi(xy) = \phi(x)\phi(y)$ for any $x, y \in S_6$. In other words, we must have $(xy)^2 = x^2y^2$ for any $x, y \in S_6$.

But

$$\begin{aligned} (xy)^2 &= x^2y^2 \\ \iff xyxy &= xxyy \\ \iff x^{-1} \cdot xyxy \cdot y^{-1} &= x^{-1} \cdot xxyy \cdot y^{-1} \\ \iff yx &= xy. \end{aligned}$$

However, S_6 is not a commutative group and so the relation $xy = yx$ does not hold for all elements $x, y \in S_6$. Thus, ϕ is not a group homomorphism. □

Problem 8. (3 points) Prove that S_{10} does not have any element of order 35. (Hint: If such an element existed, what would its cycle decomposition look like?)

Solution. Suppose x is an element of order 35. We consider its cycle decomposition. Suppose it is of the form $x = \tau_1\tau_2\cdots\tau_r$ where $\tau_1, \ldots, \tau_r$ are disjoint cycles of length $n_1, n_2 \ldots, n_r$ respectively. Then, $n_1 + n_2 + \cdots + n_r = 10$. Also, $ord(x) = lcm(n_1, \ldots, n_r)$.

As 35 divides $lcm(n_1, \ldots, n_r)$, the cycle decomposition of x must contain a cycle whose length is divisible by 7. As the length of the cycle has to be less than or equal to 10, we see that there must exist a cycle of length 7. Let us suppose this is the cycle τ_i, where $1 \leqslant i \leqslant r$.

Similarly, there must exist a cycle whose length is divisible by 5. As the length of the cycle has to be less than or equal to 10, it can be either 5 or 10.

We know that $n_1 + n_2 + \ldots + n_r = 10$. We know that there exists a cycle of length 7 and another cycle of length either 5 or 10. But $7 + 5 = 12 > 10$ and $7 + 10 = 17 > 10$. This is a contradiction. Thus, there is no such element. □
