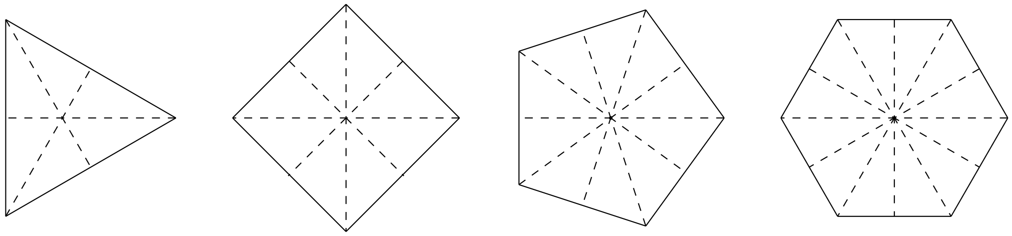
DIHEDRAL GROUPS

KEITH CONRAD

1. Introduction

For $n \geq 3$, the dihedral group D_n is defined as the rigid motions[1] taking a regular n-gon back to itself, 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.

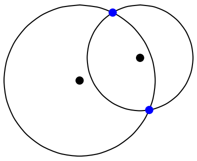


In addition to reflections, a rotation by a multiple of $2\pi/n$ radians around the center carries the polygon back to itself, so D_n contains some rotations.

We will look at elementary aspects of dihedral groups: listing its elements, relations between rotations and reflections, the center, and conjugacy classes. *Throughout,* $n \geq 3$.

2. Finding the elements of D_n

Points in the plane at a specified distance from a given point form a circle, so points with specified distances from two given points are the intersection of two circles, which is two points (non-tangent circles) or one point (tangent circles). 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 blue dots be adjacent vertices of a regular polygon. The line segment connecting them is an edge of the polygon and the polygon is entirely on one side of the line through the blue dots. So the two black dots can't both be on the polygon,

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

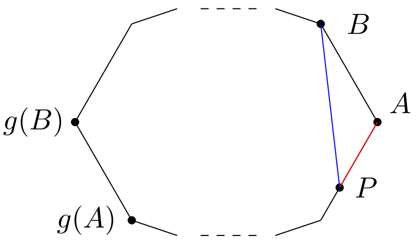
which means each point on the polygon is distinguished from all other points on the polygon (not from all other points in the plane!) by its distances from two adjacent vertices. □

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 taking the n-gon back to itself, 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 each 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 rotations and n reflections of a regular n-gon.

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 taking a regular n-gon back to itself, look at the pictures on the first page: if n is 3 or 5 there are lines of reflection connecting each vertex to the midpoint of the opposite side, and if n is 4 or 6 there are lines of reflection connecting opposite vertices and lines of reflection connecting midpoints of opposite sides. These descriptions of 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.

The rotations and reflections are different in D_n since a non-identity rotation fixes no point on the polygon, the identity rotation fixes all points, and a reflection fixes two points. □

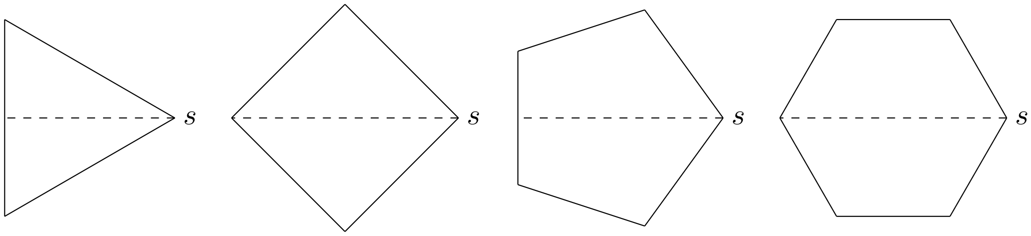
In D_n it is standard to write r for the counterclockwise rotation by $2\pi/n$ radians. This rotation depends on n, so the r in D_3 means something different from the r in D_4. However, as long as we are dealing with one value of n, there shouldn't be confusion.

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

Here and below, we designate the identity rigid motion as 1.

Proof. The rotations $1, r, r^2, \ldots, r^{n-1}$ are different since r has order n. □

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



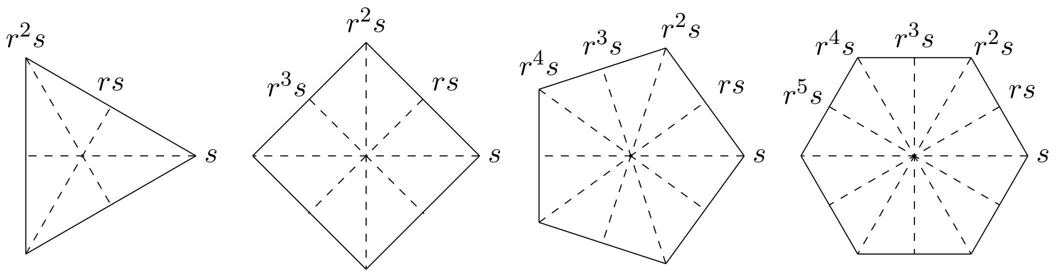
Theorem 2.4. *The n reflections in D_n are $s, rs, r^2s, \ldots, r^{n-1}s$.*

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 right by s. No r^ks is a rotation because if $r^ks = r^\ell$ then $s = r^{\ell-k}$, but s is not a rotation.

Since D_n has n rotations and n reflections, and no r^ks is a rotation, they're 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 reflections s, rs, r^2s, and so on is this: drawing all lines of reflection for a regular n-gon and moving clockwise around the polygon starting from a vertex fixed by s, we meet successively the lines fixed by $rs, r^2s, \ldots, r^{n-1}s$. See the polygons below. Convince yourself, for instance, that if s is the reflection across the line through the rightmost vertex then rs is the next line of reflection counterclockwise.



Let's summarize what we have now found.

[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.

Theorem 2.5. *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 each element of D_n with order greater than 2 has to be a power of r, because each 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.

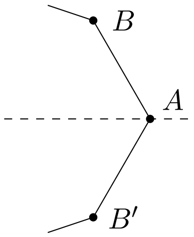
Theorem 3.1. *In D_n,*

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

Proof. A short proof comes from rs being a reflection: $(rs)^2 = 1 \Rightarrow rsrs = 1 \Rightarrow srs = r^{-1}$, and $s = s^{-1}$ since s has order 2.

We now want to prove (3.1) in a longer way using a geometric interpretation of both sides. 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 a 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} agree at A and at B, they agree on the polygon, so $srs^{-1} = r^{-1}$. □

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 every integer k. In other words, every power of r can be moved to the other side of s by inversion. This also follows from $r^k s$ being a reflection:

$$1 = (r^k s)^2 = r^k s r^k s \Rightarrow sr^k = r^{-k}s^{-1} = r^{-k}s.$$

Example 3.2. In D_7, using (3.3)

$$r^2sr^6sr^3 = r^2(sr^6)sr^3 = r^2(r^{-6}s)sr^3 = r^2r^{-6}ssr^3 = r^{-4}r^3 = r^{-1} = r^6$$

and

$$sr^4sr^3sr^2 = s(r^4s)r^3(sr^2) = s(sr^{-4})r^3(r^{-2}s) = ssr^{-4}r^3r^{-2}s = r^{-3}s = r^4s.$$

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)

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

In the other order,

$$\begin{aligned}r^j(r^is) &= r^ir^js\\ &= r^isr^{-j}\\ &= (r^is)r^{-j}.\end{aligned}$$

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

Knowing how rotations and reflections interact under multiplication lets us compute the center of D_n. The answer depends on whether n is even or odd.

Theorem 3.3. *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. No reflections are in the center of D_n since reflections do not commute with r:

$$(r^is)r = r^i(sr) = r^ir^{-1}s = r^{i-1}s, \quad r(r^is) = r^{i+1}s$$

so if r^is commutes with r then $r^{i-1} = r^{i+1}$, which implies $r^2 = 1$, but r has order $n \geq 3$.

Which rotations r^j could be in the center of D_n? Without loss of generality $0 \leq j \leq n-1$. We would need r^j to commute with s, so $r^js = sr^j$, which is equivalent to $r^js = r^{-j}s$, which implies $r^{2j} = 1$. Since r has order n, $r^{2j} = 1$ only if $n \mid 2j$. For odd n this implies $n \mid j$, so j is a multiple of n and thus $r^j = 1$. Hence for odd n the only rotation that could be in the center of D_n is 1. Certainly 1 is in the center, so for odd n the center of D_n is $\{1\}$.

For even n, the condition $n \mid 2j$ is equivalent to $n/2 \mid j$, and for $0 \leq j \leq n-1$ the only choices for j are $j = 0$ and $j = n/2$. Thus $r^j = r^0 = 1$ or $r^j = r^{n/2}$. Certainly 1 is in the center, and to show $r^{n/2}$ is in the center we check it commutes with every rotation and reflection in D_n. That $r^{n/2}$ commutes with rotations is obvious since all rotations are powers of r and thus they all commute with each other. To check $r^{n/2}$ commutes with every reflection in D_n, the key point is that $r^{n/2} = r^{-n/2}$, which follows from $r^n = 1$. (This also makes sense geometrically since $r^{n/2}$ is a 180° rotation, and rotating by 180° or −180° has the same effect.) Now we check $r^{n/2}$ commutes with each reflection $r^i s$:

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

□

Example 3.4. 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 3.3 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).

4. Conjugacy

In D_n the geometric description of reflections depends on the parity of n: for odd n, the lines of reflection look the same – each line connects a vertex and the midpoint on the opposite side – but for even n the lines of reflection fall into two types – lines through pairs of opposite vertices and lines through midpoints of opposite sides. See Figures 1 and 2.

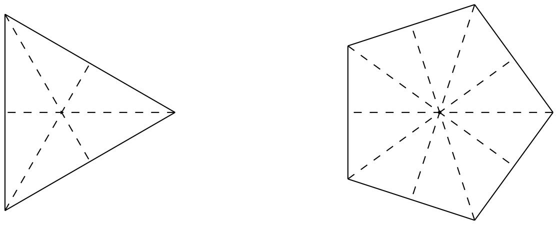


Figure 1. Lines of Reflection for $n = 3$ and $n = 5$.

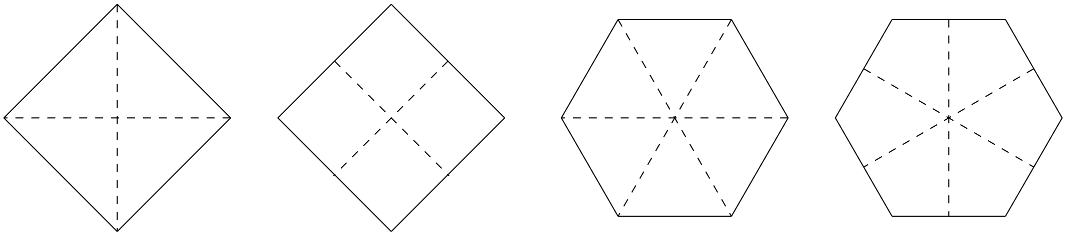


Figure 2. Lines of Reflection for $n = 4$ and $n = 6$.

These different geometric descriptions of reflections in D_n for even and odd n manifest themselves in the algebraic structure of the group D_n when we describe its conjugacy classes.

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: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \dots, \{r^{\pm(\frac{n}{2}-1)}\}$,*
- *the reflections 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 (if n is even) except for the 180-degree rotation $r^{n/2}$. Also 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^is for some integer i. Therefore to find the conjugacy class of an element g we will compute r^igr^{-i} and $(r^is)g(r^is)^{-1}$.

The formulas

$$r^ir^jr^{-i} = r^j, \quad (r^is)r^j(r^is)^{-1} = r^{-j}$$

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

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

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 we can solve $k \equiv 2i \bmod n$ for i given k). Therefore when n is odd

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

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:

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

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

Since elements in the center of a group are those whose conjugacy class has size 1, the calculation of the conjugacy classes in D_n gives another proof that the center of D_n is trivial for odd n and $\{1, r^{n/2}\}$ for even n: we see in Theorem 4.1 that for odd n the only conjugacy class of size 1 is $\{1\}$, while for even n the only conjugacy classes of size 1 are $\{1\}$ and $\{r^{n/2}\}$.

Appendix A. Commutators in D_n

In a group, a commutator is a product of the form $ghg^{-1}h^{-1}$, which is denoted $[g,h]$. The set of commutators is not necessarily closed under multiplication (it is closed under inversion since $[g,h]^{-1} = hgh^{-1}g^{-1} = [h,g]$), so this set may not be a subgroup. We have $[g,h] = e$ if and only if $gh = hg$, so the commutator is related to commuting. What are the commutators in dihedral groups?

Theorem A.1. *The commutators in D_n form 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, $[r^i, s] = r^isr^{-i}s^{-1} = r^ir^iss^{-1} = r^{2i}$, 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.

Writing $g = r^i$ and $h = r^j$, these commute so $ghg^{-1}h^{-1}$ is trivial.

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

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

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

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 reflections.

Write $g = r^is$ and $h = r^js$. Then $g^{-1} = g$ and $h^{-1} = h$, so

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

□

Remark A.2. If n is odd, $\langle r^2\rangle = \langle r\rangle$. If n is even, $\langle r^2\rangle$ is a proper subgroup of $\langle r\rangle$.