Problem §1 (2.2) Let G be the group of permutations on $S = \{1, 2, \dots, n\}$. Prove that G is a finite group, and give a formula for the order of G.

Then, let P_n be a regular n-gon with n vertices $1, 2, \dots, n$. Show that the map $\phi : \mathcal{D}_n \to \mathcal{S}_n$, that sends each element of the dihedral group $\mathcal{D}_n$ to the permutation of the corresponding vertices, is a homomorphism. Is ϕ injective? Surjective?

Solution: We first observe that G is a group (by definition). A valid permutation of a set $S = \{1, 2, \dots, n\}$ is a bijective function $\pi : S \to S$ that assigns every $s \in S$ to another $s' \in S$ (not necessarily distinct). We observe that there are n ways to assign one element (say, without loss of generality, $1 \in S$): it can be assigned to some $i \in \{1, 2, \dots, n\}$. Then, there are $n - 1$ ways to assign another element (say, without loss of generality again, $2 \in S$); it can be assigned to some $j \in \{1, 2, \dots, n\} \setminus \{i\}$. This process repeats until the last element (e.g. n), which can only be assigned to one possible $k \in S \setminus \underbrace{\{i, \dots, j\}}_{n-1 \text{ elements of } S}$. In other words, there are

$$n \cdot (n - 1) \cdot \ldots \cdot 1 = n!$$

possible unique permutations of S. Hence G is a finite group of order $n!$.

Now, let P_n be the regular n-gon with vertices $N = 1, 2, \dots, n$. Let $\sigma \in \mathcal{D}_n$, and let $\phi(\sigma) = \pi$ map every σ to its corresponding permutation $\pi \in \mathcal{S}_n$; that is, for every $i \in N$, we have $\sigma(i) = \pi(i)$.
Let $\sigma_1, \sigma_2 \in \mathcal{D}_n$. Then $\phi(\sigma_1 \circ \sigma_2) = \pi$ for some $\pi \in \mathcal{S}_n$ such that $\pi(i) = \sigma_1 \circ \sigma_2(i)$ for every $i \in N$. But since every $\sigma_j \in \mathcal{D}_n$ corresponds to some $\phi(\sigma_j) = \pi_j \in \mathcal{S}_n$ where $\sigma_j(i) = \pi_j(i)$, $\forall i \in N$, we can deconstruct π into $\pi_1 \circ \pi_2$, where $\pi_1 = \sigma_1$ and $\pi_2 = \sigma_2$. Then

$$\phi(\sigma_1 \circ \sigma_2) = \pi = \pi_1 \circ \pi_2 = \phi(\sigma_1) \circ \phi(\sigma_2), .$$

and so ϕ is a homomorphism.

For all $n \in \mathbb{N}$, $\phi : \mathcal{D}_n \to \mathcal{S}_n$ is injective, since every unique permutation σ on vertices $1, \dots, n$ corresponds to only one unique permutation π of $\{1, \dots, n\}$; namely, $\sigma(i) = \pi(i)$ for every $i \in \{1, \dots, n\}$. Formally, suppose $\pi_1 = \phi(\sigma_1)$, $\pi_2 = \phi(\sigma_2) \in \mathcal{S}_n$ and $\pi_1(i) = \pi_2(i)$, $\forall i \in \{1, \dots, n\}$. Then $\sigma(i) = \phi(\sigma)(i) = \pi(i)$ for any $\sigma \in \mathcal{D}_n$, so $\sigma_1(i) = \sigma_2(i)$, or equivalently, $\sigma_1 = \sigma_2$. Hence ϕ is injective.
ϕ is surjective only for $n \in \{1, 2, 3\}$. From Exercise 1.16, we know that ϕ injective implies ϕ surjective if

$$|\mathcal{D}_n| = |\mathcal{S}_n|\,;$$

and for $n = \{1, 2, 3\}$, the above property holds ($|\mathcal{D}_n| = |\mathcal{S}_n| = 1, 2, 6$ for $1, 2, 3$ respectively; for $n = 1, 2$, the flips and rotations yield the same permutation). However, for any $n > 3$, ϕ is not surjective. There does not exist a $\sigma \in \mathcal{D}_n$ that fixes two vertices and rotates the rest, i.e.:

$$\sigma(1) = 1, \sigma(2) = 2, \sigma(i) = i + 1 \text{ for } 2 < i < n, \sigma(n) = 3;$$

hence $|\mathcal{S}_n| > |\mathcal{D}_n|$, and surjectivity fails.
Thus ϕ is bijective for $n \in \{1, 2, 3\}$, and injective only for all $n > 3$.

Problem §2 WIP

Solution: WIP

Problem §3 (2.11) Prove that the dihedral group $\mathcal{D}_n$ has exactly $2n$ elements.

Solution: We start with a few notational adjustments. For this problem, we "zero-index" the set of n numbers $1, 2, \dots, n$; that is, instead of $\{1, 2, \dots, n\}$, we write $\{0, 1, \dots, n - 1\}$. We denote this

$$V_n = \{0, 1, \dots, n - 1\}.$$

Further, we use modular arithmetic: for $a, b \in V_n$, $a \pm b$ becomes $a \pm b \mod n$.
Finally, we define $\mathcal{P}_n$ as the regular n-gon with vertices $(0, 1, \ldots, n-1)$ [an ordered n-tuple].

We define the set of all valid permutations on an n-gon P_n as the $n^{\mathbf{th}}$ **dihedral group**, or $\mathcal{D}_n$. Roughly, we get the intuition that any permutation of vertices $\sigma \in \mathcal{D}_n$ is valid only if it "preserves geometric structure;" for example, given a square, rotating the square by 90° or reflecting it horizontally preserves structure, but fixing two vertices and swapping the other two "breaks" the structure.

Formally, we define a permutation $\sigma \in \mathcal{D}_n$ (σ is a valid permutation of $\mathcal{P}_n$) if, for any $i \in V_n$,

$$\sigma(i) = j \text{ implies } \sigma(i \pm 1) = j \pm 1 \text{ or } j \mp 1 \text{ for some } j \in V_n.$$

In other words, the permutation must maintain the adjacent vertices of any vertex, either in original or reverse order.

Now, we define a rotation r_i, $i \in \mathbb{Z}_{\geq 0}$, as

$$r_i(j) = j + i, \ \forall j \in V_n.$$

So, for a square with vertices $\{0, 1, 2, 3\}$, $r_1(0) = 1,\ r_1(1) = 2,\ r_1(2) = 3,\ r_1(3) = 0$ (note the modulo). It is clear that $r_i \in \mathcal{D}_n$, as $\forall j \in V_n$,

$$r_i(j-1) = (j+i) - 1,\ r_i(j) = (j+i),\ r_i(j+1) = (j+i) + 1.$$

Additionally, we define a flip f_i, $i \in \mathbb{Z}_{\geq 0}$, as

$$f_i(j) = n - j + i, \ \forall j \in V_n.$$

So, for a square, $f_0(0) = 0 (n \mod n \equiv 0),\ f_0(1) = 3,\ f_0(2) = 2,\ f_0(3) = 1$. Similarly, it is clear that $f_i \in \mathcal{D}_n$, as $\forall j \in V_n$,

$$f_i(j-1) = (n-j+i) + 1,\ f_i(j) = (n-j+i),\ f_i(j+1) = (n-j+i) - 1.$$

Now, we make two observations about rotations and flips:

1. For every $i \in V_n$, r_i can be formed by raising r_1 to some power:

   $$r_i(j) = j + i = j + \underbrace{1 + \ldots + 1}_{i \text{ times}} = r_1(j) + \underbrace{1 + \ldots + 1}_{i-1 \text{ times}} = \ldots = (\underbrace{r_1 \circ \ldots \circ r_1}_{i \text{ times}})(j) = r_1^i(j).$$

   [for $i = 0$, $r_1^0(j) = r_0(j) = j$].

   Moreover, any r_k for $k \geq n$ is identical to r_i, where $i = k \mod n = k - n \in V_n$:

   $$r_k(j) = j + k \equiv j + k \mod n = j + (k - n) = r_j(j).$$

   Thus, there are n **unique rotations in** $\mathcal{D}_n$.

2. Similarly, for every $i \in V_n$, f_i can be formed by composing f_0 with some power (specifically, i) of r_1 (that is, $f_i = r_0^i \circ f_0$):

   $$f_i(j) = n - j + i = n - j + \underbrace{1 + \ldots + 1}_{i \text{ times}} = (\underbrace{r_1 \circ \ldots \circ r_1}_{i \text{ times}})(f_0)(j) = r_1^i \circ f_0(j),$$

   and like rotations, any f_k for $k \geq n$ is identical to f_i, where $i = k \mod n = k - n \in V_n$:

   $$f_k(j) = n - j + k \equiv n - j + k \mod n = n - j + (k - n) = n - j + i = f_i(j).$$

   Thus, there are n **unique flips in** $\mathcal{D}_n$.

From this, we get that $\mathcal{D}_n$ has at least $2n$ elements: n rotations and n flips. Now, it remains to show that

$$D_n = \{\sigma \mid \sigma = r_1^i \circ f_0^j, i \in V_n, j \in \{0,1\}\};$$

that is, the entire group $\mathcal{D}_n$ consists of those $2n$ rotations and flips.

Let $\sigma \in \mathcal{D}_n$. Then for $\sigma(i) = j$, where $i, j \in V_n$,

$$\sigma(i \pm 1) = j \pm 1, \text{ or } \sigma(i \pm 1) = j \mp 1.$$

If $\sigma(i \pm 1) = j \pm 1$, let $k = j - i \in V_n$ (if $i \geq j$, recall modular arithmetic; $k = j - i \mod n = n + j - i \in V_n$). Then

$$r_1^k(i \pm 1) = r_k(i \pm 1) = (i \pm 1) + k = (i \pm 1) + j - i = j \pm 1 = \sigma(i \pm 1),$$

and so $\sigma = r_k = r_1^k \circ f_0^0$ (no flip).
Alternatively, if $\sigma(i \pm 1) = j \mp 1$, let $k = j + i \in V_n$ (again, if $j + i \geq n$, we have $k = j + i - n \in V_n$). Then

$$r_1^k \circ f_0^1(i \pm 1) = r_k \circ f_0(i \pm 1) = r_k(n - (i \pm 1) + 0) = r_k(n - i \mp 1) = (n - i \mp 1) + k = (n - i \mp 1) + j + i = n + j \mp 1 \equiv j \mp 1 = \sigma(i \pm 1),$$

and so $\sigma = r_k \circ f_0 = r_1^k \circ f_0^1$.

Thus, if $\sigma \in \mathcal{D}_n$, then σ is either a rotation ($r_k = r_1^k = r_1^k \circ f_0^0$) or a flip ($f_k = r_1^k \circ f_0^1$). Hence, the entire group $\mathcal{D}_n$ consists of only the unique rotations and flips, and so $\mathcal{D}_n$ has order $2n$.