MATH 411: INTRODUCTION TO ABSTRACT ALGEBRA
HOMEWORK #6

TRUNG DANG
33858723

Problem 1

Problem statement: The goal of this exercise is to finish the proof of the first isomorphism theorem using an outline from the lecture. Let $f : G \to K$ be a surjective homomorphism of the groups. Let H be the kernel of f. Let G/H be the quotient group. Define a function $\tau : G/H \to K$ by the formula $\tau(gH) = f(g)$

(1) Show that τ is well-defined

(2) Show that τ is surjective

(3) Show that τ is injective

(4) Show that τ is an isomorphism

Solution. (1) For every left cosets $g_1H = g_2H \in G/H$, then we have $g_2 = g_1h$ for some $h \in H$. Then $f(g_2) = f(g_1h) = f(g_1)f(h) = f(g_1)$ (since H is the kernel of f) . Therefore, τ is well-defined.

(2) Since $G \to K$ is subjective, $\forall k \in K, k = f(g) = \tau(gH)$ for some $g \in G$. Therefore, τ is surjective

(3) Assume that there are 2 disjoint left cosets $g_1H, g_2H \in G/H$ such that $\tau(g_1H) = \tau(g_2H)$. Then, $f(g_1) = f(g_2)$. Let $g_1 = g_2g$ for some $g \in G$. Then $f(g_1) = f(g_1)f(g)$. Left multiply both sides by $f(g_1)^{-1}$, we have $f(g) = e_k$, the identity of k, so g must be in the kernel of f.
In other words, $g \in H$, so $g_2 = g_1g \in g_1H$, a contradiction.
Therefore, τ is injective

(4) Let $g_1H, g_2H \in G/H$ be 2 arbitrary left cosets. Then, $\tau(g_1H \cdot g_2H) = \tau(g_1g_2H) = f(g_1g_2) = f(g_1)f(g_2) = \tau(g_1H)\tau(g_2H)$ (because f is already a homomorphism). Therefore, τ is a homomorphism.
From (2), and (3), we also have τ is a bijection. Therefore, τ is an isomorphism.

■

Problem 2

Problem Statement: Use the first isomorphism theorem to compute the quotient groups:

(1) $\mathbb{Z}_{24}/ < 6 >$

(2) $GL_n(\mathbb{R})/SL_n(\mathbb{R})$

Solution. (1) Let G be $\mathbb{Z}_{24}$, K be $\mathbb{Z}_6$, and the function f takes elements in $\mathbb{Z}_{24}$ to its modulo 6 in $\mathbb{Z}_6$. Clearly, f is a surjective function. Also, the kernel of f is $H =< 6 >$.
By the proof of the first isomorphism, let τ be a bijection from $G/H \to K$ such that $\tau(gH) = f(g) \forall g \in G$. Therefore the cosets in the quotient group $\mathbb{Z}_{24}/ < 6 >$ can be computed by finding the elements g corresponding to each $f(g) \in \mathbb{Z}_6$.
But we already know that $f(x) = x \mod 6$. Therefore,

$$f(0) = 0, f(1) = 1, \cdots, f(5) = 5$$

And thus, the quotient group is: $\{H, 1+H, \cdots 5+H\}$

(2) Let G be $GL_n(\mathbb{R})$, K be $\mathbb{R}^*$, and f takes elements in G to its determinant (which is a real number in K).
We first show that f is a surjective function. Indeed, for all x in $\mathbb{R}^*$,

$$x = \det \begin{bmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

Therefore f is an injective function. Also, the kernel of f is $H = SL_n(\mathbb{R})$.
Now using the first isomorphism theorem, it suffices to find ONE g such that $f(g) = x$ for each $x \in \mathbb{R}^*$, then the quotient group of $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ follows as the group of gH for each g found.
But from the equation above, we have shown the matrix that satisfies $det = x$ for each $x \in \mathbb{R}^*$. Therefore, the desired quotient group is:

$$\{gSL_n(\mathbb{R}) : g = \begin{bmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}, x \in \mathbb{R}^*\}$$

■

Problem 3

When X is an infinite set, the group S_X of all bijections $f : X \to X$ is often too big for practical purposes. So while every action of a group G on X is still defines a homomorphism $\alpha : G \to S_X$ as discussed in class, it is often desirable to find a smaller, more interesting subgroup of S_X so that the image of f is contained in that subgroup. Show that the following subsets of S_X are subgroups:

(1) $S^0_{\mathbb{R}} = \{f \in S_{\mathbb{R}} | f \text{ is a continuous function }\}$

(2) $\text{Isom}(\mathbb{R}^n) = \{f \in S_{\mathbb{R}^n} | f \text{ preserves distance between points }\}$

Solution. (1) First $S^0_{\mathbb{R}}$ contains the identity function, that is: $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x, \forall x \in \mathbb{R}$. Therefore, $S^0_{\mathbb{R}}$ is non-empty and contains the identity element.
Second, $\forall f, g \in S^0_{\mathbb{R}}$, $f \cdot g(x) = f(g(x))$ is a continuous function (since the composition of 2 continuous functions is a continuous function). Therefore, $S^0_{\mathbb{R}}$ is closed under operation.
Third, for every $f \in S^0_{\mathbb{R}}$, its inverse is also a continuous function. Therefore, $S^0_{\mathbb{R}}$ is closed under inverse.

By the subgroup test, we therefore conclude that $S^0_{\mathbb{R}}$ is a subgroup of $S_{\mathbb{R}}$

(2) First $Isom(\mathbb{R}^n)$ contains the identity function, that is: $f : \mathbb{R}^n \to \mathbb{R}^n$ such that $f(x) = x, \forall x \in \mathbb{R}^n$. Therefore, $Isom(\mathbb{R}^n)$ is non-empty and contains the identity element.
Second, $\forall f, g \in Isom(\mathbb{R}^n)$, $f \cdot g(x) = f(g(x))$ preserves the distance between points. Indeed, let $d(a,b)$ be the distance between points a,b. then $d(a,b) = d(g(a), g(b)) = d(f(g(a)), f(g(b)))$. Therefore, $Isom(\mathbb{R}^n)$ is closed under operation.
Third, for every $f \in Isom(\mathbb{R}^n)$, its inverse is also preserves the distance between points. Let $c = f^{-1}(a), d = f^{-1}(b)$, then $d(c,d) = d(f(c), f(d)) = d(a,b)$ Therefore, $Isom(\mathbb{R}^n)$ is closed under inverse.

By the subgroup test, we therefore conclude that $Isom(\mathbb{R}^n)$ is a subgroup of $S^n_{\mathbb{R}}$

■

Problem 4

Problem Statement: Show that both groups (a) $S^0_{\mathbb{R}}$ and (b) Isom($\mathbb{R}^n$) from the previous exercise admit a surjective homomorphism to $\mathbb{Z}_2$. Describe its kernel.

Solution. (1) Observe that since f is continuous and f is a bijection from $\mathbb{R} \to \mathbb{R}$, then f must be monotonic. Then, consider the function τ which maps increase functions to 0 and decrease functions to 1. Then, for 2 functions $f, g \in S^0_{\mathbb{R}}$

- If f, g are both increase functions, then $a > b \Longrightarrow g(a) \geq g(b) \Longrightarrow f(g(a)) \geq f(g(b))$. Thus $f \cdot g$ is an increasing function.
- If f is an increase function, g is a decrease function, then $a \geq b \Longrightarrow g(a) \leq g(b) \Longrightarrow f(g(a)) \leq f(g(b))$
- If f is a decrease function, g is an increase function, then $a \geq b \Longrightarrow g(a) \geq g(b) \Longrightarrow f(g(a)) \leq f(g(b))$
- If f is a decrease function, g is a decrease function, then $a \geq b \Longrightarrow g(a) \leq g(b) \Longrightarrow f(g(a)) \geq f(g(b))$

Thus, $\tau(f)\tau(g) = \tau(fg)$, and $S^0_{\mathbb{R}}$ is homomorphic to $\mathbb{Z}_2$.
The kernel of the homomorphism is the set of all increasing functions. (Note that it can also be the set of all decreasing functions if τ is defined reversedly)

(2) Note that $Isom(\mathbb{R}^n)$ is comprised of combinations of rotations and reflections and that an odd number of reflections results in a reflection, and an even number of reflections result in a rotation. (1)
Therefore, let τ be a function that maps $Isom(\mathbb{R}^n)$ to the number of reflections mod 2. Then, by (1), we can conclude that $\tau(fg) = \tau(f)\tau(g), \forall f, g \in Isom(\mathbb{R}^n)$.
Thus, $Isom(\mathbb{R}^n)$ is homomorphic to $\mathbb{Z}_2$, and the kernel of it is the set of all rotations in $\mathbb{R}^n$

■

Problem 5

Problem Statement: Let G be an abelian group written additively, let n be a positive integer, and let $\phi_n : G \to G$ be the function $\phi_n(x) = x + \cdots + x$ (n summands).

(1) Prove that ϕ_n is a homomorphism

(2) Suppose $G \approxeq H \times K$ where H is a cyclic group. Show that $\phi_n(G) \neq G$ for some n.

(3) Show that $\mathbb{Q}$ is not isomorphic to a direct product of cyclic groups.

Solution. (1) For every $x, y \in G$, we have:

$$\begin{aligned}\phi_n(x+y) &= \underbrace{(x+y)+\cdots+(x+y)}_{n \text{ times}} \\ &= (\underbrace{x+\cdots+x}_{n \text{ times}}) + (\underbrace{y+\cdots+y}_{n \text{ times}}) \text{ (since G is abelian, we can swap x's and y's)} \\ &= \phi_n(x) + \phi_n(y)\end{aligned}$$

Therefore, ϕ_n is a homomorphism

(2) Let $a \in H$ be the generator of cyclic group H, e_h be the identity of H, e_k be the identity of K, n be the order of H, and e be the identity of G. Then, we have:

$$\phi_n(e) = e$$

Also, let $f : G \to H \times K$ be the bijection that maps G to its isomorphism, and let $t \in G$ be the element such that: $f(t) = (a, e_k)$. Then $f(\underbrace{t+t+\cdots+t}_{\text{n times}}) = \underbrace{f(t)+f(t)+\cdots+f(t)}_{\text{n times}} = \underbrace{(a,e_k)+\cdots+(a,e_k)}_{\text{n times}} = (a+a+\cdots+a, e_k) = (e_h, e_k)$

Thus, $\underbrace{t+t+\cdots+t}_{\text{n times}} = e$, or $\phi_n(t) = e$. Also, since $a \neq e_h$, we must have $e \neq t$. Thus,

$$\exists e \neq t : \phi_n(e) = \phi_n(t)$$

, which implies $|\phi_n(G)| < |G|$. Thus, $\phi_n(G) \neq G$ for $n = ord(H)$

(3) Assume that $\mathbb{Q}$ is isomorphic to a direct product of cyclic groups. Then we can write $\mathbb{Q} \approxeq H \times K$ for some cyclic group H and K is the product of the remaining cyclic groups. Then, by part (2), we have that $\phi_n(\mathbb{Q}) \neq \mathbb{Q}$ for some n. (1).
Nonetheless, we also have that $\phi_n(x) = nx \neq ny = \phi_n(y), \forall x \neq y \in \mathbb{Q}$, and $\phi_n(x/n) = x, \forall x \in \mathbb{Q}$, so $\phi_n : \mathbb{Q} \to \mathbb{Q}$ is a bijection for all positive integer n. Thus, $\phi_n(\mathbb{Q}) = \mathbb{Q}$ for all positive integers n. (2).
From (1), and (2), we have a contradiction, so the assumption is false, and $\mathbb{Q}$ is not isomorphic to any direct product of cyclic groups.

■

Problem 6

Problem Statement: Let p be a prime number and take a direct product $G = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$, where $n_1 \geq n_2 \geq \cdots \geq n_k$. Let H be the kernel of the homomorphism ϕ_p from the previous problem and let K be its image.

(1) Prove that $H \approxeq (\mathbb{Z}_p)^k$

(2) Prove that $K \approxeq \mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}}$

(3) Prove that the numbers $n_1, \cdots, n_k$ are determined by G uniquely, i.e. if $\mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}} \approxeq \mathbb{Z}_{p^{n_1'}} \times \cdots \times \mathbb{Z}_{p^{n_{k'}'}}$ then $k = k'$ and $n_1 = n_1', \cdots$, etc.

Solution. (1) We will first investigate the properties of the elements in the kernel H of ϕ_p. If $(a_1, a_2, \cdots, a_k) \in H$, then $(pa_1, pa_2, \cdots, pa_k) = (0, 0, \cdots, 0)$, where pa_i is the regular multiplication notation. Then,

$$\begin{aligned} pa_1 &\equiv 0 \mod p^{n_1} \\ pa_2 &\equiv 0 \mod p^{n_2} \\ &\vdots \\ pa_k &\equiv 0 \mod p^{n_k} \end{aligned}$$

or $a_i = b_i p^{n_i - 1}$, for some $b_i \in \{0, 1, \cdots, p-1\}$.
Then let $f : H \to (\mathbb{Z}_p)^k$ be a function that maps $(a_1, a_2, \cdots, a_k) \mapsto (b_1, b_2, \cdots, b_k)$.
Then apparently

$$f((a_{11}, a_{21}, \cdots, a_{k1})) = f((a_{12} a_{22}, \cdots, a_{k2})) \iff a_{11} \equiv a_{12} \mod p^{n_1}, \cdots, a_{k1} \equiv a_{k2} \mod p^{n_k}$$

, Thus, f is a injection. (1)
For every element $y = (b_1, b_2, \cdots, b_k) \in (\mathbb{Z})_p^k$, by definition, we also have an element $x = (b_1 p^{n_1 - 1}, \cdots, b_k p^{n_k - 1})$ such that $f(x) = y$, so f is a surjection. (2)
Last but not least, it is easy to verify that $f(x + y) = f(x) + f(y) \forall x, y \in H$. (3)
Combining (1). (2), (3), we have that f is an isomorphism between H and $(\mathbb{Z}_p)^k$

(2) Let $x = (a_1, a_2, \cdots, a_k)$ be an arbitrary element of G. Then, $\phi_p(x) = (pa_1, pa_2, \cdots, pa_k)$. Then let g be a function that maps $K \to \mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}}$ such that:

$$g(\phi_p(x)) = (a_1 \mod p^{n_1 - 1}, a_2 \mod p^{n_2 - 1}, \cdots, a_k \mod p^{n_k - 1})$$

We will prove that g is the desired isomorphism.
Let $x = (a_1, a_2, \cdots, a_k), y = (b_1, b_2, \cdots, b_k)$ be elements of G such that $g(\phi_p(x)) = g(\phi_p(y))$. Then,

$$\begin{aligned} a_1 \equiv b_1 \mod p^{n_1 - 1} &\implies pa_1 \equiv pb_1 \mod p^{n_1} \\ &\vdots \\ a_k \equiv b_k \mod p^{n_k - 1} &\implies pa_k \equiv pb_k \mod p^{n_k} \end{aligned}$$

Thus, $\phi_p(x) = \phi_p(y)$, or g is an injection. (1)
By definition, for all $x \in \mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}}$, we also have $g(\phi(x)) = x$, therefore g is a surjection. (2)
Lastly, $g(\phi_p(x)+\phi_p(y)) = (a_1+b_1 \mod p^{n_1-1}, \cdots, a_k+b_k \mod p^{n_k-1}) = (a_1 \mod p^{n_1-1}, \cdots, a_k \mod p^{n_k-1}) + (b_1 \mod p^{n_1-1}, \cdots, b_k \mod p^{n_k-1}) = g(\phi_p(x)) + g(\phi_p(y))$. Thus, g is a homomorphism. (3)
From (1), (2), (3), we conclude that $K \approxeq \mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}}$

(3) We first notice that if $\mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}} \approxeq \mathbb{Z}_{p^{n'_1}} \times \cdots \times \mathbb{Z}_{p^{n'_{k'}}}$, then the kernel of both representation must be the same, that is $H \approxeq (\mathbb{Z}_p)^k \approxeq (\mathbb{Z}_p)^{k'}$. This implies that $k = k'$ (1)
Observe that the image of ϕ_p on G must be the same, so

$$\mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}} \approxeq \mathbb{Z}_{p^{n'_1-1}} \times \cdots \mathbb{Z}_{p^{n'_k-1}}$$

WLOG, assume that $n_k < n'_k$. Then we have:

$$\begin{aligned}
&\mathbb{Z}_{p^{n_1-1}} \times \cdots \mathbb{Z}_{p^{n_k-1}} \approxeq \mathbb{Z}_{p^{n'_1-1}} \times \cdots \mathbb{Z}_{p^{n'_k-1}} \\
\iff &\mathbb{Z}_{p^{n_1-2}} \times \cdots \mathbb{Z}_{p^{n_k-2}} \approxeq \mathbb{Z}_{p^{n'_1-2}} \times \cdots \mathbb{Z}_{p^{n'_k-2}} \\
\iff &\cdots \\
\iff &\mathbb{Z}_{p^{n_1-n_k}} \times \cdots \mathbb{Z}_{p^{n_k-n_k}} \approxeq \mathbb{Z}_{p^{n'_1-1}} \times \cdots \mathbb{Z}_{p^{n'_k-n_k}} \\
\iff &\mathbb{Z}_{p^{n_1-n_k}} \times \cdots \mathbb{Z}_{p^{n_{k-1}}} \approxeq \mathbb{Z}_{p^{n'_1-n_k}} \times \cdots \mathbb{Z}_{p^{n'_k-n_k}}
\end{aligned}$$

But then the left-hand-side of the expression only consists of $k-1$ elements, while the right-hand-side of the expression contains k elements (contradicts with (1)).
Therefore, $n_k \geq n'_k$. Similarly, we also have $n_k \leq n'_k$, so $n_k = n'_k$.
Applying the same reasonings to $k-1, k-2, \cdots, 1$, we have: $n_1 = n'_1, n_2 = n'_2, \cdots$ (2)

From (1) and (2) we conclude that $n_1, n_2, \cdots$ are determined by G uniquely

■

Problem 7

Problem Statement: Consider the action of the group A_4 on itself by conjugation. Describe the stabilizer of every element.

Solution. The elements of A_4 are:

$$Id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)$$

These elements form 3 conjugacy classes, namely: $Id, \{(12)(34), (13)(24), (14)(23)\}$, $\{(123), (132), (124), (142), (134), (143), (234), (243)\}$ It suffices to describe the stabilizer of one element of each group, and the properties of other elements should follow.

- First, since $geg^{-1} = e, \forall g \in A_4$, the stabilizer of Id is A_4 itself.
- Let τ be an element in the stabilizer of $(12)(34)$. Then $\tau(12)(34)\tau^{-1} = \tau(12)\tau^{-1}\tau(34)\tau^{-1} = (\tau(1)\tau(2))(\tau(3)\tau(4))$. Substituing different cases of $\tau(1)$ in, we have the stabilizer of $(12)(34)$ is: $\{Id, (12)(34), (13)(24), (14)(23)\}$. From this, one can verify that for all elements of the form $(ab)(cd)$, its stabilizer is : $\{Id, (ab)(cd), (ac)(bd), (ad)(bc)\}$
- Lastly, let τ be an element in the stabilizer of (123), then $\tau(123)\tau^{-1} = (\tau(1)\tau(2)\tau(3))$. If $\tau(1) = 1$, then $\tau(2) = 2, \tau(3) = 3$, so $\tau = Id$. If $\tau(1) = 2$, then $\tau(2) = 3$, $\tau(3) = 1$, so $\tau = (123)$. If $\tau(1) = 3$, then $\tau(2) = 1$, $\tau(3) = 2$, so $\tau = (132)$. Note that $\tau(1) \neq 4$ since this will not preserve the cycle structure (123). Thus, the stabilizer of (123) is $\{Id, (123), (132)\}$. In general, the stabilizer of (abc) is $\{Id, (abc), (acb)\}$

■

Problem 8

Problem Statement:

(1) Show that S_n acts on the power set $2^{\{1,2,3,\cdots,n\}}$ as follows: if $\sigma \in S_n$ and $S = \{i_1, \cdots, i_k\}$, then $\sigma \star S = \{\sigma_{i_1}, \cdots, \sigma_{i_k}\}$

(2) Find the number of orbits of this action

(3) Find the stabilizer in S_n of a subset $S = \{1, \cdots, k\} \subset \{1, \cdots, n\}$

(4) Use the orbit-stabilizer theorem to compute the size of each orbit

Solution. (1) Denote $P = S_{2^{\{1,2,3,\cdots,n\}}}$. We will check the axioms of the action $S_n \curvearrowright P$.

- Let $S = \{i_1, i_2, \cdots, i_k\}$, e be the identity element of S_n. Then, $e \star S = \{i_1, i_2, \cdots, i_k\} = S$
- Define the same s and let σ_1, σ_2 be 2 elements of S_n. Then, $(\sigma_1\sigma_2)\star x = \{\sigma_1\sigma_2 i_1, \cdots, \sigma_1\sigma_2 i_k\} = \sigma_1 \star \{\sigma_2 i_1, \cdots, \sigma_2 i_k\} = \sigma_1 \star \sigma_2 \star S$

Thus, the function satisfies the action axioms, and therefore is an action $S_n \curvearrowright P$

(2) We will show that for every subset S of length k, the orbit of S is the set of all sets of size k of $2^{\{1,2,3,\cdots,n\}}$.
Indeed, for every $\sigma \in S_n$, σS has size k. Now we show that for every $Q = \{j_1, j_2, \cdots, j_k\}$, choose σ such that $\sigma(i_l) = j_l, \forall\, l \in \{1, 2, \cdots, k\}$. Then $\sigma S = Q$.
Thus, the orbits of this action are the sets that contain subsets of the same size, so there are (n+1) orbits.

(3) Let $\sigma \in S_n$ be an element in the stabilizer of $\{1, 2, 3, \cdots, k\} \subset \{1, \cdots, n\}$. Then for all $\forall\, i \leq k$, $\sigma(i) \leq k$, and for all $i > k, \sigma(i) > k$. Thus, the stabilizer in S_n of S is the set $S_{k,n}$, which contains the union of the permutations of elements from 1 to k and the permutations of elements from $k+1$ to n.

(4) From the previous question, we have $|S_{k,n}| = k!(n-k)!$. Therefore, the size of the orbit of the sets with size k has size:

$$|Orb(x)| = \frac{|G|}{|G_x|} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

■

Problem 9

Problem Statement: Let G be a group acting on a set X and suppose that this action is transitive. Let $x, y \in X$. Prove there exists $g \in G$ such that $G_y = gG_xg^{-1}$

Solution. Since the action is transitive, there is only one orbit, and thus $\forall x, y \in X$, there exists $g \in G$ such that $g \star x = y$. We will show that $G_y = gG_xg^{-1}$.
Indeed, let a be an arbitrary element of G_y, then we will show that $g^{-1}ag$ is in G_x.

$$\begin{aligned} g^{-1}ag(x) &= g^{-1}a(g \star x) \\ &= g^{-1}a \star y \\ &= g^{-1} \star y = x \end{aligned}$$

Therefore, $g^{-1}ag$ maps x to itself, therefore belongs to G_x. Thus, $G_y \subseteq gG_xg^{-1}$. (1)
Reversedly, let b be an arbitrary element of G_x, then

$$\begin{aligned} gbg^{-1}(y) &= gb(g^{-1} \star y) \\ &= gb \star x \\ &= g \star x \\ &= y \end{aligned}$$

so gbg^{-1} maps y to itself, therefore belongs to G_y. Thus, $gG_xg^{-1} \subseteq G_y$. (2)
From (1), and (2), the proof is completed. ■

Problem 10

Problem Statement: Let G be the group of rotations of the cube.

(1) Show that G acts on the set of 4 diagonals of the cube.

(2) Show that no element of G except for the identity element takes every diagonal to itself.

(3) Show that G is isomorphic to S_4

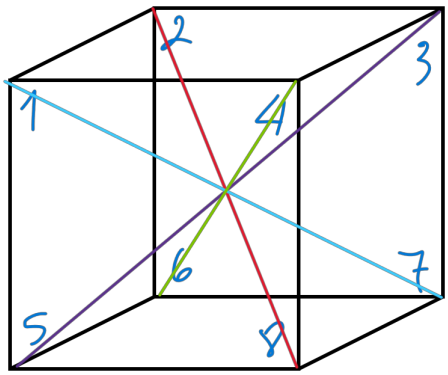


FIGURE 1

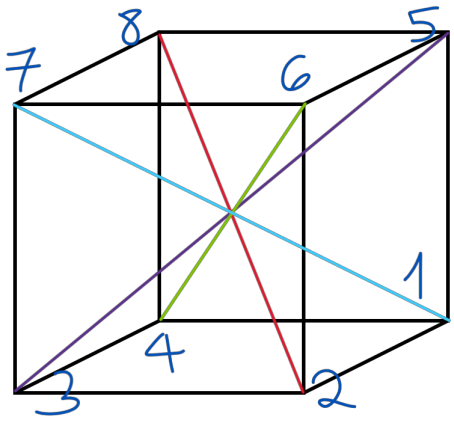
Solution. (1) Consider the cube with vertices labeled and 4 diagonals colored as above. Let X be the set of permutations of diagonals of the cube. We will show that $G \curvearrowright X$ satisfies the axioms of actions:

- $ex = e \star x = x \forall x \in X$
- Let g_1, g_2 be arbitrary rotations of the cube, then by definition of cube rotation, g_1 permutes the diagonals obtained by the permutation of g_2 on the original arrangement of permutations. Therefore, $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Thus, G acts on the set of 4 diagonals of the cube.

(2) Assume that there is another element g of G that takes every diagonal to itself. Then consider the cube in the figure above.
Since g is not the identity, at least one of the diagonals must be affected. WLOG assumes that g acts on the red diagonal resulting in 2 and 8 swapping places. Then, by Euler's Theorem, since rotations preserve the orientation of the cube, (1,7), (3,5), and (4,6) must

also swap places. So we get:



But then the cube changed orientation, since viewing from the center, 1 initially goes to 2 counterclockwise, but now 1 goes to 2 clockwise.
Thus, the assumption is false, and the identity is the only element of G that takes every diagonal to itself.

(3) Let x be the original state of the cube as demonstrated in Figure 1. Then, we will show that G is isomorphic to the group of permutations of the diagonals X, which is equivalent to S_4. Define $f : G \to X$ as $f(g) = gx = g \star x, \forall g \in G$, and x defined above.
First, we observe that we can swap any two diagonals by applying a rotation on another diagonal: For instance, we can swap the purple and blue diagonals by rotating around the green diagonal 180 degrees. And since any permutations can be written as a product of transpositions, f is onto.
Second, assume that there are 2 rotations g, g' that result in the same diagonal permutations. Assume $g = hg'$ for some $h \in G$. Then, $gx = hg'x = h(g'x) = h(gx)$. Thus, h takes gx to gx, so from (2), h must be identity. Thus, $g = g'$, or f is one-to-one.
Third, since $f(g_1g_2) = (g_1g_2)x = g_1(g_2x) = g_1f(g_2) = f(g_1)f(g_2)$ by definition of action, so f is homomorphic.
Thus, f is an isomorphism between G and X, thus an isomorphism between G and S_4.
■