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 in Figure 1. 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.[2]
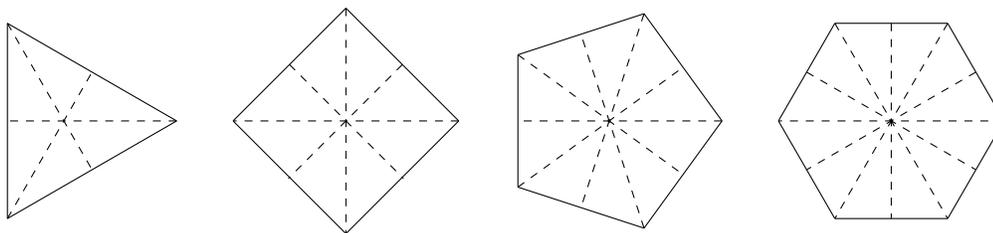

FIGURE 1. Regular n-gons for $n = 3, 4, 5, 6$

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 to a given point form a circle, so points with specified distances to 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 distance to each of the two black points (centers of the circles). So given two distinct points (the black points), there are at most two points in the plane (the blue points) that can have specified distances to them.

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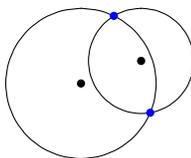
[1]A *rigid motion* is a distance-preserving transformation, such as a rotation, a reflection, and a translation, and is also called an *isometry*.

[2]Group theorists write D_{2n} where other mathematicians write D_n, so a group theorist writes the group of rigid motions of the square as D_8, not D_4. Why do they do this? See https://math.stackexchange.com/questions/2560348.

Points that are equidistant to the two blue points are on the line through the two black points, so if we pick a third point *not collinear* with the black points, then its distances to the two blue points are different. That means a point in the plane is uniquely specified by its *distances to three noncollinear points*. But on a regular polygon there is a sharper result.

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

Proof. Let A and B be adjacent vertices of a regular polygon, so the line segment $\overline{AB}$ is an edge of the polygon.

We want to show different points P and Q on the polygon can't have the same distance to A and the same distance to B. If they did, then P and Q would lie on two circles C_A and C_B centered at A and B. Since $C_A \cap C_B$ has size at most two, and P and Q lie in $C_A \cap C_B$, P and Q are the only points in $C_A \cap C_B$. However, that places P and Q on opposite sides of $\overline{AB}$, and a regular polygon doesn't have two of its points on opposite sides of an edge of the polygon: a regular polygon is always on one side of the line through an edge.

Therefore two points in a regular polygon can't share the same distance to both A and B, which means each point of the polygon is determined by its distances to A and B. $\qquad\square$

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

Proof. Our argument has two parts: first show $|D_n| \leq 2n$ then construct $2n$ different elements of D_n.

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

Pick two adjacent vertices of a regular n-gon, and call them A and B as in Figure 2 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.
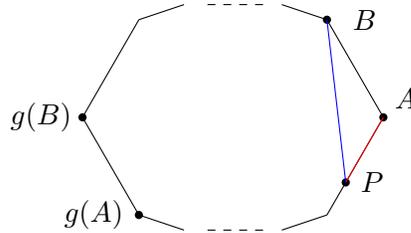

FIGURE 2. Effect of $g \in D_n$ on vertices A and B.

For each point P on the polygon, the location of $g(P)$ is determined by its distances to the adjacent vertices $g(A)$ and $g(B)$ by Lemma 2.1, so g is determined by $g(A)$ and $g(B)$. Thus to bound $|D_n|$, it suffices to bound 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 $g(A)$, the vertex $g(B)$ has at most 2 possibilities (it is 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 in Figure 1: 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. $\square$

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. $\square$

Let s be a reflection across a line *through a vertex*. See examples in Figure 3 below.[3] A reflection has order 2, so $s^2 = 1$ and $s^{-1} = s$.
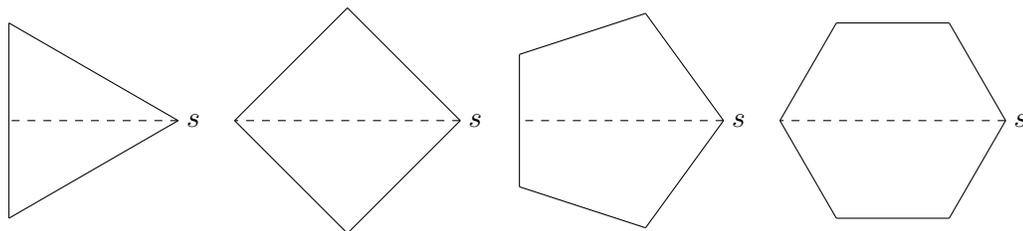

FIGURE 3. Some lines of reflection for $n = 3, 4, 5, 6$.

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

---

[3] The convention here that s denotes a reflection across a line through a vertex matters only for even n, where there are some reflections across a line that does not pass through a vertex, namely a line connecting midpoints of opposite sides. When n is odd, all reflections fix a line through a vertex, and any of them could be used as 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, each r^ks is a reflection. $\qquad\square$

The elements of D_n are rotations or reflections; there is no "mixed rotation-reflection": the product of a rotation r^i and a reflection r^js (in either order) is just 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 Figure 4. 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.
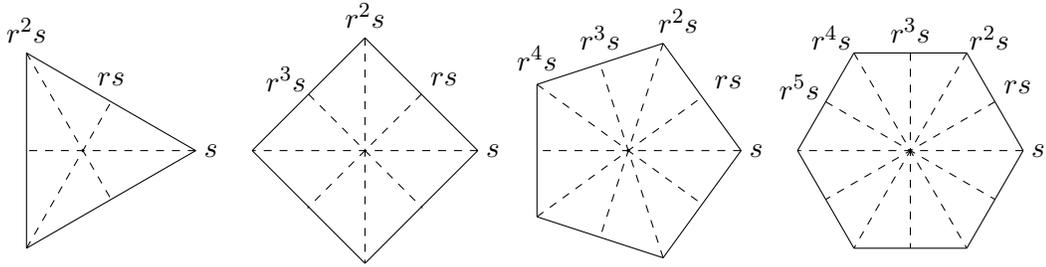

FIGURE 4. Lines of reflection in D_n labeled by element of D_n fixing them.

Let's summarize what we have now found.

Theorem 2.5. *The group D_n has $2n$ elements. As a list,*

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

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

Warning. Although each element of D_n with order greater than 2 has to be a power of r, because the non-rotations are reflections and thus have order 2, 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,*

$$(3.1) \qquad srs^{-1} = r^{-1}.$$

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 srs^{-1}. 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 Figure 5, where the dashed line through A is fixed by s. We have $r(A) = B$, $r^{-1}(A) = B'$, $s(A) = A$, and $s(B) = B'$.
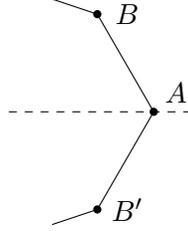

FIGURE 5. A vertex A and two adjacent vertices B and B'.

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 $srs^{-1} = r^{-1}$. $\quad\square$

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

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

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

$$(3.3) \qquad\qquad sr^k = r^{-k}s, \quad r^k s = sr^{-k}$$

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)

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

and

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

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, *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.

Remark 3.3. The group $D_5 = \{1, r, r^2, r^3, r^4, s, rs, r^2 s, r^3 s, r^4 s\}$ has order 10 and is non-abelian, so it is fundamentally different from $\mathbf{Z}/(10)$ despite having the same size. To detect incorrectly typed or scanned commercial product ID numbers (ISBN for books, UPC for supermarket items, VIN for cars, *etc.*), they often include an additional number called a check digit. The check digit, which is based on the rest of the ID number, is sometimes computed by a calculation mod 10, and some methods of computing a check digit can detect all single-digit errors (misreading one digit in an ID number), and many adjacent transposition errors (*e.g.*, misreading $\ldots 29 \ldots$ as $\ldots 92 \ldots$), but using mod 10 can't detect every adjacent transposition error. By labeling the 10 elements of D_5 with $0, 1, \ldots, 9$, Verhoeff [5, Chap. 4] used the nonabelian group law in D_5 to create a novel method of assigning check digits to ID numbers that detects all single-digit errors and all adjacent transposition errors. It has never been widely adopted in practice, even after the basic idea was rediscovered by Gumm [1]. Other references about this potential application of dihedral groups are [2], [3], [4, Chap. 5] and [6].

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 3.4. *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 reflection is in the center of D_n since reflections do not commute with r:

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

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

Suppose a rotation r^j is in the center of D_n. Without loss of generality, $0 \leq j < n$. Having r^j in $Z(D_n)$ implies $r^j s = s r^j$, which is equivalent to $r^j s = r^{-j} s$, so $r^j = r^{-j}$. Thus $r^{2j} = 1$. Since r has order n, from $r^{2j} = 1$ we get $n \mid 2j$, and $0 \leq 2j < 2n$. The only multiples of n in $\{0, 1, \ldots, 2n-1\}$ are 0 and n, so $2j = 0$ or $2j = n$. If $2j = 0$ then $j = 0$, so $r^j = r^0 = 1$. If $2j = n$ then (i) n is even and (ii) $j = n/2$, so $r^j = r^{n/2}$, which is a 180-degree rotation.

If n is odd then the only option is $j = 0$, so $r^j = 1$. Obviously $1 \in Z(D_n)$, so $Z(D_n) = \{1\}$.

If n is even then r^j is 1 or $r^{n/2}$. Again, obviously $1 \in Z(D_n)$. Is $r^{n/2}$ in $Z(D_n)$? Let's check $r^{n/2}$ commutes with every rotation and reflection in D_n. Clearly $r^{n/2}$ commutes with every r^i, since all powers of r commute with each other. Now we check $r^{n/2}$ commutes with each reflection $r^i s$:

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

where $r^{n/2} = r^{-n/2}$ because this follows from $r^n = 1$. (That $r^{n/2}$ is its own inverse also makes sense geometrically, since rotating by $180°$ or $-180°$ has the same effect.) $\square$

Example 3.5. The group D_3 has trivial center. The group D_4 has center $\{1, r^2\}$.

For even n, the rotation $r^{n/2}$ on a regular n-gon is by 180 degrees. Theorem 3.4 says this rotation for even n is the only nontrivial rigid motion of a regular n-gon that commutes with all other rigid motions of the n-gon. A 180-degree rotation around the origin commutes with all rigid motions of $\mathbf{R}^2$ fixing the origin, but a 180-degree rotation is not in D_n for odd n because a regular n-gon for odd n is not carried back to itself by a 180-degree rotation.

4. CONJUGACY

In D_n the geometric description of reflections depends on the parity of n: for odd n, the lines of reflection all 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 6 and 7.
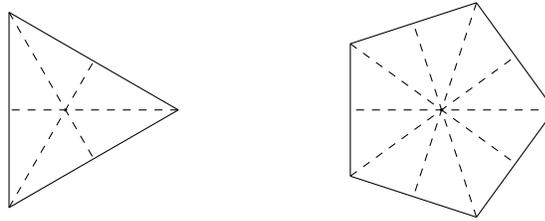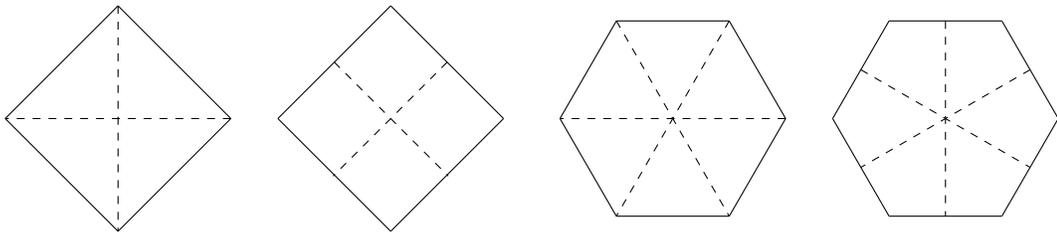

FIGURE 6. Lines of Reflection for $n = 3$ and $n = 5$.

FIGURE 7. Lines of Reflection for $n = 4$ and $n = 6$.

The geometrically different types of reflections in D_n for even n arise algebraically in the conjugacy classes of D_n: the conjugacy class of g is all xgx^{-1} for $x \in D_n$.

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 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 7: 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 $sr^j s^{-1} = r^{-j}$ 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 we can solve $k \equiv 2i \bmod n$ for i given k). Therefore when n is odd

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

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:

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

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

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 $[g, h]$. (We have $[g, h] = e$ if and only if $gh = hg$, so the commutator is related to commuting.) The set of commutators in a group contains the identity and it is closed under inversion since $[g, h]^{-1} = hgh^{-1}g^{-1} = [h, g]$, but it is not necessarily closed under multiplication. For example, the matrix $-I_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{R})$ is a product of commutators since $-I_2 = (\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right))^2$ and each matrix on the right side is a commutator in $\mathrm{SL}_2(\mathbf{R})$: $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = [\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1/2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1/3 \\ 0 & 1 \end{smallmatrix}\right)]$ and $\left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right) = [\left(\begin{smallmatrix} 1 & 0 \\ 2/3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1/2 & 0 \\ 0 & 2 \end{smallmatrix}\right)]$. However, $-I_2$ is *not* a commutator in $\mathrm{SL}_2(\mathbf{R})$.[4] So the set of commutators in a group may not be a subgroup.

What is the set of commutators in dihedral groups?

Theorem A.1. *The commutators in D_n form the subgroup $\langle r^2 \rangle$.*

---

[4]See the answer by Tom Goodwillie in https://mathoverflow.net/questions/44269/. Note $-I_2$ is a commutator in the larger group $\mathrm{GL}_2(\mathbf{R})$: $-I_2 = [\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)]$.

Proof. The commutator $[r, s]$ is $rsr^{-1}s^{-1} = rrss^{-1} = r^2$, so r^2 is a commutator. More generally, $[r^i, s] = r^i sr^{-i}s^{-1} = r^i r^i ss^{-1} = r^{2i}$, 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.

$\underline{\text{Case 1}}$: g and h are rotations.

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

$\underline{\text{Case 2}}$: g is a rotation and h is a reflection.

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

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

$\underline{\text{Case 3}}$: g is a reflection and h is a rotation.

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

$\underline{\text{Case 4}}$: g and h are reflections.

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

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

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

References

[1] H. Peter Gumm, "A new class of check-digit methods for arbitrary number systems," IEEE Transactions on Information Theory **31** (1985), 102–105. URL https://www.mathematik.uni-marburg.de/~gumm/Papers/ANewClassOfCheckDigitMethods.pdf.

[2] J. A. Gallian, "The mathematics of identification numbers," *The College Math. Journal* **22** (1991), 194–202. URL https://www.d.umn.edu/~jgallian/ident.pdf.

[3] J. A. Gallian, "Error detection methods," *ACM Computing Surveys* **28** (1996), 504–517.

[4] J. Kirtland, *Identification Numbers and Check Digit Schemes*, MAA, Washington, DC, 2001.

[5] J. Verhoeff, *Error Detecting Decimal Codes*, The Mathematical Centre, Amsterdam, 1969. URL https://ir.cwi.nl/pub/13046.

[6] S. J. Winters, "Error detecting schemes using dihedral groups," *The UMAP Journal* **11** (1990), 299–308.