Problem §1 (2.22) Let $\mathcal{C}_n$ denote a cyclic group of order n, $\mathcal{D}_n$ denote the n^{th} dihedral group, and $\mathcal{S}_n$ the n^{th} symmetric group.

(a) Prove that $\mathcal{C}_2$ and $\mathcal{S}_2$ are isomorphic.

(b) Prove that $\mathcal{D}_3$ and $\mathcal{S}_3$ are isomorphic.

(c) Let $m \geq 3$. Prove that for every n, $\mathcal{C}_m$ and $\mathcal{S}_n$ are not isomorphic.

(d) Prove that for every $n \geq 4$, $\mathcal{D}_n$ and $\mathcal{S}_n$ are not isomorphic.

(e) More generally, let $m \geq 4$ and $n \geq 4$. Prove that $\mathcal{D}_m$ and $\mathcal{S}_n$ are not isomorphic.

(f) Prove that $\mathcal{D}_4$ and $\mathcal{Q}$ are not isomorphic.

Solution:

(a) $\mathcal{C}_2 = \{e, g\}$, $\mathcal{S}_2 = \{e, \pi\}$. Define a mapping $\phi : \mathcal{C}_2 \to \S_2$, where $\phi(e) = e,\ \phi(g) = \pi$. ϕ is clearly a bijective homomorphism; thus $\mathcal{C}_2$ is isomorphic to $\mathcal{S}_2$.

(b) Let $\phi_3 : \mathcal{D}_3 \to \mathcal{S}_3$ be the mapping that sends every $\sigma \in \mathcal{D}_3$ to the $\pi \in \mathcal{S}_3$ such that $\sigma(i) = \pi(i),\ i \in \{1, 2, 3\}$. Problem 1 from last week's problem set shows that a map $\phi_n : \mathcal{D}_n \to \mathcal{S}_n$, as defined above, is a homomorphism, is injective for all $n \in \mathbb{Z}^+$, and surjective for $1 \leq n \leq 3$. Hence ϕ_3 is bijective, and so $\mathcal{D}_3$ is surjective to $\mathcal{S}_3$. (Alternatively, one could simply list all permutations in $\mathcal{S}_3$ and all transformations in $\mathcal{D}_3$, and observe that such a ϕ_3 is isomorphic. The reader is spared the work here.)

(c) We begin with two lemmas.

Lemma 1. *Let G, H be groups, and let G be cyclic. If G is isomorphic to H, then H is cyclic.*

Proof. Given groups G, H, suppose G is cyclic and let $f : G \to H$ be an isomorphism.

Let $g_0 \in G$ be a generator for G, and let $f(g) = h \in H$ for some $g \in G$. Since G is cyclic, $g = g_0^m$ for some $m \in \mathbb{Z}$. Then

$$\begin{aligned} h = f(g) &= f(g_0^m) \\ &= f(g_0 \cdot \ldots \cdot g_0) \\ &= f(g_0)^m = h_0^m \text{ for some } h_0 \in H\ . \end{aligned}$$

Hence for any $h \in H$, $h = h_0^m$ for some $h_0 \in H$. Thus any $h \in H$ is in $\langle h_0 \rangle$, and so H is cyclic as well. $\square$

Lemma 2. *Let G be a group. If G is cyclic, then any subgroup $H < G$ is cyclic.*

Proof. Let G be a group, and let $H < G$. Suppose G is cyclic. Then for any $g \in G$, $g = g_0^m$, where g_0 is a generator of G.

Let $h \in H$. Since G is cyclic and $h \in G$, $h = g_0^m$ for some $m \in \mathbb{Z}$. Let $k \in \mathbb{Z}$ be the smallest k such that $g_0^k \in H$. Then for any $h = g_0^m \in H$, we have $m = kq + r$ for some $q, r \in \mathbb{Z},\ 0 \leq r < k$. Thus

$$\begin{aligned} g_0^m &= g_0^{kq+r} \\ &= g_0^{kq} g_0^r. \end{aligned}$$

Since H is a subgroup, any $h \in H$ has $h^{-1} \in H$. Thus

$$\begin{aligned} g_0^m &= g_0^{kq} g^r \\ g_0^{-kq} g_0^m &= g_0^r \\ g_0^{m-kq} &= g_0^r, \end{aligned}$$

and by closure, $g_0^r \in H$ as well. But k is the smallest integer such that $g_0^k \in H$, and $0 \leq r < k$; thus $r = 0$ (otherwise, we have a contradiction).

Thus for any $h \in H$, $h = (g_0^k)^q$, and so H is a cyclic group generated by g_0^k. $\square$

From Lemma 2, we get its contrapositive: *if a subgroup H of a group G is not cyclic, then G is not cyclic*, and we make one observation: $\mathcal{S}_3$ **is not cyclic** (one can easily see that any $\pi \in \mathcal{S}_3$ does not generate $\mathcal{S}_3$). From the contrapositive to Lemma 2, since $\mathcal{S}_3$ is a subgroup of $\mathcal{S}_n$, and $\mathcal{S}_3$ is not cyclic, $\mathcal{S}_n$ is not cyclic. Taking the contrapositive of Lemma 1, (if G is cyclic and H is not cyclic, H is not isomorphic to G), since $\mathcal{S}_n$ is not cyclic and $\mathcal{C}_m$ is cyclic, they are not isomorphic.

(d) Recall that $\mathcal{D}_n$ has order $2n$, while $\mathcal{S}_n$ has order $n!$. Since for any $n > 3$, $2n \neq n!$, $\mathcal{D}_n$ is not isomorphic to $\mathcal{S}_n$.

(e) We start with another lemma:

Lemma 3. *Let G, H be groups. If G is isomorphic to H, then for any $g \in G$, the corresponding (unique) $f(g) = h \in H$ has the same order as g.*

Proof. Let $f : G \to H$ be an isomorphism, let $g \in G$ have order n, and let $f(g) = h \in H$. Recall that for a homomorphism, $f(e) = e'$, where $e' \in H$ is the identity. Then

$$\begin{aligned} f(e) = f(g^n) &= f(g) \cdot \ldots \cdot f(g) \\ &= f(g)^n \\ &= h^n = e'. \end{aligned}$$

Since f is isomorphic, and any $g^m \neq e$ when $m \in \mathbb{Z}$ and $m < n$, n is the smallest positive integer such that $h^n = e'$; that is, $h \in H$ has order n as well. $\square$

Now, consider the dihedral group $\mathcal{D}_m$. We observe that all flips have order 2: if we flip an n-gon twice, we get back to the original shape (formally, if we define a flip $f_j(i) = m - j + i$, then $f_j(f_j(i)) = f_j(m - i + j) = m - (m - i + j) + j = m - m - j + j + i = i$ for all $0 \leq j < m$. Refer back to problem set 2 for a more complete definition of the dihedral group.) Additionally, we observe that there are only two rotations with order 3: given a rotation

$$r_j(i) = i + j, \ j \in \{0, \ldots, m-1\},$$

$r_j^3(i) = i$ only when $i + 3j \mod m = i$; that is, $3j \mod m \equiv 0$. Since $j \in \{0, \ldots, m-1\}$, this is only the case when $j = \frac{m}{3}$ or $\frac{2m}{3}$. Thus $\mathcal{D}_m$ only has two elements of order 3.

On the other hand, $\mathcal{S}_n$ clearly has more than 2 elements with order 3: one can easily choose permutations $\pi_1 = (123), \ \pi_2 = (124), \ \pi_3 = (234)$ for any $\mathcal{S}_n$ when $n \geq 4$.

By the Lemma, if $\mathcal{D}_m$ and $\mathcal{S}_n$ were isomorphic, then any $\pi \in \mathcal{S}_n$ with order k would correspond with a unique $\sigma \in \mathcal{D}_m$, also with order k; specifically, elements with order 3 in $\mathcal{S}_n$ would have to map to unique elements of order 3 in $\mathcal{D}_m$. However, there are more elements with order 3 in $\mathcal{S}_n$ than there are in $\mathcal{D}_m$; hence no such isomorphism exists between the two sets.

(f) In $\mathcal{Q}$, there are 6 elements with order 4: $\pm i$, $\pm j$, and $\pm k$; and 1 element with order 2: -1. However, in $\mathcal{D}_4$, there are only 2 elements with order 4: r_1 and r_3; and 5 with order 2: all flips, and r_2. Thus, since the number of elements with order 2 and order 4 are different, by Lemma 3 they cannot be isomorphic.

Problem §2 (2.28) Consider the dihedral group $\mathcal{D}_4 = \{e, \rho_1, \rho_2, \rho_3, \phi_1, \phi_2, \phi_3, \phi_4\}$ and the quaternion group $\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$. For each of the following groups and subgroups, explicitly write down the cosets.

(a) $G = \mathcal{D}_4, \ H = \{e, \phi_1\}$

(b) $G = \mathcal{D}_4, \ H = \{e, \phi_1, \phi_2, phi_3\}$

(c) $G = \mathcal{D}_4$, $H = \{e, \phi_2\}$

(d) $G = \mathcal{Q}$, $H = \{\pm 1\}$

(e) $G = \mathcal{Q}$, $H = \{\pm 1, \pm i\}$

Solution:

(a)

$$\begin{aligned} eH &= \{e,\phi_1\} & \rho_1 H &= \{\rho_1,\phi_2\} & \rho_2 H &= \{\rho_2,\phi_3\} & \rho_3 H &= \{\rho_3,\phi_4\} \\ \phi_1 H &= \{\phi_1, e\} & \phi_2 H &= \{\phi_2,\rho_1\} & \phi_3 H &= \{\phi_3,\rho_2\} & \phi_4 H &= \{\phi 4,\rho_3\}. \end{aligned}$$

(b)

$$\begin{aligned} eH &= \{e,\rho_1,\rho_2,\rho_3\} & \rho_1 H &= \{\rho_1,\rho_2,\rho_3,e\} & \rho_2 H &= \{\rho_2,\rho_3,e,\rho_1\} & \rho_3 H &= \{\rho_3,e,\rho_1,\rho_2\} \\ \phi_1 H &= \{\phi_1,\phi_4,\phi_3,\phi_2\} & \phi_2 H &= \{\phi_2,\phi_1,\phi_4,\phi_3\} & \phi_3 H &= \{\phi_3,\phi_2,\phi_1,\phi_4\} & \phi_4 H &= \{\phi_4,\phi_3,\phi_2,\phi_1\}. \end{aligned}$$

(c)

$$\begin{aligned} eH &= \{e,\rho_2\} & \rho_1 H &= \{\rho_1,\rho_3\} & \rho_2 H &= \{\rho_2,e\} & \rho_3 H &= \{\rho_3,\rho_1\} \\ \phi_1 H &= \{\phi_1,\phi_3\} & \phi_2 H &= \{\phi_2,\phi_4\} & \phi_3 H &= \{\phi_3,\phi_1\} & \phi_4 H &= \{\phi_4,\phi_2\}. \end{aligned}$$

(d)

$$\begin{aligned} 1H &= \{\pm 1\} & -1H &= \{\pm 1\} & iH &= \{\pm i\} & -iH &= \{\pm i\} \\ jH &= \{\pm j\} & -jH &= \{\pm j\} & kH &= \{\pm k\} & -kH &= \{\pm k\}. \end{aligned}$$

(e)

$$\begin{aligned} 1H &= \{\pm 1,\pm i\} & -1H &= \{\pm 1,\pm i\} & iH &= \{\pm i,\pm 1\} & -iH &= \{\pm i,\pm 1\} \\ jH &= \{\pm j,\pm k\} & -jH &= \{\pm j,\pm k\} & kH &= \{\pm k,\pm j\} & -kH &= \{\pm k,\pm j\}. \end{aligned}$$

Problem §3
(2.31) Let G be a group. The **center** of G is defined

$$Z(G) = \{g \in G \mid gg' = g'g \text{ for every } g' \in G\}.$$

(a) Prove that $Z(G)$ is a subgroup of G.

(b) When does $Z(G)$ equal G?

(c) Compute the center of the symmetric group $\mathcal{S}_n$.

(d) Compute the center of the dihedral group $\mathcal{D}_n$.

(e) Compute the center of the quaternion group $\mathcal{Q}$.

(2.34) Let G be a finite group whose only subgroups are $\{e\}$ and G. Prove that either $G = \{e\}$, or G is a cyclic group whose order is prime.

Solution:

(2.31)

(a) Let $g_1, g_2 \in Z(G)$. Then for any $g' \in G$, we have

$$g'(g_1g_2) = (g'g_1)g_2 = (g_1g')g_2 = g_1(g'g_2) = g_1(g_2g') = g_1g_2g'.$$

Hence g_1g_2 commutes with every $g' \in G$, and so $g_1g_2 \in Z(G)$.
By definition, $e \in Z(G)$.
Let $g \in Z(G)$. Then $gg' = g'g$ for any $g' \in G$. From this, we get

$$\begin{aligned} gg' &= g'g \\ g^{-1}gg' &= g^{-1}g'g \\ g' &= g^{-1}g'g \\ g'g^{-1} &= g^{-1}g'gg^{-1} \\ g'g^{-1} &= g^{-1}g'. \end{aligned}$$

Hence for any $g \in Z(G)$, $g^{-1} \in Z(G)$.

Therefore $Z(G)$ is a subgroup of G.

(b) Suppose $Z(G) = G$. Then for any $g \in Z(G)$, $g \in G$. Additionally, for every $g \in Z(G)$, $gg' = g'g$ for any $g' \in G$. Thus if $Z(G) = G$, by definition G is an Abelian group. (If G is cyclic, $Z(G) = G$ as well; but all cyclic groups are Abelian).

(c) $Z(\mathcal{S}_n) = \{e\}$; in other words, $\mathcal{S}_n$ has a trivial center.

Proof. Consider the set of bijective permutations $\prod$, where for some $\pi_j \in \prod$,

$$\pi_j(i) = \begin{cases} i & i = j \\ k \text{ (for some } k \neq i) & i \neq j \end{cases}, i, j, k \in \{1, 2, \ldots, n\}$$

Let $\pi_i \in \prod$, $i \in \{1, \ldots, n\}$, and consider any permutation π not in $\prod$ (except e). Suppose $\pi(i) = j$ for some $j \in \{1, \ldots, n\}$, and let k be some number in $\{1, \ldots, n\}$ such that $\pi_i(j) = k$. Then

$$\pi_i \circ \pi(i) = \pi_i(j) = k,$$

while

$$\pi \circ \pi_i(i) = \pi(i) = j.$$

Hence $\pi_i\pi \neq \pi\pi_i$, and so any $\pi \notin \prod$ (except obviously e) does not commute with any $\pi_i \in \prod$.

Since for any $n \geq 3$, there exists some non-trivial $\pi_i \in \prod$, and some non-trivial $\pi \notin \prod$, the only element that commutes with every $pi \in \mathcal{S}_n$ is e; therefore $Z(\mathcal{S}_n) = \{e\}$. □

(d) For odd $n \geq 3$, $Z(\mathcal{D}_n) = \{e\}$; for even $n \geq 3$, $Z(\mathcal{D}_n) = \{e, r_{\frac{n}{2}}\}$, where $r_{\frac{n}{2}}$ is the half (180°) rotation.

Proof. Recall (from my problem set 2) that $V_n = \{0, \ldots, n-1\}$, arithmetic is defined modulo n, a rotation $r_j \in \mathcal{D}_n$ is defined

$$r_j(i) = i + j,\ j \in V_n,$$

a flip is defined

$$f_j(i) = n - i + j,\ j \in V_n,$$

and $\mathcal{D}_n$ is composed entirely of rotations and flips; that is,

$$\mathcal{D}_n = \{\sigma \mid \sigma = r_1^j f_0^k,\ j \in V_n,\ k \in \{0, 1\}\}.$$

From this, we see three things:

- f_j has order 2 (and so $f_j = f_j^{-1}$): $f_j(f_j(i)) = f_j(n - i + j) = n - (n - i + j) + j = i$.

- $r_j^{-1} = r_{n-j}$: $r_{n-j}(r_j(i)) = r_{n-j}(i+j) = i+j+n-j = i+n = i$, and $r_j(r_{n-j})(i) = r_j(i+n-j) = i+n-j+j = i+n = i$.
- $f_j r_i f_j = r_i^{-1}$: $f_j(r_i(f_j(k))) = f_j(r_i(n-k+j)) = f_j(n-k+j+i) = n-(n-k+j+i)+j = n-n+k-i-j+j = k-i = k+(n-i) = r_i^{-1}(k)$.

Now, observe that any rotation commutes with another rotation, and not every flip commutes with every other flip. Thus, any center must be a rotation that commutes with every flip (because then the rotation commutes with all rotations and all flips); in other words, for $r_j \in \mathcal{D}_n$, we must have $r_j f = f r_j$ for some flip f. From above, we have

$$\begin{aligned} f r_j f &= r_j^{-1} \\ f f r_j f &= f r_j^{-1} \\ r_j f &= f r_j^{-1}. \end{aligned}$$

Thus r_j commutes with any f if $r_j = r_j^{-1}$. We know that $r_j^{-1} = r_{n-j}$; thus $r_j = r_{n-j}$ requires $j = n-j$, or equivalently $j = \frac{n}{2}$. For odd n, this is not closed in $\mathbb{Z}$; thus $r_{\frac{n}{2}} \in \mathcal{D}_n$ only if n is even.

By definition, e commutes with every element in $\mathcal{D}_n$. Therefore, $Z(\mathcal{D}_n) = \{e\}$ when n is odd, and $Z(\mathcal{D}_n) = \{e, r_{\frac{n}{2}}\}$ when n is even. $\square$

(e) From the definition of the quaternion group $\mathcal{Q}$, one can clearly see that none of i, j, k commute ($ij = k \neq -k = ij$, $jk = i \neq -i = kj$, etc.), while ± 1 do commute (1 is the identity, and for any $a \in \{i, j, k\}$, $-1 \cdot a = -a = a \cdot -1$); hence $Z(\mathcal{Q}) = \{\pm 1\}$.

(2.34) We start with two lemmas: