THE NUMBER OF ORDER 2 ELEMENTS IN DIHEDRAL GROUP

GOEUN HAN!

1. Introduction

There are various procedures that could be applied to n-gon with $n \geq 3$. The dihedral group D_n is a group defined by the result of carrying out rotation and reflection to the n-gon. In this paper, we will look at the elements of D_n, figure out the properties of the elements, and evaluate the number of order 2 elements based on the value of n.

2. Elements of the Dihedral Group D_n

Definition 2.1. Let D_n be an arbitrary dihedral group. Then r denotes a $2\pi/n$ counter-clockwise rotation across the center.

Example 2.2. In the dihedral group D_3, r represents counterclockwise rotations about the center of $2\pi/3$ of an equilateral triangle. Notice that performing three consecutive $\pi/3$ counterclockwise rotation brings each vertex of the equilateral triangle back to its original position.

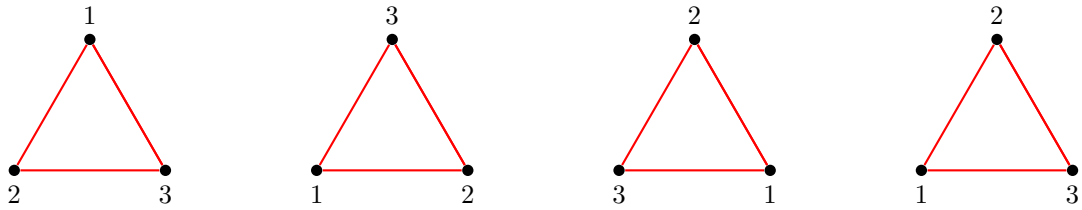

Figure 1. Rotations of equilateral triangle

Example 2.3. In the dihedral group D_4, r represents counterclockwise rotations about the center of $\pi/2$ of a square. Notice that performing four consecutive $\pi/2$ counterclockwise rotation brings each vertex of the square back to its original position.

Definition 2.4. Let D_n be an arbitrary dihedral group. Then s denotes a reflection across the line connecting vertex 1 and the center of the n-gon as shown in figure 3 below.

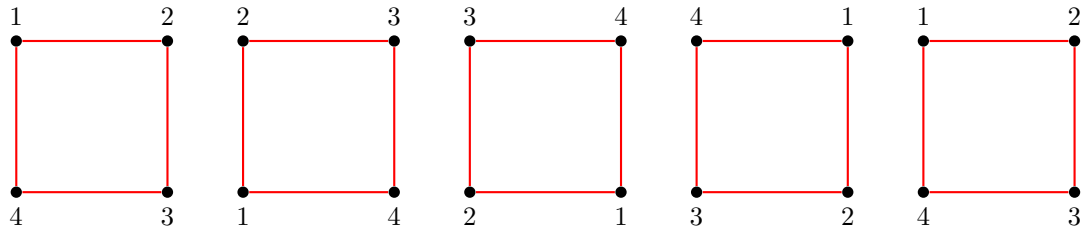

FIGURE 2. Rotations of square

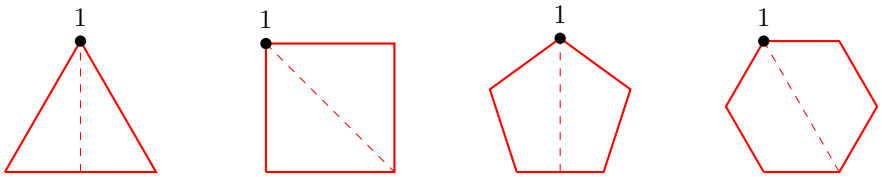

FIGURE 3. Possible lines of reflection for n-gon with n = 3, 4, 5, 6

3. Properties of rotation and reflection

In this section, the following contents will be introduced:
basic properties of r and s
number of elements in D_n
sample multiplication table with $D_3, and D_4$.

Theorem 3.1. *Let D_n be an arbitrary dihedral group. Then:*
i) $o(r) = n$; *and*
ii) $o(s) = 2$

Proof. *i)* Let $r = (1, 2, \ldots, n)$. Then, r maps $1 \mapsto 2, 2 \mapsto 3, \cdots, n \mapsto 1$. Similarly, r^2 maps $1 \mapsto 3, 2 \mapsto 4, \cdots n \mapsto 2$. Then, observe a pattern such that for $i \in \mathbb{N}$ and $i \in \{1, 2, \ldots, n\}$

$$r^k(i) = \begin{cases} i + k \pmod n & \text{if } i + k \pmod n \neq 0 \\ n & \text{if } i + k \pmod n = 0 \end{cases} \tag{1}$$

Then, r^{n-1} maps $1 \mapsto n, 2 \mapsto 1, \cdots, n \mapsto n - 1$. It then follows that r^n maps $1 \mapsto 1, 2 \mapsto 2, \cdots, n \mapsto n$. Therefore, $r^n = e$.

Observe $1 \in \{1, 2, \ldots, n\}$. Notice that $r^k(1) = 1 + k$ for $k \in \mathbb{N}$ such that $k < n$. Then, there is no k such that $r^k(1) = 1$. Then, n is the smallest positive integer such that $r^n = e$. Therefore we can conclude that $o(r) = n$ for all dihedral groups.

ii) First, suppose that n is even. Then, when $n = 4, s = (2, n) = (2, 4)$. Similarly, for $n > 4$, $s = (2, n) \circ (3, n - 1) \circ \cdots \circ (\frac{n}{2}, \frac{n}{2} + 2)$. Then, as s is a composition of 2-cycle, s^2 maps all the elements to itself. Then, as $s^2 = e$, $o(s) = 2$ when n is even.

Now, suppose that n is odd. Then, when $n = 3, s = (2, n) = (2, 3)$. Similarly, for $n > 3$, $s = (2, n) \circ (3, n-1) \circ \cdots \circ (\frac{n+1}{2}, \frac{n+1}{2} + 2)$. By similar argument, s^2 maps all the elements to itself. Then, as $s^2 = e, o(s) = 2$ when n is odd. Notice that as we exhaust all possible cases of n, we can conclude that $o(s) = 2$ for all dihedral groups. □

Lemma 3.2. *Let D_n be an arbitrary dihedral group. Then $srs^{-1} = r^{-1}$.*

Proof. A proof of the above theorem can be found in [1, Theorem 3.1]. □

Theorem 3.3. *Let D_n be an arbitrary dihedral group. Then $sr = r^{-1}s$.*

Proof. From Lemma 3.2, we know that $srs^{-1} = r^{-1}$. Notice that as $s^2 = e, s^{-1} = s$. Then,

$$\begin{aligned} srs^{-1} = r^{-1} &\iff srs = r^{-1} \quad (\text{since } s^2 = e) \\ &\iff srss = r^{-1}s \quad (\text{multiplying both sides by s}) \\ &\iff sr = r^{-1}s \quad (\text{since } s^2 = e) \end{aligned} \tag{2}$$

□

Theorem 3.4. *Let D_n be an arbitrary dihedral group. Then, $sr^k = r^{-k}s$ for all $k \in \mathbb{Z}$.*

Proof. Let D_n be an arbitrary dihedral group, and let $k \in \mathbb{Z}$ be arbitrary. We will show that $sr^k = r^{-k}s$ using induction.

When $k = 1$, $sr^k = sr$. From Theorem 3.3, we know that $sr = r^{-1}s$. Thus, the claim holds when $k = 1$.

Now, assume the claim holds in the $k = j$th case when $j \in \mathbb{Z}$ and $2 \leq j$. Then, $sr^j = r^{-j}s$.

Finally, consider the case when $k = j + 1$. Notice that

$$\begin{aligned} sr^j = r^{-j}s &\iff sr^j r = r^{-j}sr \qquad (\text{multiplying both sides by r}) \\ &\iff sr^{j+1} = r^{-j}sr \\ &\iff sr^{j+1} = r^{-j}r^{-1}s \qquad (\text{by Theorem 3.3}) \\ &\iff sr^{j+1} = r^{-j-1}s \\ &\iff sr^{j+1} = r^{-(j+1)}s \end{aligned}$$

Thus, as we let D_n be an arbitrary dihedral group and let $k \in \mathbb{Z}$ be arbitrary, we can conclude that $sr^k = r^{-k}s$ for all $k \in \mathbb{Z}$. □

Theorem 3.5. *Let D_n be an arbitrary dihedral group.*
Then $D = \{e, r, r^2, \cdots, r^{n-1}, s, rs, r^2s, \cdots, r^{n-1}s\}$ and $|D| = 2n$.

Proof. Let D_n be an arbitrary dihedral group. To begin with, we prove that $D = \{e, r, r^2, \cdots, r^{n-1}, s, rs, r^2s, \cdots, r^{n-1}s\}$.

Let us sketch a proof that all the elements of D_n constructed by compositions of rotations r, reflections s, or both and are of the form $r^k s^j$ with $k, j \in \mathbb{Z}$. Notice

that by using Theorem 3.4, we can move all the r to the left and all the s to the right. For instance,

$$\begin{aligned} & srsr^3sr^5 \\ &= r^{-1}ssr^3sr^5 && \text{(by Theorem 3.4)} \\ &= r^{-1}r^3sr^5 \\ &= r^2sr^5 \\ &= r^2r^{-5}s && \text{(by Theorem 3.4)} \\ &= r^{-3}s \end{aligned}$$

By a similar method, we can reduce sr^7sr^{-2} to $r^{-7}s$ and $srs^8r^{-3}s^7$ to r^2s^2.

Now assume that we reduced an arbitrary composition of rotations and reflections in D_n to r^ks^j with aribtrary $k, j \in \mathbb{Z}$. Similarly, as we know from Theorem 3.1 that $o(s) = 2, s^j \in \{e, s\}$. Notice that $o(r) = n$ and $o(s) = 2$. Then, there are four cases that r^ks^j can be simplified to.

First, consider a case when $r^k = e$ and $s^j = e$. Then, clearly $r^ks^j = ee = e$.

Now, consider a case when $r^k = e$ and $s^j \neq e$. In such case, by Theorem 3.1, $s^j = s$. Then, $r^ks^j = es = s$.

Next, consider a case when $r^k \neq e$ and $s^j = e$. Then, $r^ks^j = r^ke = r^k$. Notice that as $o(r) = n$, $r \neq r^2 \neq \cdots \neq r^{n-1} \neq e$ and $r^j \in \{r, r^2, \cdots, r^{n-1}, e\}$ for all $j \in \mathbb{Z}$. Since $k \in \mathbb{Z}$ and $r^k \neq e$, it then follows that $r^ks^j = r^k \in \{r, r^2, \cdots, r^{n-1}\}$.

Finally, consider a case when $r^k \neq e$ and $s^j \neq e$. From the third case, we know that $r^k \in \{r, r^2, \cdots, r^{n-1}\}$ and $s^j = s$. It then follows that $r^ks^j = r^ks \in \{rs, r^2s, \cdots, r^{n-1}s\}$. Also, notice that $rs, r^2s, \cdots, r^{n-1}s$ are all distinct. Let $r^as, r^bs \in \{rs, r^2s, \cdots, r^{n-1}s\}$ such that $r^as = r^bs$. Then, multiplying s to both sides of the equation, we get $r^a = r^b$. It then follows that $a \pmod n = b \pmod n$. Yet, notice that $1 \leq a, b < n$. Then, it forces that $a = b$. So, for an aribtrary $r^as, r^bs \in \{rs, r^2s, \cdots, r^{n-1}s\}$, if $r^as = r^bs$ when $a = b$. Therefore, we can conclude that there exists $n - 1$ unique elements in D_n that can be simplified into the compositions of both r and s.

Now we show that all elements of different cases are distinct. To begin with, clearly, $r \neq r^2 \neq \cdots \neq r^{n-1} \neq e$ as $o(r) = n$. So, e is distinct from all unique elements from case 2. Similarly, as $o(s) = 2, e$ is distinct from all unique elements from case 3.

Next, we show that all the unique elements in case 2 are distinct from s, the element in case 3. Suppose, for the sake of contradiction, that there exists $k \in \mathbb{Z}$ such that $r^k = s$. Consider $1 \in \{1, 2, \dots n\}$. By the definition of $s, s(1) = 1$. As $r^k = s$, it follows that $r^k(1) = 1$. Yet, based on the proof of Theorem 3.1,

$$r^k(1) = \begin{cases} 1 + k \pmod n & \text{if } 1 + k \pmod n \neq 0 \\ n & \text{if } 1 + k \pmod n = 0. \end{cases} \tag{3}$$

Then, notice that $r^k(1) = 1 \iff 1 + k \pmod{n} = 1 \iff \exists \alpha \in \mathbb{Z}$ such that $k = n\alpha$. As we assumed $r^k = s$, substituting k with $n\alpha$, we get $r^k = r^{n\alpha} = (r^n)^\alpha = e$. Then, as $e = s$, we have a contradiction. Therefore, we can conclude that $r^k \neq s$ for all $k \in \mathbb{N}$ with $1 \leq k < n$. So, we can conclude that all the elements in case 2 and distinct from the elements in case 3.

Now, we prove that all the elements in case 4 are distinct from the elements in case 2. Suppose, for the sake of contradiction, that there exists r^a and $r^b s$ with $a, b \in \mathbb{Z}$ such that $r^a = r^b s$. Then, by multiplying both sides of the equation by r^{-b}, we get $r^{-b+a} = s$. Yet, notice that as r^{-b+a} is a composition of only r, it falls into case 3, and earlier we proved that all elements that are created by composition of only r are distinct from s. So, we have a contradiction and conclude that all the elements of in case 4 are distinct from all the element in case 2.

Similarly, to prove that all the elements in case 4 are distinct from the element in case 3, for the sake of contradiction we claim that there exists $r^a s$ from case 4 and s from case 3 such that $r^a s = s$. By multiplying both sides of the equation by s, we get $r^a = e$. Yet, as $r^a s$ is an element from case 4, by assumption $r^a \neq e$. So, we have a contradiction. Therefore, we can conclude that all the elements of in case 4 are distinct from all the element in case 3.

Finally, we show that all the elements in case 4 are distinct from the element in case 1. Suppose, for the sake of contradiction, that there exists an element $r^k s$ in case 4 such that $r^k s = e$. Multiplying both sides of the equation by s gives $r^k = s$. Yet, notice that as r^k is in case 4, $r^k \neq e$. As it is the composition of only rotation, r^k is in case 1 and we have shown that all the elements in case 1 are distinct from s. So, we have a contradiction. Therefore, we can conclude that all the elements of in case 4 are distinct from all the element in case 1. Thus, we have proven that all the elements in each of the cases are distinct from one another. Also, it follows that $D = \{e, r, r^2, \cdots, r^{n-1}, s, rs, r^2 s, \cdots, r^{n-1} s\}$.

Now, we calculate the size of D_n. To begin with, notice that there are only one identity element. So, there is one distinct element that is in case 1. Next, we have shown that there are $n - 1$ distinct elements in case 2 and 1 distint element in case 3. Also, we have shown that there are $n - 1$ unique elements in case 4. Therefore, we can conclude that the size of D_n is $1 + (n - 1) + 1 + (n - 1) = 2n$. □

Example 3.6. $D_3 = \{e, r, r^2, s, rs, r^2 s\}$ and the multiplication in D_3 is shown in the table below.

Example 3.7. $D_4 = \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$ and the multiplication in D_3 is shown in the table below.

$\circ$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

TABLE 1. Multiplication table for D_3

$\circ$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

TABLE 2. Multiplication table for D_4

4. Element of order 2 in the dihedral Group

Theorem 4.1. *Let D_n be an arbitrary dihedral group. Then, $(r^ks)^2 = e$ for all $k \in \mathbb{N}$ such that $k < n$.*

Proof. Let D_n be an arbitrary dihedral group, and let $k \in \mathbb{N}$ be arbitrary with $k < n$. We will show that $(r^ks)^2 = e$ using induction.

When $k = 1$, $(r^ks)^2 = (rs)^2 = (rs) \circ (rs)$. Then,

$$\begin{aligned}
(rs)^2 &= (rs) \circ (rs) \\
&= r \circ s \circ r \circ s \\
&= r \circ (s \circ r) \circ s && \text{(by associativity of } D_n\text{)} \\
&= r \circ r^{-1} \circ s \circ s && \text{(by Theorem 3.3)} \\
&= e.
\end{aligned}$$

Thus, the claim holds when $k = j$.
Now, assume the claim holds in the $k = j-1$th case when $1 \leq j-1 \leq n-2$. Then, $(r^{j-1}s)^2 = (r^{j-1}s) \circ (r^{j-1}s) = e$.

Finally, consider the case when $k = j$. Notice that $(r^j s)^2$ can be written as $(r^j s) \circ (r^j s)$. Then,

$$\begin{aligned}
(r^j s)^2 &= (r^j s) \circ (r^j s) \\
&= r^j \circ s \circ r^j \circ s \\
&= r^j \circ s \circ r \circ r^{j-1} \circ s \\
&= r^j \circ (s \circ r) \circ r^{j-1} \circ s && \text{(by associativity of } D_n) \\
&= r^j \circ (r^{-1} s) \circ r^{j-1} \circ s && \text{(by Theorem 3.3)} \\
&= (r^{j-1} \circ r^{-1}) s \circ r^{j-1} \circ s && \text{(by associativity of } D_n) \\
&= (r^{j-1} s) \circ (r^{j-1} s) && \text{(by associativity of } D_n) \\
&= (r^{j-1} s)^2.
\end{aligned}$$

By our assumption on $(r^{j-1}s)^2$, we can substitute $(r^{j-1}s)^2$ with e. It then follows that $(r^j s)^2 = e$. Thus, as we let D_n be an arbitrary dihedral group and let $k \in \mathbb{N}$ be arbitrary with $k < n$, we can conclude that $(r^k s)^2 = e$ for all $k \in \mathbb{N}$ with $k < n$. □

Lemma 4.2. *Let G be a group and $x \in G$. Then:*
i)If $o(x) = n$ and $x^m = e$, then n divides m.
ii)If $o(x) = n$ and $(m, n) = d$, then $o(x^m) = n/d$

Proof. A proof of the above lemma can be found in [2, Theorem 4.4(ii, iii)]. □

Theorem 4.3. *Let D_n be an arbitrary dihedral group. Then the number of the elements of order 2 is:*
i) n if n is odd
ii) $n + 1$ if n is even.

Proof. i) Let D_n be an arbitrary dihedral group with n be odd number. From the proof of Theorem 3.5, we know that $D_n = \{e, r, r^2, \dots r^{n-1}, s, rs, \dots, r^{n-1}s\}$. To begin with, clearly, the order of e is 1. So, e is not the element of order 2. We then check if there is an element of order 2 of the form r^k for $1 \leq k < n$. We suppose for a contradiction, that there exists $r^a \in \{r, r^2, \dots r^{n-1}\}$ such that $o(r^a) = 2$. Then, $(r^a)^2 = e$. By lemma 4.2, it follows that n divides 2. As we let n to be odd, we have a contradiction. Therefore, we can conclude that $r, r^2, \dots r^{n-1}$ are not the elements of order 2. Next, we consider s. By Theorem 3.1, clearly $o(s) = 2$. So, s is the element of D_n with order 2. Finally, we check all the elements of the form $r^k s$ in D_n with $k \in \mathbb{Z}$ and $1 \leq k < n$. Notice that by Theorem 4.1, they all have order 2. From the proof for Theorem 3.5, we know that there are $n - 1$ elements of such form. As these exhaust all the elements in D_n, we can conclude that the number of the elements of order 2 is $1 + (n - 1) + 1 = n$ when n is odd.

ii) Let D_n be an arbitrary dihedral group with n be odd number. From the proof of Theorem 3.5, we know that$D_n = \{e, r, r^2, \dots r^{n-1}, s, rs, \dots, r^{n-1}s\}$. From the proof from part i, we know that e is not the identity element. Also, by similar argument, s and the elements of the form $r^k s$ in D_n with $k \in \mathbb{Z}$ and $1 \leq k < n$ have order 2. Now, we check the order of $r, r^2, \dots r^{n-1}$. By Lemma 4.2, we know that for $r^k \in \{r, r^2, \dots r^{n-1}\}, o(r^k) = n/(k, n)$. Let $n/(k, n) = 2$. Then, $k = n/2$. Since n is an even number, $n/2 \in \mathbb{Z}$ and $1 \leq n/2 < n$. It then follows that

$r^{n/2} \in \{r, r^2, \dots r^{n-1}\}$ and $r^{n/2}$ is the only element of the form r^k in D_n with order 2. As these exhaust all the elements in D_n, we can conclude that the number of the elements of order 2 is $1 + (n-1) + 1 + 1 = n + 1$ when n is even. □

References

[1] K. Conrad. *DIHEDRAL GROUPS*. https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf

[2] D. Saracino. *ABSTRACT ALGEBRA*.