DIHEDRAL GROUPS

KEITH CONRAD

1. Introduction

For $n \geq 3$, the dihedral group D_n is defined as the rigid motions of the plane preserving a regular n-gon, with the operation of composition. Our model n-gon will be an n-gon centered at the origin, with vertices at the n-th roots of unity. For example, a rotation by a multiple of $2\pi/n$ radians carries this n-gon back to itself, and thus is an element of D_n. There are also several reflections across various lines which bring this n-gon back to itself (*e.g.*, reflection across the x-axis), and such reflections are also in D_n.

In this handout, we will look at various elementary aspects of dihedral groups: an explicit list of the elements, relations between rotations and reflections in this group, and systems of generators.

Throughout, $n \geq 3$.

2. Finding the elements of D_n

Theorem 2.1. *The size of* D_n *is at most* $2n$.

Proof. (Sketch) A rigid motion preserving our model n-gon has to carry vertices to other vertices. The vertex at 1 can go to any of n positions. Then the next vertex (say, measured counterclockwise from 1) has only 2 choices of where to go, namely one of the vertices adjacent to the vertex where 1 was sent. Once we fix where this second vertex goes, we can "see" by the geometry that the positions where every other point on the n-gon must go is completely determined. Thus, each rigid motion in D_n is determined by where it sends 1 and where it sends the next vertex counterclockwise past 1. There are a total of $n \cdot 2 = 2n$ decisions to make, each one completely determining where every other point goes, so $\#D_n \leq 2n$. $\square$

Now we want to show the upper bound is reached, by writing down $2n$ different rigid motions. We will find exactly half of them are rotations and half of them are reflections. Along the way, we will work out a fundamental formula linking rotations and reflections.

There are two standard ways to think about points in the plane: as vectors or as complex numbers. We will adopt the complex number point of view, since the corresponding calculations are less involved notationally.

Before starting, we recall how complex conjugation on $\mathbf{C}$ interacts with the complex numbers both algebraically and geometrically. For a complex number $z = a+bi$, its complex conjugate is $\overline{z} = a - bi$. Complex conjugation "commutes" with addition and multiplication of complex numbers:

$$\overline{z+w} = \overline{z} + \overline{w}, \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}. \tag{2.1}$$

(Thus, by an easy induction, the conjugate of any finite sum or product of terms if the sum or product of the conjugates of those terms, *e.g.*, $\overline{z^2} = \overline{z}^2$.) The length of z is $|z| = \sqrt{a^2+b^2}$, and in particular

$$|z| = |\overline{z}|. \tag{2.2}$$

Our basic motions in D_n are a rotation r_n which goes counterclockwise by $2\pi/n$ radians and the reflection s across the x-axis. We will think about the points in the plane as complex numbers and represent these transformations as functions of complex numbers:

$$r_n(z) = \rho_n z, \quad s(z) = \overline{z}. \tag{2.3}$$

We write ρ_n for the basic n-th root of unity $\cos(2\pi/n) + i\sin(2\pi/n)$. Multiplication by ρ_n is a rotation. (A special case you can check is that multiplying by i rotates complex numbers $\pi/2$ radians $= 90$ degrees counterclockwise. This is the case $n = 4$: $r_4(z) = iz$.)

A transformation $T\colon \mathbf{C} \to \mathbf{C}$ that preserves distances ($|T(z) - T(w)| = |z - w|$ for all z and w in $\mathbf{C}$) is called a *rigid motion* or *isometry*. Let's check (2.3) defines rigid motions, using (2.1) and (2.2):

$$|r_n(z) - r_n(w)| = |\rho_n z - \rho_n w| = |\rho_n(z - w)| = |\rho_n||z - w| = |z - w|$$

and

$$|s(z) - s(w)| = |\overline{z} - \overline{w}| = |\overline{z - w}| = |z - w|.$$

If you prefer matrices to complex numbers, we can also realize r_n and s as matrix transformations on $\mathbf{R}^2$:

$$r_n\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, \quad s\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

However, the notation of complex numbers is much more concise than that of matrices, so we use complex numbers.

It is standard to drop the subscript n on r_n, and just speak about the basic rotation r in D_n. This of course can lead to ambiguity, as 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 a single value of n, there shouldn't be any confusion. (Notice s has no need for a subscript from the start: it is always complex conjugation, for any n.)

From the rotation r, we get n rotations in D_n by taking its powers (r has order n):

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

(Note how we adopt common group-theoretic notation and designate the identity rigid motion simply as 1.) As an explicit transformation on complex numbers, r^k has the effect of multiplication by ρ_n^k:

$$r(z) = \rho_n z \Longrightarrow r^k(z) = \rho_n^k(z).$$

Here r^k means the k-fold composite of r with itself (using inverses if $k < 0$), while ρ_n^k is the k-th power of ρ_n.

The order of s is 2: $s^2(z) = \overline{\overline{z}} = z$. The reflection s is not a power of r. For instance, s fixes the vertex 1 but is not the identity, while no power of r fixes the vertex 1 except for the identity r^n. Another way to see s is not a power or r is to check that r and s do not commute. In fact, their commutation relation is a fundamental formula for computations in D_n, and goes as follows.

Theorem 2.2. *In D_n,*

$$srs^{-1} = r^{-1}. \tag{2.4}$$

Since s has order 2, we can write this as $srs = r^{-1}$, but (2.4) stresses the conjugation aspect.

Proof. To check (2.4), we can think about r and s as functions of either complex numbers or of vectors. Taking the complex number point of view, for any $z \in \mathbf{C}$ we have (using (2.1))

$$\begin{aligned} srs^{-1}(z) &= srs(z) \\ &= \overline{r(\overline{z})} \\ &= \overline{\rho_n \overline{z}} \\ &= \overline{\rho}_n \overline{\overline{z}} \\ &= \overline{\rho}_n z. \end{aligned}$$

Since ρ_n is a root of unity, it has length 1:

$$1 = |\rho_n|^2 = \rho_n \overline{\rho}_n.$$

Therefore $\overline{\rho}_n = \rho_n^{-1}$: complex conjugation inverts ρ_n. Thus

$$srs^{-1}(z) = \rho_n^{-1} z = r^{-1}(z).$$

Since this holds for every $z \in \mathbf{C}$, $srs^{-1} = r^{-1}$. The reader can verify (2.4) using the matrix realizations of r and s too. Those calculations are a bit more tedious. $\square$

Check the following two equations are equivalent ways of writing (2.4), keeping in mind that s has order 2 (so $s^{-1} = s$):

$$sr = r^{-1}s, \quad rs = sr^{-1}. \tag{2.5}$$

What these mean is we can move r to the other side of s by just inverting it. By induction (or by raising both sides of (2.4) to an integral power), you can check

$$sr^k = r^{-k}s, \quad r^k s = sr^{-k} \tag{2.6}$$

for any integer k. In other words, any power of r can be moved to the other side of s by inversion.

Example 2.3. Each of $s, rs, r^2s, \ldots, r^{n-1}s$ has order 2 since, using (2.6),

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

The elements in Example 2.3 are different from each other (since they arise as different powers of r all multiplied on the same side by s). Are they different from the powers of r? Sure, since if $r^k s = r^i$ for some i we get $s = r^{i-k}$, so s is a power of r. But this is false.

In Example 2.3 we found n new elements of D_n, and these exhaust the upper bound on $\#D_n$ in Theorem 2.1.

Let's summarize what we have now found.

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

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}, \tag{2.7}$$

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

Persuade yourself, by looking at the cases $n = 3, 4, 5$, and 6 that the elements of order 2 in Example 2.3 are reflections across different lines. When n is odd, each reflection in D_n is across a line connecting a vertex to the midpoint of the opposite side. When n is even, half the reflections in D_n are across lines connecting opposite vertices and the other half are across lines connecting midpoints of opposite edges. That all reflections for odd n can be described in the same way, while reflections for even n come in two flavors, will manifest itself later in our consideration of conjugacy classes in D_n.

It's worth bearing in mind that every element of D_n is either a rotation or a reflection. There is no such thing as a "rotation-reflection": the product of a rotation r^i and a reflection $r^j s$ is always another reflection $r^{i+j}s$.

Corollary 2.5. *The group D_n is generated by r and s or by s and rs:*

$$D_n = \langle r, s\rangle = \langle s, rs\rangle.$$

Proof. Every element of D_n is a product of powers of r and s, so $D_n = \langle r, s\rangle$. Since $r = rs \cdot s$, we can write any element in terms of rs and s instead. □

The interesting aspect of the generating set s and rs is that they are both reflections, and thus of order 2: D_n can be generated not only by an element of order n and an element of order 2, but also by two elements of order 2.

3. Relations between rotations and reflections

Geometrically, the elements of D_n are rotations and reflections. In (2.7), the first n elements are rotations and the last n elements are reflections across different lines.

The relation (2.5) involves a particular rotation and a particular reflection in D_n. In (2.6), we extended (2.5) to any rotation and a particular reflection in D_n. Can we extend (2.6) to any rotation and any reflection in D_n? Any reflection in D_n has the form $r^k s$, so we can multiply any reflection and any rotation using (2.6):

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

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. Or, stated in terms of conjugation,

$$(r^i s)r^j(r^i s)^{-1} = r^{-j}, \tag{3.1}$$

so *any* rotation is conjugated to its inverse by *any* reflection. This geometric description makes such algebraic formulas easier to remember and understand.