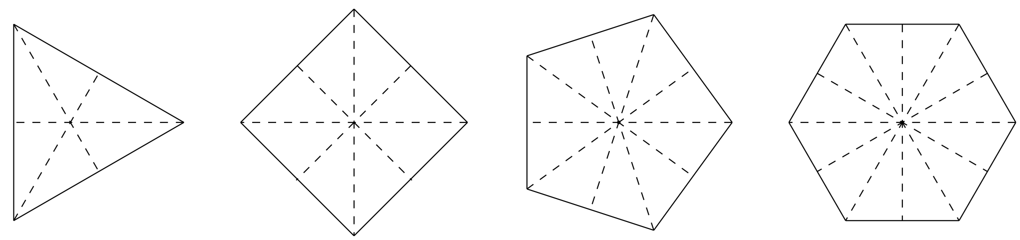
DIHEDRAL GROUPS

KEITH CONRAD

1. Introduction

For $n \geq 3$, the dihedral group D_n is defined as the rigid motions[1] of the plane preserving a regular n-gon, with the operation being composition. These polygons for $n = 3, 4$, 5, and 6 are pictured below. The dotted lines are lines of reflection: reflecting the polygon across each line brings the polygon back to itself, so these reflections are in D_3, D_4, D_5, and D_6.



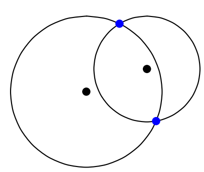
In addition to reflections, a rotation by any multiple of $2\pi/n$ radians around the center carries the polygon back to itself, so D_n contains some rotations.

We will look at elementary aspects of dihedral groups: listing its elements, relations between rotations and reflections, conjugacy classes, the center, and commutators.

Throughout, $n \geq 3$.

2. Finding the elements of D_n

The points in the plane that have a specified distance from a given point is a circle, so the points with specified distances from two given points are the intersection of two circles, which is two points. For instance, the blue points in the figure below have the same distances to each of the two black points.



Lemma 2.1. *Every point on a regular polygon is determined, among all points on the polygon, by its distances from two adjacent vertices of the polygon.*

Proof. In the picture above, let the black dots be adjacent vertices of a regular polygon. Since they are adjacent, the line segment connecting them is an edge of the polygon and the polygon is entirely on one side of the line through the black dots. That shows the two

[1]A *rigid motion* is a distance-preserving transformation, like a rotation, a reflection, or a translation, and is also called an *isometry*.

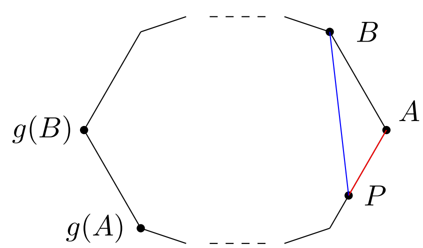
blue dots can't both be on the polygon, so a point on the polygon is distinguished from all other points on the polygon (not from all other points in the plane!) by its distances from the two adjacent vertices. □

Theorem 2.2. *The size of D_n is $2n$.*

Proof. Our argument has two parts: an upper bound and then a construction of enough rigid motions to achieve the upper bound.

Step 1: $\#D_n \leq 2n$.

Pick two adjacent vertices of a regular n-gon, and call them A and B as in the figure below. An element g of D_n is a rigid motion preserving the polygon, and it must carry vertices to vertices (how are vertices unlike other points in terms of their distance relationships with all points on the polygon?) and g must preserve adjacency of vertices, so $g(A)$ and $g(B)$ are adjacent vertices of the polygon.



For any point P on the polygon, the location of $g(P)$ is determined by $g(A)$ and $g(B)$, because the distances of $g(P)$ from the adjacent vertices $g(A)$ and $g(B)$ equal the distances of P from A and B, and therefore $g(P)$ is determined on the polygon by Lemma 2.1. To count $\#D_n$ it thus suffices to find the number of possibilities for $g(A)$ and $g(B)$.

Since $g(A)$ and $g(B)$ are a pair of adjacent vertices, $g(A)$ has at most n possibilities (there are n vertices), and for each choice of that $g(B)$ has at most 2 possibilities (one of the two vertices adjacent to $g(A)$). That gives us at most $n \cdot 2 = 2n$ possibilities, so $\#D_n \leq 2n$.

Step 2: $\#D_n = 2n$.

We will describe n different rotations and n different reflections of a regular n-gon. This is $2n$ different rigid motions since a rotation and a reflection are not the same: a rotation fixes just one point, the center, but a reflection fixes a line.

A regular n-gon can be rotated around its center in n different ways to come back to itself (including rotation by 0 degrees). Specifically, we can rotate around the center by $2k\pi/n$ radians where $k = 0, 1, \ldots, n-1$. This is n rotations.

To describe reflections preserving a regular n-gon, look at the pictures on the first page: for $n = 3$ and $n = 5$ there are lines of reflection connecting each vertex to the midpoint of the opposite side, and for $n = 4$ and $n = 6$ there are lines of reflection connecting opposite vertices and lines of reflection connecting midpoints of opposite sides. These descriptions of the possible reflections work in general, depending on whether n is even or odd:

- For odd n, there is a reflection across the line connecting each vertex to the midpoint of the opposite side. This is a total of n reflections (one per vertex). They are different because each one fixes a different vertex.
- For even n, there is a reflection across the line connecting each pair of opposite vertices ($n/2$ reflections) and across the line connecting midpoints of opposite sides (another $n/2$ reflections). The number of these reflections is $n/2+n/2 = n$. They are

different because they have different types of fixed points on the polygon: different pairs of opposite vertices or different pairs of midpoints of opposite sides.

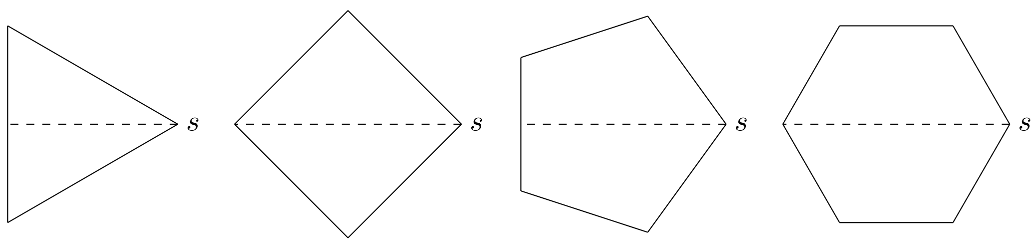
□

In D_n it is standard to write r for the counterclockwise rotation by $2\pi/n$ radians. This rotation depends on n, so the r in D_3 means something different from the r in D_4. However, as long as we are dealing the dihedral group for one value of n, there shouldn't be any confusion. From the rotation r, we get n rotations in D_n by taking powers (r has order n):

$$1, r, r^2, \ldots, r^{n-1}.$$

(We adopt common group-theoretic notation and designate the identity rigid motion as 1.)

Let s be a reflection across a line *through a vertex*. See examples in the polygons below.[2] Any reflection has order 2, so $s^2 = 1$ and $s^{-1} = s$.



Theorem 2.3. *The n reflections in D_n are $s, rs, r^2s, \ldots, r^{n-1}s$.*

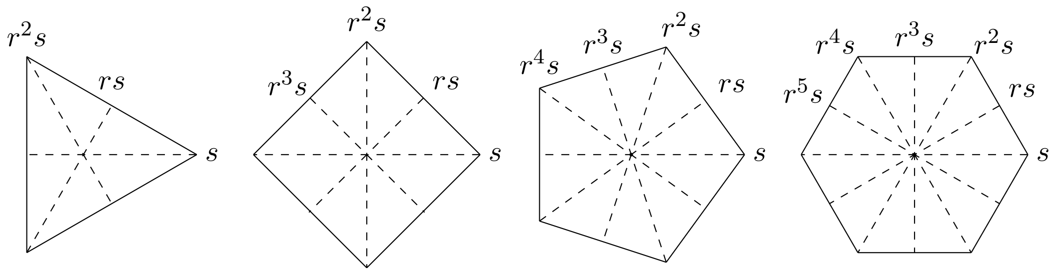
Proof. The rigid motions $s, rs, r^2s, \ldots, r^{n-1}s$ are different since $1, r, r^2, \ldots, r^{n-1}$ are different and we just multiply them all on the left by the same element s. No r^ks is a rotation because if $r^ks = r^\ell$ then $s = r^{\ell-k}$, but s is not a rotation.

The group D_n consists of n rotations and n reflections, and no r^ks is a rotation, so they are all reflections. □

Since each element of D_n is a rotation or reflection, there is no "mixed rotation-reflection": the product of a rotation r^i and a reflection r^js (in either order) is a reflection.

The geometric interpretation of the successive reflections s, rs, r^2s, and so on is this: drawing all the lines of reflection for the regular n-gon and moving clockwise around the polygon starting from a vertex fixed by s we meet successively the lines fixed by rs, $r^2s, \ldots, r^{n-1}s$. In the polygons below, we let s be the reflection across the line through the rightmost vertex and then label the other lines of reflection accordingly. Convince yourself, for instance, that rs is the next line of reflection if we follow them around counterclockwise.

[2]The convention that s fixes a line through a vertex matters only for even n, where there are some reflections across a line that doesn't pass through a vertex, namely a line connecting midpoints of opposite sides. When n is odd, all reflections fix a line through a vertex, so any of them could be chosen as s.



Let's summarize what we have now found.

Theorem 2.4. *The group D_n has $2n$ elements. As a list,*

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}, \tag{2.1}$$

In particular, all elements of D_n with order greater than 2 are powers of r.

Watch out: although any element of D_n with order greater than 2 has to be a power of r, because any element that isn't a power of r is a reflection, it is *false* in general that the only elements of order 2 are reflections. When n is even, $r^{n/2}$ is a 180-degree rotation, which has order 2. Clearly a 180-degree rotation is the only rotation with order 2, and it lies in D_n only when n is even.

3. Relations between rotations and reflections

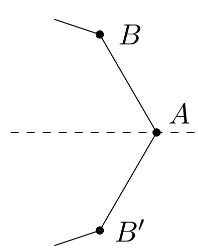
The rigid motions r and s do not commute. Their commutation relation is a fundamental formula for computations in D_n, and goes as follows.

Theorem 3.1. *In D_n,*

$$srs^{-1} = r^{-1}. \tag{3.1}$$

Proof. Since every rigid motion of a regular n-gon is determined by its effect on two adjacent vertices, to prove $srs^{-1} = r^{-1}$ in D_n it suffices to check srs^{-1} and r^{-1} have the same values at some pair of adjacent vertices.

Recall s is a reflection fixing a vertex of the polygon. Let A be a vertex fixed by s and write its adjacent vertices as B and B', with B appearing counterclockwise from A and B' appearing clockwise from A. This is illustrated in the figure below, where the dashed line through A is fixed by s. We have $r(A) = B$, $r^{-1}(A) = B'$, $s(A) = A$, and $s(B) = B'$.



The values of srs^{-1} and r^{-1} at A are

$$(srs^{-1})(A) = (srs)(A) = sr(s(A)) = sr(A) = s(B) = B' \quad \text{and} \quad r^{-1}(A) = B',$$

while their values at B are

$$(srs^{-1})(B) = (srs)(B) = sr(s(B)) = sr(B') = s(A) = A \quad \text{and} \quad r^{-1}(B) = A.$$

Since srs^{-1} and r^{-1} are equal at A and at B, they are equal everywhere on the polygon, and therefore $srs^{-1} = r^{-1}$ in D_n. □

Equivalent ways of writing $srs^{-1} = r^{-1}$ are (since $s^{-1} = s$)

$$sr = r^{-1}s, \quad rs = sr^{-1}. \tag{3.2}$$

What these mean is that when calculating in D_n we can move r to the other side of s by inverting it. By induction (or by raising both sides of (3.1) to an integral power) check

$$sr^k = r^{-k}s, \quad r^k s = sr^{-k} \tag{3.3}$$

for any integer k. In other words, any power of r can be moved to the other side of s by inversion. For example, consistent with $r^k s$ being a reflection we can check its square is trivial:

$$(r^k s)^2 = r^k s r^k s = r^k r^{-k} ss = s^2 = 1.$$

The relation (3.2) involves a particular rotation and a particular reflection in D_n. In (3.3), we extended (3.2) to any rotation and a particular reflection in D_n. We can extend (3.3) to any rotation and any reflection in D_n: a general reflection in D_n is $r^i s$, so by (3.3)

$$\begin{aligned}(r^i s)r^j &= r^i r^{-j} s \\ &= r^{-j} r^i s \\ &= r^{-j}(r^i s).\end{aligned}$$

In the other order,

$$\begin{aligned}r^j(r^i s) &= r^i r^j s \\ &= r^i s r^{-j} \\ &= (r^i s)r^{-j}.\end{aligned}$$

This has a nice geometric meaning: when multiplying in D_n, *any* rotation can be moved to the other side of *any* reflection by inverting the rotation. This geometric description makes such algebraic formulas easier to remember.

Let's put these formulas to work by computing all the commutators in D_n.

Theorem 3.2. *The commutators in D_n are the subgroup $\langle r^2 \rangle$.*

Proof. The commutator $[r, s]$ is $rsr^{-1}s^{-1} = rrss^{-1} = r^2$, so r^2 is a commutator. More generally, $[r^i, s] = r^i s r^{-i} s^{-1} = r^i r^i s s^{-1} = r^{2i}$, so every element of $\langle r^2 \rangle$ is a commutator.

To show every commutator is in $\langle r^2 \rangle$, we will compute $[g, h] = ghg^{-1}h^{-1}$ when g and h are rotations or reflections and check the answer is always a power of r^2.

Case 1: g and h are rotations.

Since any two rotations commute, $ghg^{-1}h^{-1}$ is trivial.

Case 2: g is a rotation and h is a reflection.

Write $g = r^i$ and $h = r^j s$. Then $h^{-1} = h$, so

$$ghg^{-1}h^{-1} = ghg^{-1}h = r^i r^j s r^{-i} r^j s = r^{i+j} r^{-(j-i)} ss = r^{2i}.$$

Case 3: g is a reflection and h is a rotation.

Since $(ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1}$, by Case 2 the commutator $hgh^{-1}g^{-1}$ is a power of r^2, so passing to its inverse tells us that $ghg^{-1}h^{-1}$ is a power of r^2.

Case 4: g and h are rotations.
Write $g = r^i s$ and $h = r^j s$. Then $g^{-1} = g$ and $h^{-1} = h$, so

$$ghg^{-1}h^{-1} = ghgh = (gh)^2 = (r^i s r^j s)^2 = (r^{i-j} ss)^2 = r^{2(i-j)}.$$

□

4. Conjugacy and Center

While the number of reflections in D_n ($n \geq 3$) has one formula for all cases, namely n, the geometric description of reflections depends on the parity of n: for odd n all lines of reflection look the same, but for even n these lines fall into two types. See Figures 1 and 2.

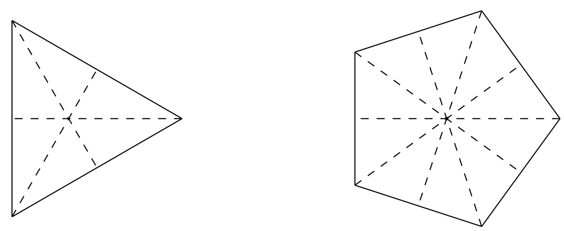


Figure 1. Lines of Reflection for $n = 3$ and $n = 5$.

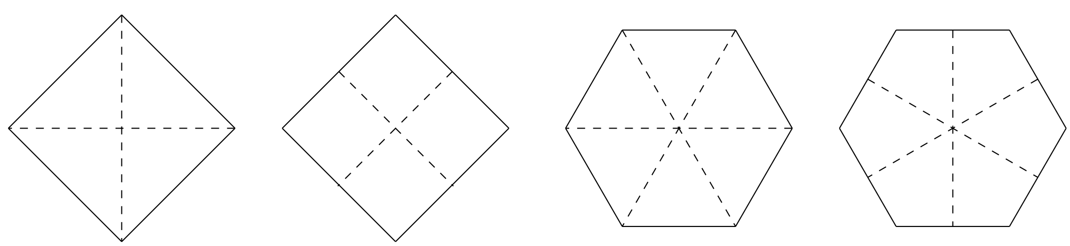


Figure 2. Lines of Reflection for $n = 4$ and $n = 6$.

The different geometric descriptions of reflections in D_n for even and odd n manifest themselves algebraically when we describe the conjugacy classes of D_n.

Theorem 4.1. *The conjugacy classes in D_n are as follows.*

(1) *If n is odd,*
- *the identity element: $\{1\}$,*
- *$(n-1)/2$ conjugacy classes of size 2: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm (n-1)/2}\}$,*
- *all the reflections: $\{r^i s : 0 \leq i \leq n-1\}$.*

(2) *If n is even,*
- *two conjugacy classes of size 1: $\{1\}$, $\{r^{\frac{n}{2}}\}$,*
- *$n/2 - 1$ conjugacy classes of size 2: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(\frac{n}{2}-1)}\}$,*
- *the reflection fall into two conjugacy classes: $\{r^{2i} s : 0 \leq i \leq \frac{n}{2} - 1\}$ and $\{r^{2i+1} s : 0 \leq i \leq \frac{n}{2} - 1\}$.*

In words, the theorem says each rotation is conjugate only to its inverse (which is another rotation except for the identity and, for even n, the 180 degree rotation $r^{n/2}$) and the reflections are all conjugate for odd n but break up into two conjugacy classes for even n. The two conjugacy classes of reflections for even n are the two types we see in Figure 2: those whose fixed line connects opposite vertices ($r^{\text{even}}s$) and those whose fixed line connects midpoints of opposite sides ($r^{\text{odd}}s$).

Proof. Every element of D_n is r^i or $r^i s$ for some integer i. Therefore to find the conjugacy class of an element g we will compute $r^i g r^{-i}$ and $(r^i s)g(r^i s)^{-1}$.

The formulas

$$r^i r^j r^{-i} = r^j, \quad (r^i s)r^j(r^i s)^{-1} = r^{-j}$$

as i varies show the only conjugates of r^j in D_n are r^j and r^{-j}. Explicitly, the basic formula $sr^js^{-1} = r^{-j}$ shows us r^j and r^{-j} are conjugate; we need the more general calculation to be sure there is nothing further that r^j is conjugate to.

To find the conjugacy class of s, we compute

$$r^i s r^{-i} = r^{2i}s, \quad (r^i s)s(r^i s)^{-1} = r^{2i}s.$$

As i varies, $r^{2i}s$ runs through the reflections in which r occurs with an exponent divisible by 2. If n is odd then every integer modulo n is a multiple of 2 (since 2 is invertible mod n so we can solve $a \equiv 2i \bmod n$ for i given any a). Therefore when n is odd

$$\{r^{2i}s : i \in \mathbf{Z}\} = \{r^i s : i \in \mathbf{Z}\},$$

so every reflection in D_n is conjugate to s. When n is even, however, we only get half the reflections as conjugates of s. The other half are conjugate to rs:

$$r^i(rs)r^{-i} = r^{2i+1}s, \quad (r^i s)(rs)(r^i s)^{-1} = r^{2i-1}s.$$

As i varies, this gives us $\{rs, r^3s, \ldots, r^{n-1}s\}$. □

The center is another aspect where D_n behaves differently when n is even and n is odd.

Theorem 4.2. *When $n \geq 3$ is odd, the center of D_n is trivial. When $n \geq 3$ is even, the center of D_n is $\{1, r^{n/2}\}$.*

Proof. The center is the set of elements that are in conjugacy classes of size 1, and we see in Theorem 4.1 that for odd n this is only the identity, while for even n this is the identity and $r^{n/2}$. □

Example 4.3. The group D_3 has trivial center. The group D_4 has center $\{1, r^2\}$.

Geometrically, $r^{n/2}$ for even n is a 180-degree rotation, so Theorem 4.2 is saying in words that the only nontrivial rigid motion of a regular polygon that commutes with all other rigid motions of the polygon is a 180-degree rotation (when n is even).