Problem §1 (2.2) Let G be the group of permutations on $S = \{1, 2, \ldots, n\}$. 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 $1, 2, \ldots, n$. 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 $S = \{1, 2, \ldots, n\}$ 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 $i \in \{1, 2, \ldots, n\}$. 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 $j \in \{1, 2, \ldots, n\} \setminus \{i\}$. This process repeats until the last element (e.g. n), which can only be assigned to one possible $k \in S \setminus \underbrace{\{i, \ldots, j\}}_{n-1 \text{ elements of } S}$. 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 $N = 1, 2, \ldots, n$. 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 $1, \ldots, n$ corresponds to only one unique permutation π of $\{1, \ldots, n\}$; namely, $\sigma(i) = \pi(i)$ for every $i \in \{1, \ldots, n\}$. Formally, suppose $\pi_1 = \phi(\sigma_1)$, $\pi_2 = \phi(\sigma_2) \in \mathcal{S}_n$ and $\pi_1(i) = \pi_2(i)$, $\forall i \in \{1, \ldots, n\}$. 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 (2.6) Let G be a group, and let $g, h \in G$, and suppose g has order n, and h has order m.

(a) If G is an Abelian group and $\gcd(m, n) = 1$, prove that the order of gh is mn.

(b) Give an example showing (a) need not be true if $\gcd(m, n) > 1$.

(c) Give an example of a non-Abelian group showing (a) need not be true even if $\gcd(m, n) = 1$.

Solution:

(a) We start with an observation, and a lemma.
Observation: For any $a, b \in G$, $a \cdot b = e$ only when $b = a^{-1}$ or $a = b = e$.

Lemma 1 (Order of Inverse). *Let G be a group, and let $g \in G$. Then $|g| = \left|g^{-1}\right|$.*

Proof. Let $|g| = n$; then $g^n = e$. From this, we get

$$e = \left(g \cdot g^{-1}\right)^n = g^n \cdot (g^{-1})^n = e \cdot (g^{-1})^n,$$

and so $(g^{-1})^n = e$ (g and g^{-1} commute, even if G is non-Abelian).
Now, we show that $\left|g^{-1}\right| = n$. Suppose $\left|g^{-1}\right| = m$,and $m < n$. Then

$$e = g^n \cdot (g^{-1})^m = (g \cdot g^{-1})^m \cdot g^{n-m} = g^{n-m}.$$

But we know that $|g| = n$, or equivalently, n is the smallest positive integer such that $g^n = e$; hence $g^{n-m} = e$ is a contradiction. Thus $m = n$, and so $\left|g^{-1}\right| = n$. $\square$

Now, let G be an Abelian group, and let $g, h \in G$, with $|g|$ and $|h|$ relatively prime, and let $|gh| = k$. By the lemma, we know that $h \neq g^{-1}$ (otherwise, the orders of g and h would not be relatively prime); hence $k \neq 1$. By the observation, $(gh)^k = g^k \cdot h^k = e$ only when $g^k = e,\ h^k = e$.

Thus, we know that n divides k, and m divides k (Proposition 2.9). Thus k is the smallest positive integer such that $n|k$ and $m|k$; in other words, $k = \text{lcm}\,(m, n)$. But by definition, $\text{lcm}\,(m, n) = \frac{mn}{\gcd\,(m,n)}$, and so $k = \frac{mn}{\gcd\,(m,n)} = mn$.

(b) Consider the group $\mathbb{Z}/3\mathbb{Z}$ with elements $\{0, 1, 2\}$ under addition. Consider elements 1 and 2 ; $|1| = |2|$; so $\gcd\,(2, 2) = 2$. But $(1 + 2)^1 = 0 = e$, so $|1 + 2| = 1 \neq 2 \cdot 2$.

(c) Consider the group $\mathcal{D}_3$, and consider elements r_1 and f_2 (r_1 rotates all vertices by 1, and f_2 flips across the second vertex, i.e. $f(1) = 3,\ f(2) = 2,\ f(3) = 1$.) $|r_1| = 3,\ |f_2| = 2$; so $\gcd\,(2, 3) = 1$. But $(r_1 \circ f_2)^2 = e$:

$$(r_1 \circ f_2)(1) = 1,\ (r_1 \circ f_2)(2) = 3,\ (r_1 \circ f_2)(3) = 2;$$

so

$$(r_1 \circ f_2)^2(1) = 1,\ (r_1 \circ f_2)^2(2) = 2,\ (r_1 \circ f_2)^2(3) = 3$$

and thus $|r_1 \circ f_2| = 2 \neq 2 \cdot 3$.

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 $1, 2, \ldots, n$; that is, instead of $\{1, 2, \ldots, n\}$, we write $\{0, 1, \ldots, n-1\}$. We denote this

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

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 $n^{\textbf{th}}$ **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 $2n$.

Problem §4 (2.14)

(a) Let
$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\},$$
with composition law being matrix multiplication. Show that $\mathrm{GL}_2(\mathbb{R})$ is a group.

(b) Let
$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R}, ad-bc = 1 \right\},$$
with composition law being matrix multiplication again. Show that $\mathrm{SL}_2(\mathbb{R})$ is a group.

(c) Fix an integer $n \geq 1$. Generalize (a) and (b) by proving that each of

- $\mathrm{GL}_n(\mathbb{R}) = \{\text{set of all } n\text{-by-}n \text{ matrices } A \text{ such that } \det(A) \neq 0\}$
- $\mathrm{SL}_n(\mathbb{R}) = \{\text{set of all } n\text{-by-}n \text{ matrices } A \text{ such that } \det(A) = 1\}$

is a group under matrix multiplication.

Solution: For all parts, recall that $\det(AB) = \det(A)\det(B)$ for any n-by-n matrices A, B; a useful corollary is that $\det(A^{-1}) = \frac{1}{\det(A)}$.

(a)
- Associativity: Let $A, B, C \in \mathrm{GL}_2(\mathbb{R})$. We know from standard linear algebra that matrix multiplication is associative; hence
$$A(BC) = (AB)C.$$
- Identity: Choose $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then for every $A \in \mathrm{GL}_2(\mathbb{R})$, we have $AI = IA = A$.
- Inverse: For every $A \in \mathrm{GL}_2(\mathbb{R})$, choose $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then $AA^{-1} = A^{-1}A = I$. (We know A^{-1} exists since $\det(A) \neq 0$ by definition).

Thus $\mathrm{GL}_2(\mathbb{R})$ is a group.

(b)
- Associativity: again, we know from standard linear algebra that given any n-by-n matrices A, B, C, we have
$$A(BC) = (AB)C.$$
- Identity: we again choose $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then for every $A \in \mathrm{SL}_2(\mathbb{R})$, we have $AI = IA = A$.
- Inverse: For every $A \in \mathrm{SL}_2(\mathbb{R})$, choose $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ (since $\det(A) = 1$, A is invertible and $\frac{1}{\det(A)} = 1$). Then $AA^{-1} = A^{-1}A = I$.

Thus $SL_2(\mathbb{R})$ is a group.

(c) Fix an integer $n \geq 1$. Define $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$; that is, for any a_{ij}, $a_{ij} = 1$ if $i = j$, 0 otherwise.

The proofs that $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{R})$ are groups are essentially identical:

- Associativity: from standard linear algebra, given any n-by-n matrices A, B, C, we have
$$A(BC) = (AB)C.$$

- Identity: Choose I_n. Then for any $A \in \mathrm{GL}_n(\mathbb{R})$ and $B \in \mathrm{SL}_n(\mathbb{R})$, we have $AI = IA = A$ and $BI = IB = B$ from standard linear algebra.
- Inverse: For any $A \in \mathrm{GL}_n(\mathbb{R})$ and $B \in \mathrm{SL}_n(\mathbb{R})$, we know that $\det(A) \neq 0$, and $\det(B) = 1 \neq 0$. Thus their inverses exist (from standard linear algebra, a matrix is invertible iff its determinant is non-zero), and we choose $A^{-1} \in \mathrm{GL}_n(\mathbb{R})$, $B^{-1} \in \mathrm{SL}_n(\mathbb{R})$. Then $AA^{-1} = A^{-1}A = I_n$, and $BB^{-1} = B^{-1}B = I_n$.

Thus both $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{R})$ are groups.

Problem §5 (2.15) Prove or disprove whether each of the following subsets of $\mathrm{GL}_2(\mathbb{R})$ is a group (and explain why).

(a) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid ad - bc = 2 \right\}$

(b) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid ad - bc \in \{-1, 1\} \right\}$

(c) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid c = 0 \right\}$

(d) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid d = 0 \right\}$

(e) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid a = d = 1,\ c = 0 \right\}$

Solution:

(a) This is not a group.

- Closure does not hold: for $A, B \in S$, we have $\det(AB) = \det(A)\det(B) = 2 \cdot 2 = 4$, and so $AB \notin S$.
- $\det(I) = 1 \neq 2$, so $I \notin S$.
- Recall that $\det(A^{-1}) = \frac{1}{\det(A)}$; thus given an $A \in S$, $\det(A^{-1}) = \frac{1}{2}$, so $A^{-1} \notin S$.

(b) This is a group.

- Let $A, B \in S$. Then $\det(A), \det(B) \in \{-1, 1\}$. So, $\det(AB) = \det(A)\det(B) \in \{-1, 1\}$ (any combination of $1 \cdot 1,\ 1 \cdot -1, -1 \cdot -1$ is in $\{-1, 1\}$). Thus $AB \in S$.
- $det(I) = 1 \in \{-1, 1\}$. Thus $I \in S$.
- Let $A \in S$. Then $\det(A) \in \{-1, 1\}$. Recall that $\det(A^{-1}) = \frac{1}{\det(A)}$; thus $\det(A^{-1}) = \frac{1}{1 \text{ or } -1} \in \{-1, 1\}$, and so $A^{-1} \in S$.

(c) This is a group.

- Let $A, B \in S$, where $A = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$. Then

$$A \cdot B = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \in S.$$

  Thus $AB \in S$.
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is clearly in S.

- Let $A \in S$, where $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Choose $A^{-1} = \frac{1}{ad}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$. A^{-1} is clearly the inverse of A:

$$A \cdot A^{-1} = \frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \frac{1}{ad}\begin{pmatrix} ad & ab - ab \\ 0 & ad \end{pmatrix} = I;$$

  Moreover, $A^{-1} \in S$, as $c = 0$.

(d) This is not a group.

- Closure does not hold: Let $A, B \in S$, where $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & 0 \end{pmatrix}$. Then

$$AB = \begin{pmatrix} a_1 & b_1 \\ c_1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & 0 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 \\ a_2c_1 + c_1c_2 & b_2c_1 \end{pmatrix} \notin S.$$

- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$, as $d \neq 0$.
- Let $A \in S$, where $A = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$. $A^{-1} = \frac{1}{0-bc}\begin{pmatrix} 0 & -b \\ -c & a \end{pmatrix}$ is not in S, as $d = a \neq 0$ necessarily.

(e) This is a group.

- Let $A, B \in S$, where $A = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}$. Then

$$A \cdot B = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix} \in S.$$

  Thus $AB \in S$.
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$, as $a = d = 1,\ c = 0$.
- For any $A \in S$, where $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, we have $A^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$. Clearly $A \cdot A^{-1} = I$, and $A^{-1} \in S$.