P1

Determine the order of each of the elements of the dihedral group D_8.

Since

$$\begin{aligned} D_8 &= \langle r, s \mid r^4 = s^2 = e, rs = sr^{-1} \rangle \\ &= \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}. \end{aligned} \tag{1}$$

Using

$$| r^k | = \frac{n}{\gcd(n, k)} = \frac{4}{\gcd(4, k)}, \tag{2}$$

and the fact that any reflection $r^k s$ is of order 2, since

$$\left(r^k s\right)^2 = r^k s r^k s = r^k r^{-k} s^2 = e, \tag{3}$$

we have:

$$\begin{gathered} |e| = 1, \\ |r| = 4, |r^2 | = 2, |r^3| = 4, \\ |s| = | rs | = | r^2 s | = | r^3 s | = 2. \end{gathered} \tag{4}$$

P2

Suppose for some $n \geq 3$ that $z \in D_{2n}$is a non-identity element s.t. $zg = gz$ for all $g \in D_{2n}$. Prove that n is even ($n = 2k$), and $z = r^k$ where r is order-n generator of $D_{2n.}$

Any element in D_{2n} is either a rotation r^a or a reflection $r^a s$ for some integer a.

- Suppose $z = r^a s$ is a reflection, m$zr = rz$. Then,

$$\begin{aligned} zr &= (r^a s)r = r^{a-1} rsr = r^{a-1} s \\ rz &= r(r^a s) = r\left(r^{a-1} s r^{-1}\right) = r^a s r^{-1} = r^{a+1} s. \end{aligned} \tag{5}$$

To have $zr = rz$, we must have $r^{a-1} s = r^{a+1} s$, which implies $r^2 = e$. This contradicts the assumption that $n \geq 3$. Thus, z must be a rotation.

- Now, consider $a \in \{1, 2, ..., n-1\}$, $z = r^a \neq e$.

Commutativity gives

$$\begin{gathered} zr = rz \Rightarrow r^{a+1} = r^{a+1}, \text{ tautology.} \\ sz = zs \Rightarrow sr^a = r^a s = r^{-a} s \end{gathered} \tag{6}$$

$$\begin{gathered} \Rightarrow r^a s = r^{-a} s \\ \Rightarrow r^a = r^{-a} \\ \Rightarrow r^{2a} = e. \end{gathered} \tag{7}$$

Since the order of r is n, we must have $n \mid 2a \Rightarrow 0 < 2a < 2n$. Since $z = r^a \neq e$, n does not divide a.

Thus, the only possibility is $2a = n$. Writing $n = 2k$, we have $a = k$ and $z = r^k$. ∎

P3

a. Prove that every element of D_{2n} which is not a power of r has order 2.
As proved in P1: For any reflection $r^k s$,

$$\left(r^k s\right)^2 = r^k s r^k s = r^k r^{-k} s^2 = e. \tag{8}$$

b.Deduce that D_{2n} is generated by s, sr , both of which have order 2.
Consider $(sr)^2 = srsr = ssr^{-1}r = ss = e$, and $s^2 = e$. Thus, both s and sr are of order 2.

Since $rs = sr^{-1} \Rightarrow r = s(sr)$.
Let $H = \langle s, sr \rangle$, then $r = s(sr) \in H, s \in H$. Thus H contains both generators of D_{2n}. But $\langle r, s \rangle = D_{2n} \Rightarrow H \subseteq D_{2n}$.
This implies $D_{2n} = H = \langle s, sr \rangle$. ■

c. Show $\langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s, b = sr$.
First, let $a := s, b := sr$. Then, using the definition for s, r :

$$\begin{gathered} a^2 = s^2 = e; \quad b^2 = (sr)^2 = srsr = ssr^{-1}r = e; \\ (ab)^n = (s(sr))^n = r^n = e. \end{gathered} \tag{9}$$

Thus the relation of a, b follows from that of s, r.

Conversely, let $s := a, r := ab$. Then, using the definition for a, b :

$$s^2 = a^2 = e; \quad r^n = (ab)^n = e; \tag{10}$$

and since $a^2 = e \Rightarrow a^{-1} = a; b^2 = e \Rightarrow b^{-1} = b, \wedge$

$$rs = (ab)a = a(ba) = a(ab)^{-1} = sr^{-1}. \tag{11}$$

Thus the relation of s, r follows from that of a, b. This shows the two presentations are equivalent. ■

P4

Prove that the group of rigid motions of a regular tetrahedron in R^3 has order 12, and that the group of rigid motions of a regular octahedron in R^3 has order 24.

- A tetrahedron has 4 vertices, which we label form 1 to 4. A rigid motion in G sents vertex 1 to four possible locations. Afterwhich, there are three possible locations for vertex 2, and then the location of the remaining two vertices are determined. Thus, by the multiplication principle, $|G| = 4 \times 3 = 12$.
- An octahedron has 6 vertices, from which we label from 1 to 6. A rigid motion in G sents vertex 1 to six possible locations. Afterwhich, there are four possible locations for vertex 2, and then the location of the remaining four vertices are determined. Thus, by the multiplication principle, $|G| = 6 \times 4 = 24$.

P5

Prove that if $\Omega = \mathbb{N}$,then the group S_Ω is infinite.

Let $\Omega = \{1, 2, 3, ...\}$ and let S_Ω be the group of all bijections $\Omega \to \Omega$ under composition.

For each $n \geq 1$, define $\sigma_n \in S_\Omega$ by:
- $\sigma_{n(2n-1)} = 2n, \quad \sigma_{n(2n)} = 2n - 1,$
- $\sigma_{n(k)} = k \forall k \neq 2n - 1, 2n.$

Thus σ_n is the transposition $(2n - 1, 2n)$, hence a bijection, so $\sigma_n \in S_\Omega$.

If $i \neq j$, then $\{2i - 1, 2i\}$ and $\{2j - 1, 2j\}$ are disjoint, and in particular:

$$\sigma_{i(2i-1)} = 2i = .\neg 2i - 1 = \sigma_{j(2i-1)}, \tag{12}$$

so $\sigma_i \neq \sigma_j$.

Therefore the set $\{\sigma_1, \sigma_2, ...\}$ gives infinitely many distinct elements of S_Ω, and S_Ω is infinite.

P6

It is clear, by observation, that

$$\begin{aligned} \sigma &= (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) \\ \tau &= (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11) \end{aligned} \tag{13}$$

and so

$$\begin{aligned} \sigma\tau &= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7 10\ 15)(13\ 14)\} \\ \tau\sigma &= (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)\} \end{aligned} \tag{14}$$

$$\begin{aligned} |\sigma| = \operatorname{lcm}(4,3,6) = 12; |\tau| = \operatorname{lcm}(2,5,2,3,2) = 30; \\ |\sigma\tau| = \operatorname{lcm}(3,2,6,2) = 6; |\tau\sigma| = \operatorname{lcm}(2,2,6,3) = 6. \end{aligned} \tag{15}$$

P7

Let a be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is a^i also a 12-cycle?

Since a is of order 12,

$$\left|a^i\right| = \frac{12}{\gcd(12, i)}. \tag{16}$$

Then, to enforce $\left|a^i\right| = 12$, we need $\gcd(12, i) = 1$, that is, $i \in \{1, 5, 7, 11\}$.

P8

Prove that if a is the m-cycle $(a_1\ a_2\ ...a_m)$, then for all $i \in \{1, 2, ..., m\}$, $a^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue modulo m when $k + i > m$. Deduce that $|a| = m$.

1. Use induction to prove $a^i(a_k) = a_{k+1} \forall i \in \{1, ..., m\}$.

- Base case: By definition, for $i = 1$,

$$a(a_k) = \begin{cases} a_{k+1} & 1 \leq k \leq m-1 \\ a_1 & k = m \end{cases}. \tag{17}$$

  exactly a_{k+1} with indices modulo m.
- Inductive step: Suppose $a^i(a_k) = a_{k+i} \forall k \in \{1, ..., m\}$. Then, for $i + 1$, we have:

$$a^{i+1}(a_k) = a(a^i(a_k)) = a(a_{k+1}) = a_{a+i+1}. \tag{18}$$

  again interpreting $k + i + 1$ modulo m. This proves the formula for $i + 1$, and by induction, for all $i \in \{1, ..., m\}$.

2. Since for every k,

$$a^m(a_k) = a_{k+m} = a_k, \tag{19}$$

we have $a^m = e$.

For $1 \leq t < m$, then

$$a^{t(a_1)} = a_{1+t} \neq a_1, \tag{20}$$

so $a^t = e$. Therefore the least positive exponent sending e to e is m, and $|a| = m$. ∎