Dihedral Groups

R. C. Daileda

Let $n \geq 3$ be an integer and consider a regular closed n-sided polygon P_n in $\mathbb{R}^2$. Cut P free from $\mathbb{R}^2$ along its edges, (rigidly) manipulate it in $\mathbb{R}^3$, and return P_n to fill the hole in $\mathbb{R}^2$ that was left behind. This yields a bijection of P_n with itself, one that maps edges to edges, and pairs of adjacent vertices to adjacent vertices. The set of all such elements in $\mathrm{Perm}(P_n)$ obtained in this way is called the *dihedral group (of symmetries of P_n)* and is denoted by D_n.[1] We claim that D_n is a subgroup of $\mathrm{Perm}(P_n)$ of order $2n$.

Since we can always just leave P_n unmoved, D_n contains the identity function. And since any manipulation of P_n in $\mathbb{R}^3$ that yields an element of D_n can certainly be reversed, D_n contains the inverse of every one of its elements. And since manipulating P_n in $\mathbb{R}^3$, returning it to the plane, picking it up and manipulating it again, and then returning it once more to $\mathbb{R}^2$, can be considered a single 3-D manipulation, we find that D_n is closed under composition. This proves that D_n is a subgroup of $\mathrm{Perm}(P_n)$.[2]

Now we need to count D_n. Every element of D_n can be described in terms of the final position of P_n after spatial manipulation. Before moving P_n, label its vertices with $1, 2, \ldots, n$ in counterclockwise order, starting with some fixed vertex. Label the vertices of its "hole" (complement in $\mathbb{R}^2$) to match. After P_n has been manipulated and returned to the plane to yield an element of D_n, vertex 1 of P_n will be in the position of the complement vertex labelled i for some i, and the labels of the remaining vertices of P_n will either increase in clockwise or counterclockwise order. Since there are n positions where vertex 1 can land, and two possible orientations for the remaining labels, we find that there are at most $2n$ final positions of P_n after being manipulated. Since it is clear that every such final orientation is possible to achieve, we conclude that $|D_n| = 2n$.

To describe D_n group theoretically, we need to construct some (fairly) specific elements of D_n. First, let $r \in D_n$ denote a counterclockwise *rotation* of P_n about its center by $2\pi/n$ radians. It should be clear that as a transformation of P_n, r has order n. Now let $f \in D_n$ denote any manipulation that flips P_n "upside down" and then puts it back (in any way at all). This will put all of the labels of P_n in clockwise order. For any $0 \leq k \leq n-1$, $r^k f$ maintains this property, and no two of these are identical since $|r| = n$. The powers r^k, $0 \leq k \leq n-1$, on the other hand, preserve the original counterclockwise ordering on the vertices of P_n, and are also distinct. Thus,

$$D_n = \{r^k f^e \mid 0 \leq k \leq n-1, e \in \{0, 1\}\}, \tag{1}$$

and the exponents in each element are unique.[3] In particular, r and f generate D_n.

[1] Be aware that some authors use the notation D_{2n} for the same group.
[2] The author first heard this particular "physical" description of D_n from Matt Galla, a former Trinity mathematics student.
[3] This actually makes D_n a *semi-direct* product, which we'll discuss below.

The order-reversing elements $r^k f \in D_n$ are called *flips* of P_n. It may seem intuitively obvious, but all flips have order 2, as we shall now prove. We begin by proving that $f^2 = e$. Suppose that f maps vertex 1 to the ith position. Then, because the vertex labels increase in clockwise order, vertex i maps to the $i-(i-1) = 1$ position. Thus f^2 will map vertex i to vertex i. Since it flips P over twice, the vertex labels must increase in the counterclockwise order once again. Since one vertex has been fixed, this means they all are, so that $f^2 = e$, as expected. The same reasoning applies to any element of D_n that reverses vertex label order, so that $(r^k f)^2 = e$ for all k. That is

$$e = (r^k f)(r^k f) = r^k(fr^k f) \quad \Leftrightarrow \quad fr^k f = r^{-k}. \tag{2}$$

When $k = 1$, in particular we have

$$frf = r^{-1}. \tag{3}$$

Two observations are in order. First, since f was taken to be an arbitrary flip, (2) shows that (3) actually holds for all rotations r and all flips f. Second, because conjugation is an automorphism, the more general (2) is a consequence of (3).

The equation $frf = r^{-1}$ can be rewritten as $fr = r^{-1}f$. This gives us a rule for computing products in D_n. Let $x, y \in D_n$ and write $x = r^k f^e$, $y = r^\ell f^d$, as above. If $e = 0$, then $xy = r^{k+\ell} f^d$, and $k + \ell$ can be reduced modulo n to get an element in (1). Otherwise, the conjugation relation (3) implies that

$$xy = r^k f r^\ell f^d = r^{k-\ell} f^{d+1}.$$

Now reduce $k - \ell$ modulo n and $d + 1$ modulo 2 to once again get into (1). So we see that, together with the orders of r and f, the conjugation relationship (3) completely determines the group structure of D_n.

Hence D_n can be completely described in terms of the *presentation*

$$D_n = \langle r, f \,:\, |r| = n, |f| = 2, frf = r^{-1} \rangle. \tag{4}$$

Any group generated by two elements satisfying these relations must necessarily be isomorphic to D_n. As an example, we use the presentation (4) to prove a classification theorem for groups of order $2p$, where p is an odd prime.

Theorem 1. *Let p be an odd prime and G a group of order $2p$. Then G is either cyclic or $G \cong D_p$.*

Proof. Suppose G is not cyclic. Note that since p is prime, this means every element of G must have order $1, 2$ or p. We must show that $G \cong D_p$. We first claim that G has an element of order p. If not, every nonidentity element of G has order 2, which makes G a finite elementary abelian 2-group. Thus

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$$

for a finite number of copies of $\mathbb{Z}/2\mathbb{Z}$. But then $|G|$ is a power of 2, which is impossible.

Let $r \in G$ have order p and set $H = \langle r \rangle$. Since $[G : H] = 2$, $H \lhd G$ and G/H is a group of order 2. Let $f \in G \setminus H$. Then we must have $H = (fH)^2 = f^2 H$ so that $f^2 \in H$. We claim that $f^2 = e$ and $|f| = 2$. If this were not the case, then since $f \neq e$, $|f| = p$, and p is odd, we would find that

$$e = f^p \;\Rightarrow\; f = f^{p+1} = (f^2)^{\frac{p+1}{2}} \in H,$$

contrary to our choice of f. This proves that every element of $G \setminus H$ has order 2.

Now fix $f \in G \setminus H$ and notice that H and $fH = Hf$ are the two disjoint cosets of H in G. It follows that $G = H \cup Hf = \langle r, f\rangle$. Moreover, $rf \notin H$, so that by what we have shown above, $|rf| = 2$. Hence

$$e = (rf)(rf) = r(frf) \;\Leftrightarrow\; frf = r^{-1}.$$

So we finally find that

$$G = \langle r, f \;:\; |r| = p, |f| = 2, frf = r^{-1}\rangle \cong D_p.$$

$\square$

Let H and G be groups and suppose we have we have a homomorphism $\psi : G \to \mathrm{Aut}(H)$. This generalizes the situation when $H \lhd G$ and we let G act on H by conjugation. To simplify notation, write ψ_x for $\psi(x)$. We define the *semi-direct product* of H and G to be the set $H \times G$ together with the following binary operation:

$$(a, x) \times_\psi (b, y) = (a\psi_x(b), xy).$$[4]

It is not hard to see that (e, e') is the identity under $\times_\psi$, and a somewhat tedious computation, using that ψ is a homomorphism, verifies that $\times_\psi$ is associative. Finally, one can show that the inverse of (a, x) under $\times_\psi$ is $(\psi_{x^{-1}}(a^{-1}), x^{-1})$. That is, $H \times G$ with $\times_\psi$ is a group.

The semi-direct product of H and G by ψ is denoted

$$H \rtimes_\psi G$$

or just $H \rtimes G$ when ψ is clear from context. The semi-direct product generalizes the following scenario, among others. Suppose G is a group, $N \lhd G$, $H < G$ and $G = NH$. H acts as automorphism of N by conjugation and for $n_1, n_2 \in N$, $h_1, h_2 \in H$ we have

$$(n_1h_1)(n_2h_2) = n_1h_1n_2h_1^{-1}h_1h_2 = (n_1\underbrace{h_1n_2h_1^{-1}}_{\text{in } N})(h_1h_2).$$

So we have multiplied two elements of NH in the same way that we would multiply elements of $N \rtimes H$, with H acting as inner automorphisms of N. If $N \cap H = \{e\}$, one can show that, in fact, $NH \cong N \rtimes H$ in this way.

We can now use the semi-direct product to give a structural description of D_n.

Theorem 2. *Let $n \geq 3$. Choose $r_0 \in D_n$ of order n and let $R_n = \langle r_0\rangle$ denote the subgroup of rotations of P_n. Choose any flip $f \in D_n \setminus R_n$. Then $R_n \lhd D_n$ and*

$$D_n = R_n \rtimes_\psi \langle f\rangle,$$

where $\psi_f(r) = r^{-1}$ for all $r \in R_n$.[5]

[4] One of my favorite algebra professors once described this operation as the ordinary direct product, but with x "getting in the way" of the multiplication in the first coordinate. This isn't perhaps the best way to think about what this construction is actually trying to accomplish, but it's a good way to remember the formula for $\times_\psi$.

[5] ψ_f "negates" in the abelian group R_n.

Proof. Let $H = \langle f \rangle$. Because $|r| = n$, $[D_n : R_n] = 2$, so that $R_n \lhd D_n$. Since we already know that $D_n = R_n H$ and $R_n \cap H = \{e\}$, the preceding discussion tells us that $D_n = R_n \rtimes_\psi H$, where ψ gives the conjugation action of H on R_n. Since the only nonidentity element of H is f, it suffices to specify $\psi_f(r) = frf^{-1} = frf = r^{-1}$ for all $r \in R_n$, by the comments following (3). $\square$

As a final remark, we note that the semi-direct product includes the direct product as a special case, namely when $\psi \equiv 1_H$.