DIHEDRAL GROUPS II

KEITH CONRAD

We will characterize dihedral groups in terms of generators and relations, and describe the subgroups of D_n, including the normal subgroups. We will also introduce an infinite group that resembles the dihedral groups and has all of them as quotient groups.

1. Abstract characterization of D_n

The group D_n has two generators r and s with orders n and 2 such that $srs^{-1} = r^{-1}$. We will show every group with a pair of generators having properties similar to r and s admits a homomorphism onto it from D_n, and is isomorphic to D_n if it has the same size as D_n.

Theorem 1.1. *Let a group G be generated by elements x and y where $x^n = 1$ for some $n \geq 3$, $y^2 = 1$, and $yxy^{-1} = x^{-1}$. There is a surjective homomorphism $D_n \to G$, and if G has order $2n$ then this homomorphism is an isomorphism.*

The hypotheses $x^n = 1$ and $y^2 = 1$ do *not* mean x has order n and y has order 2, but only that their orders divide n and divide 2. For instance, the trivial group has the form $\langle x, y \rangle$ where $x^n = 1$, $y^2 = 1$, and $yxy^{-1} = x^{-1}$ (take x and y to be the identity).

Proof. The equation $yxy^{-1} = x^{-1}$ implies $yx^jy^{-1} = x^{-j}$ for all $j \in \mathbf{Z}$ (raise both sides to the jth power). Since $y^2 = 1$, we have for all $k \in \mathbf{Z}$

$$y^k x^j y^{-k} = x^{(-1)^k j}$$

by considering even and odd k separately. Thus for all $j, k \in \mathbf{Z}$,

$$y^k x^j = x^{(-1)^k j} y^k. \tag{1.1}$$

This shows each product of x's and y's (like $y^5x^{-7}y^3x^2y^{-4}x^{21}$) can have all the x's brought to the left and all the y's brought to the right. So *every element of G looks like x^ay^b*. Taking into account that $x^n = 1$ and $y^2 = 1$, we can say

$$\begin{aligned} G &= \langle x, y \rangle \\ &= \{x^j, x^jy : j \in \mathbf{Z}\} \\ &= \{1, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}. \end{aligned} \tag{1.2}$$

Thus G is a finite group (we had not assumed G is finite) with $|G| \leq 2n$.

To write down an explicit homomorphism from D_n onto G, the equations $x^n = 1$, $y^2 = 1$, and $yxy^{-1} = x^{-1}$ suggest we should be able send r to x and s to y by a homomorphism. This suggests the function $f\colon D_n \to G$ defined by

$$f(r^js^k) = x^jy^k.$$

This equation defines f on all of D_n since all elements of D_n have the form r^js^k for some j and k.[1] To see f is well-defined, the only ambiguity in writing an element of D_n as r^js^k is

[1] See Theorem 2.5 in https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf.

that j changes mod n and k changes mod 2: $r^js^k = r^{j'}s^{k'} \Rightarrow r^{j-j'} = s^{k'-k} \in \langle r\rangle \cap \langle s\rangle = \{1\}$, so $j' \equiv j \bmod n$ and $k' \equiv k \bmod 2$. Such changes to j and k have no effect on x^jy^k since $x^n = 1$ and $y^2 = 1$.

To check f is a homomorphism, we use (1.1):

$$\begin{aligned} f(r^js^k)f(r^{j'}s^{k'}) &= x^jy^kx^{j'}y^{k'} \\ &= x^jx^{(-1)^kj'}y^ky^{k'} \\ &= x^{j+(-1)^kj'}y^{k+k'} \end{aligned}$$

and

$$\begin{aligned} f((r^js^k)(r^{j'}s^{k'})) &= f(r^jr^{(-1)^kj'}s^ks^{k'}) \\ &= f(r^{j+(-1)^kj'}s^{k+k'}) \\ &= x^{j+(-1)^kj'}y^{k+k'}. \end{aligned}$$

The results agree, so f is a homomorphism from D_n to G. It is onto since every element of G has the form x^jy^k and these are all values of f by the definition of f.

If $|G| = 2n$ then surjectivity of f implies injectivity, so f is an isomorphism. □

Remark 1.2. The homomorphism $f\colon D_n \to G$ constructed in the proof is the only one where $f(r) = x$ and $f(s) = y$: if there is such a homomorphism then $f(r^js^k) = f(r)^jf(s)^k = x^jy^k$. So a more precise formulation of Theorem 1.1 is this: for each group $G = \langle x, y\rangle$ where $x^n = 1$ for some $n \geq 3$, $y^2 = 1$, and $yxy^{-1} = x^{-1}$, there is a *unique* homomorphism $D_n \to G$ sending r to x and s to y. Mathematicians describe this state of affairs by saying D_n with its generators r and s is "universal" as a group with two generators satisfying the three equations in Theorem 1.1: all such groups are homomorphic images of D_n.

As an application of Theorem 1.1, we can write down a matrix group over $\mathbf{Z}/(n)$ that is isomorphic to D_n when $n \geq 3$. Set

$$\widetilde{D}_n = \left\{ \begin{pmatrix} \pm 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbf{Z}/(n) \right\} \tag{1.3}$$

inside $\mathrm{GL}_2(\mathbf{Z}/(n))$. The group $\widetilde{D}_n$ has order $2n$ (since $1 \not\equiv -1 \bmod n$ for $n \geq 3$). Inside $\widetilde{D}_n$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2 and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order n. A typical element of $\widetilde{D}_n$ is

$$\begin{aligned} \begin{pmatrix} \pm 1 & c \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^c\begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

so $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ generate $\widetilde{D}_n$. Moreover, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$ are conjugate by $\left(\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$:

$$\begin{aligned} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}. \end{aligned}$$

Thus, by Theorem 1.1, $\widetilde{D}_n$ is isomorphic to D_n, using $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in the role of r and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in the role of s.

This realization of D_n inside $\mathrm{GL}_2(\mathbf{Z}/(n))$ should not be confused with the geometric realization of D_n in $\mathrm{GL}_2(\mathbf{R})$ using real matrices: $r = \left(\begin{smallmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{smallmatrix}\right)$ and $s = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

For even n, D_n has a nontrivial center $\{1, r^{n/2}\}$, where $r^{n/2}$ is a 180-degree rotation. When $n/2$ is odd, the center can be split off in a direct product decomposition of D_n.

Corollary 1.3. *If $n \geq 6$ is twice an odd number then $D_n \cong D_{n/2} \times \mathbf{Z}/(2)$.*

For example, $D_6 \cong D_3 \times \mathbf{Z}/(2)$ and $D_{10} \cong D_5 \times \mathbf{Z}/(2)$.

Proof. Let $H = \langle r^2, s\rangle$, where r and s are taken from D_n. Then $(r^2)^{n/2} = 1$, $s^2 = 1$, and $sr^2s^{-1} = r^{-2}$, so Theorem 1.1 tells us there is a surjective homomorphism $D_{n/2} \to H$. Since r^2 has order $n/2$, $|H| = 2(n/2) = n = |D_{n/2}|$, so $D_{n/2} \cong H$.

Set $Z = \{1, r^{n/2}\}$, the center of D_n. The elements of H commute with the elements of Z, so the function $f\colon H \times Z \to D_n$ by $f(h, z) = hz$ is a homomorphism. Writing $n = 2k$ where $k = 2\ell + 1$ is odd, we get $f((r^2)^{-\ell}, r^{n/2}) = r^{-2\ell+k} = r$ and $f(s, 1) = s$, so the image of f contains $\langle r, s\rangle = D_n$. Thus f is surjective. Both $H \times Z$ and D_n have the same size, so f is injective too and thus is an isomorphism. □

Figure 1 is a geometric interpretation of the isomorphism $D_6 \cong D_3 \times \mathbf{Z}/(2)$. Every rigid motion preserving the blue triangle also preserves the red triangle and the hexagon, and this is how D_3 naturally embeds into D_6. The quotient group D_6/D_3 has order 2 and it is represented by the nontrivial element of $\mathbf{Z}/(2)$, which corresponds to the nontrivial element of the center of D_6. That is a 180-degree rotation around the origin, and the blue and red equilateral triangles are related to each other by a 180-degree rotation.

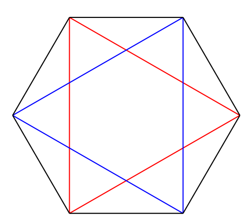

FIGURE 1. Two equilateral triangles inside a regular hexagon.

When $n \geq 6$ is twice an even number (*i.e.*, $4 \mid n$ and $n > 4$), the conclusion of Corollary 1.3 is false: $D_n \not\cong D_{n/2} \times \mathbf{Z}/(2)$. That's because n and $n/2$ are even, so the center of D_n has order 2 while the center of $D_{n/2} \times \mathbf{Z}/(2)$ has order $2 \cdot 2 = 4$. Since the groups D_n and $D_{n/2} \times \mathbf{Z}/(2)$ have nonisomorphic centers, the groups are nonisomorphic.

As an application of Theorem 1.1 and Remark 1.2 we can describe the automorphism group of D_n as a concrete matrix group.

Theorem 1.4. *For $n \geq 3$,*

$$\mathrm{Aut}(D_n) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(n))^\times, b \in \mathbf{Z}/(n) \right\}.$$

In particular, the order of $\mathrm{Aut}(D_n)$ is $n\varphi(n)$.

Proof. Each automorphism f of D_n is determined by where it sends r and s. Since $f(r)$ has order n and all elements outside $\langle r\rangle$ have order 2, which is less than n, we must have $f(r) = r^a$ with $(a, n) = 1$, so $f(\langle r\rangle) = \langle r\rangle$. Then $f(s) \notin \langle r\rangle$, so

$$f(r) = r^a, \quad f(s) = r^b s$$

where $a \in (\mathbf{Z}/(n))^\times$ and $b \in \mathbf{Z}/(n)$.

Conversely, for each $a \in (\mathbf{Z}/(n))^\times$ and $b \in \mathbf{Z}/(n)$, we will show a unique automorphism of D_n maps r to r^a and s to $r^b s$. By Theorem 1.1 and Remark 1.2, it suffices to show

- $(r^a)^n = 1$,
- $(r^b s)^2 = 1$,
- $(r^b s)(r^a)(r^b s)^{-1} = r^{-a}$.

That $(r^a)^n = 1$ follows from $r^n = 1$. That $(r^b s)^2 = 1$ follows from all elements of D_n outside $\langle r\rangle$ having order 2. To show the third relation,

$$(r^b s)(r^a)(r^b s)^{-1} = r^b s r^a s^{-1} r^{-b} = r^b r^{-a} s s^{-1} r^{-b} = r^b r^{-a} r^{-b} = r^{-a}.$$

We have shown $\mathrm{Aut}(D_n)$ is parametrized by pairs (a, b) in $(\mathbf{Z}/(n))^\times \times \mathbf{Z}/(n)$: for each (a, b), there is a unique $f_{a,b} \in \mathrm{Aut}(D_n)$ determined by the conditions $f_{a,b}(r) = r^a$ and $f_{a,b}(s) = r^b s$. For two automorphisms $f_{a,b}$ and $f_{c,d}$ of D_n,

$$(f_{a,b} \circ f_{c,d})(r) = f_{a,b}(r^c) = (f_{a,b}(r))^c = (r^a)^c = r^{ac}$$

and

$$(f_{a,b} \circ f_{c,d})(s) = f_{a,b}(r^d s) = (f_{a,b}(r))^d f_{a,b}(s) = r^{ad}(r^b s) = r^{ad+b} s,$$

so $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. Since $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right)$, the map $f_{a,b} \mapsto \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ is an isomorphism

$$\mathrm{Aut}(D_n) \to \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(n))^\times, b \in \mathbf{Z}/(n) \right\}. \qquad \square$$

Corollary 1.5. *For every pair of elements g and h in $D_n - \langle r\rangle$, there is a unique automorphism f of D_n such that f fixes all of $\langle r\rangle$ and $f(g) = h$.*

Proof. Each $f \in \mathrm{Aut}(D_n)$ is determined by $f(r) = r^a$ and $f(s) = r^b s$ where $a \in (\mathbf{Z}/(n))^\times$ and $b \in \mathbf{Z}/(n)$. That f fixes all of $\langle r\rangle$ means $a \equiv 1 \bmod n$. How can we force $f(g) = h$?

Write $g = r^i s$ and $h = r^j s$ for some i and j (unique modulo n). Then $f(g) = f(r)^i f(s) = r^i r^b s = r^{i+b} s$, so the condition $f(g) = h$ says $r^{i+b} s = r^j s$, or equivalently $b \equiv j - i \bmod n$. Therefore $f_{1,j-i}$ fixes $\langle r\rangle$, maps g to h, and is the only such automorphism of D_n. $\square$

2. Dihedral groups and generating elements of order 2

Since $D_n = \langle r, s\rangle = \langle rs, s\rangle$, D_n is generated by the two reflections s and rs. The reflections s and rs fix lines separated by an angle $2\pi/(2n)$, as illustrated in Figure 2 for $3 \leq n \leq 6$. A nice visual demonstration that s and rs generate D_n for $2 \leq n \leq 5$ is given[2] by Richard Borcherds in Lecture 13 of his online group theory course on YouTube: watch `https://www.youtube.com/watch?v=kHBDFx0ExcA` starting at 14:43. He uses the term "involution" rather than "reflection" since elements of order 2 in abstract groups are called involutions. (A 180-degree rotation in $\mathbf{R}^2$ is an involution that is not a reflection.)

Which finite groups besides D_n for $n \geq 3$ can be generated by two elements of order 2? Suppose $G = \langle x, y\rangle$, where $x^2 = 1$ and $y^2 = 1$. If x and y commute, then $G = \{1, x, y, xy\}$. This has size 4 provided $x \neq y$. Then we see G behaves just like the group $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$,

[2] We have not yet defined D_n for $n = 2$: D_2 is $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$. This will be explained after Theorem 2.1.

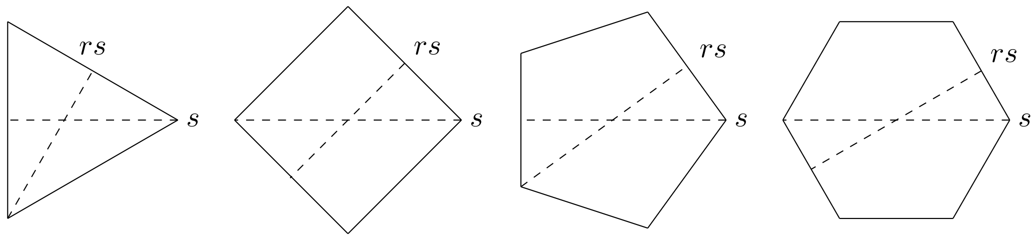

FIGURE 2. The reflections s and rs on a regular polygon.

where x corresponds to $(1, 0)$ and y corresponds to $(0, 1)$. If $x = y$, then $G = \{1, x\} = \langle x\rangle$ is cyclic of size 2. If x and y do not commute, then G is essentially a dihedral group!

Theorem 2.1. *Let G be a finite nonabelian group generated by two elements of order 2. Then G is isomorphic to a dihedral group.*

Proof. Let the two elements be x and y, so each has order 2 and $G = \langle x, y\rangle$. Since G is nonabelian and x and y generate G, x and y do not commute: $xy \neq yx$.

The product xy has some finite order, since we are told that G is a *finite* group. Let the order of xy be denoted n. Set $a = xy$ and $b = y$. (If we secretly expect x is like rs and y is like s in D_n, then this choice of a and b is understandable, since it makes a look like r and b look like s.) Then $G = \langle x, y\rangle = \langle xy, y\rangle$ is generated by a and b, where $a^n = 1$ and $b^2 = 1$. Since a has order n, $n \mid |G|$. Since $b \notin \langle a\rangle$, $|G| > n$, so $|G| \geq 2n$.

The order n of a is greater than 2. Indeed, if $n \leq 2$ then $a^2 = 1$, so $xyxy = 1$. Since x and y have order 2, we get

$$xy = y^{-1}x^{-1} = yx,$$

but x and y do not commute. Therefore $n \geq 3$. Since

$$bab^{-1} = yxyy = yx, \quad a^{-1} = y^{-1}x^{-1} = yx, \tag{2.1}$$

where the last equation is due to x and y having order 2, we obtain $bab^{-1} = a^{-1}$. By Theorem 1.1, there is a surjective homomorphism $D_n \to G$, so $|G| \leq 2n$. We saw before that $|G| \geq 2n$, so $|G| = 2n$ and $G \cong D_n$. $\square$

Theorem 2.1 says we know all the finite *nonabelian* groups generated by two elements of order 2. What about the finite abelian groups generated by two elements of order 2? We discussed this before Theorem 2.1. Such a group is isomorphic to $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ or (in the degenerate case that the two generators are the same element) to $\mathbf{Z}/(2)$. So we can *define* new dihedral groups of order 2 and 4:

$$D_1 := \mathbf{Z}/(2), \quad D_2 := \mathbf{Z}/(2) \times \mathbf{Z}/(2).$$

In terms of generators, $D_1 = \langle r, s\rangle$ where $r = 1$ and s has order 2, and $D_2 = \langle r, s\rangle$ where r and s have order 2 and they commute. With these definitions,

- $|D_n| = 2n$ for every $n \geq 1$,
- the dihedral groups are precisely the finite groups generated by two elements of order 2,
- the description of the commutators in D_n for $n > 2$ (namely, they are the powers of r^2) is true for $n \geq 1$ (commutators are trivial in D_1 and D_2, and so is r^2 in these cases),

- for even $n \geq 1$, Corollary 1.3 is true when n is twice an odd number (including $n = 2$) and false when n is a multiple of 4,
- the model for D_n as a subgroup of $\mathrm{GL}_2(\mathbf{R})$ when $n \geq 3$ is valid for all $n \geq 1$.

However, D_1 and D_2 don't satisfy all properties of D_n when $n > 2$. For example,

- D_n is nonabelian for $n > 2$ but not for $n \leq 2$,
- the description of the center of D_n when $n > 2$ (trivial for odd n and of order 2 for even n) is false when $n \leq 2$, where $Z(D_n) = D_n$ has order 2 for $n = 1$ and order 4 for $n = 2$,
- the matrix model for D_n over $\mathbf{Z}/(n)$ in (1.3) is invalid when $n \leq 2$,
- the matrix model for $\mathrm{Aut}(D_n)$ over $\mathbf{Z}/(n)$ in Theorem 1.4 doesn't work when $n = 2$: $\mathrm{Aut}(D_2) = \mathrm{GL}_2(\mathbf{Z}/(2))$ has order 6, which is not $n\varphi(n)$ if $n = 2$.

Remark 2.2. Unlike finite groups generated by two elements of order 2, there is no elementary description of all the finite groups generated by two elements with equal order > 2 or all the finite groups generated by two elements with order 2 and n for some $n \geq 3$. As an example of how complicated such groups can be, most finite simple groups are generated by a pair of elements with order 2 and 3.

Theorem 2.3. *Nontrivial quotient groups of dihedral groups are isomorphic to dihedral groups: if $N \lhd D_n$ and H has index $m > 1$, then m is even and $D_n/N \cong D_{m/2}$.*

Proof. The group D_n/N is generated by $\overline{rs}$ and $\overline{s}$, which both square to the identity, so they have order 1 or 2 and they are not both trivial since D_n/N is assumed to be nontrivial. Thus $|D_n/N|$ is even, so m is even. If $\overline{rs}$ and $\overline{s}$ both have order 2 then $D_n/N \cong D_{m/2}$ by Theorem 2.1 if D_n/N if nonabelian, and D_n/N is isomorphic to $\mathbf{Z}/(2)$ or $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ if D_n/N is abelian, which are also dihedral groups by our convention on the meaning of D_1 and D_2. If $\overline{rs}$ or $\overline{s}$ have order 1 then only one of them has order 1, which makes $D_n/N \cong \mathbf{Z}/(2) = D_1$. $\square$

Example 2.4. For even $n \geq 3$, $Z(D_n) = \{1, r^{n/2}\}$, so $D_n/Z(D_n)$ has order $(2n)/2 = n = 2(n/2)$ and is generated by the images $\overline{r}$ (with order $n/2$ in $D_n/Z(D_n)$) and $\overline{s}$ (with order 2), subject to the relation $\overline{s}\,\overline{r}\,\overline{s}^{-1} = \overline{r}^{-1}$. Therefore $D_n/Z(D_n) \cong D_{n/2}$. Note for $n = 4$ that we are using the definition $D_2 := \mathbf{Z}/(2) \times \mathbf{Z}/(2)$. (For odd $n \geq 3$, $Z(D_n) = \{1\}$ so $D_n/Z(D_n) = D_n$, which is boring.)

Example 2.5. For $n \geq 3$, the commutator subgroup $[D_n, D_n]$ is $\langle r^2 \rangle$, which is $\langle r \rangle$ for odd n, so $D_n/[D_n, D_n]$ has order $(2n)/2n = 2$ for odd n and order $2n/(n/2) = 4$ for even n. The group $D_n/[D_n, D_n]$ is abelian and is generated by the images $\overline{r}$ and $\overline{s}$. where $\overline{s}$ has order 2. For odd n, $\overline{r}$ is trivial so $D_n/[D_n, D_n] = \langle \overline{s} \rangle \cong \mathbf{Z}/(2)$. For even n, $\overline{r}$ has order 2 and doesn't equal $\overline{s}$, so $D_n/[D_n, D_n] \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$. These formulas for $D_n/]D_n, D_n]$ equal D_1 for odd n and D_2 for even n.

We will see the proper normal subgroups of D_n in Theorem 3.8: besides subgroups of index 2 (which are normal in all groups) they turn out to be the subgroups of $\langle r \rangle$.

3. Subgroups of D_n

We will list all subgroups of D_n and then collect them into conjugacy classes of subgroups. Our results will be valid even for $n = 1$ and $n = 2$. Recall $D_1 = \langle r, s \rangle$ where $r = 1$ and s has order 2, and $D_2 = \langle r, s \rangle$ where r and s have order 2 and commute.

Theorem 3.1. *Every subgroup of D_n is cyclic or dihedral. A complete listing of the subgroups is as follows:*

(1) $\langle r^d\rangle$, *where* $d \mid n$, *with index* $2d$,
(2) $\langle r^d, r^i s\rangle$, *where* $d \mid n$ *and* $0 \le i \le d-1$, *with index* d.

Every subgroup of D_n occurs exactly once in this listing.

In this theorem, subgroups of the first type are cyclic and subgroups of the second type are dihedral: $\langle r^d\rangle \cong \mathbf{Z}/(n/d)$ and $\langle r^d, r^i s\rangle \cong D_{n/d}$.

Proof. It is left to the reader to check $n = 1$ and $n = 2$ separately. We now assume $n \ge 3$.

Let H be a subgroup of D_n. Since $\langle r\rangle$ is cyclic of order n, if $H \subset \langle r\rangle$ then $H = \langle r^d\rangle$ where $d \mid n$ (and $d > 0$). The order of $\langle r^d\rangle$ is n/d, so its index in D_n is $2n/(n/d) = 2d$.

Now assume $H \not\subset \langle r\rangle$, so H contains some $r^i s$. First we'll treat the case $s \in H$ and then we'll reduce the more general case (some $r^i s$ is in H) to the case $s \in H$.

The intersection $H \cap \langle r\rangle$ is a subgroup of $\langle r\rangle$, so it is $\langle r^d\rangle$ for some $d > 0$ that divides n. If $s \in H$ then let's show $H = \langle r^d, s\rangle$. We have $\langle r^d, s\rangle \subset H$ since r^d and s are in H. To prove the reverse containment, pick $h \in H$. If $h \in \langle r\rangle$ then $h \in H \cap \langle r\rangle = \langle r^d\rangle \subset \langle r^d, s\rangle$. If $h \notin \langle r\rangle$ then $h = r^i s$ for some i. Since $s \in H$, we get $r^i = hs^{-1} \in H \cap \langle r\rangle$, so $r^i = r^{dk}$ for some k. Thus $h = r^i s = r^{dk} s = (r^d)^k s \in \langle r^d, s\rangle$, so $H \subset \langle r^d, s\rangle$.

Consider now the case where $H \not\subset \langle r\rangle$ and we don't assume $s \in H$. In H is an element of the form $r^i s$. Since s and $r^i s$ are not in $\langle r\rangle$, by Corollary 1.5 there's an automorphism f of D_n such that $f(r) = r$ and $f(r^i s) = s$. Then $f(H)$ is a subgroup of D_n containing s, so by the previous paragraph $f(H) = \langle r^d, s\rangle$ where $d \mid n$ (and $d > 0$). Then $H = f^{-1}(\langle r^d, s\rangle) = \langle f^{-1}(r)^d, f^{-1}(s)\rangle = \langle r^d, r^i s\rangle$. Since $\langle r^d, r^i s\rangle = \langle r^d, r^j s\rangle$ when $j \equiv i \bmod d$, we can adjust $i \bmod d$ without affecting $\langle r^d, r^i s\rangle$ and thus write $H = \langle r^d, r^i s\rangle$ where $0 \le i \le d-1$.

What is the index of $\langle r^d, r^i s\rangle$ in D_n when $d \mid n$ and $d > 0$? Because $r^i s$ has order 2 and $(r^i s) r^k = r^{-k}(r^i s)$, all elements of $\langle r^d, r^i s\rangle$ that are not powers of r have the form $(r^d)^\ell (r^i s) = r^{d\ell} r^i s$. Thus $H = \langle r^d, r^i s\rangle = \langle r^d\rangle \cup \langle r^d\rangle r^i s$ (a disjoint union), so $|H| = 2|\langle r^d\rangle| = 2(n/d)$, which makes $[D_n : H] = 2n/(2(n/d)) = d$.

It remains to show the subgroups in the theorem have no duplications. First let's show the two lists are disjoint. Everything in $\langle r^d\rangle$ commutes with r while $\langle r^d, r^i s\rangle$ contain $r^i s$ that does not commute with r, so these types of subgroups are not equal.

Among subgroups on the first list, there are no duplications since $\langle r^d\rangle$ determines d when d is a positive divisor of n: it has index $2d$. If two subgroups of the second type are equal, then they have equal index in D_n, say d, so they must be $\langle r^d, r^i s\rangle$ and $\langle r^d, r^j s\rangle$ where i and j are in $\{0, \dots, d-1\}$. Then $r^j s \in \langle r^d, r^i s\rangle = \langle r^d\rangle \cup \langle r^d\rangle r^i s$, so $r^j s = r^{dk+i} s$ for some $k \in \mathbf{Z}$. Therefore $j \equiv dk + i \bmod n$. We can reduce both sides mod d, since $d \mid n$, to get $j \equiv i \bmod d$. That forces $j = i$ since $0 \le i, j \le d-1$. □

Corollary 3.2. *Let n be odd and $m \mid 2n$. If m is odd then there are m subgroups of D_n with index m. If m is even then there is one subgroup of D_n with index m.*

Let n be even and $m \mid 2n$.

- *If m is odd then there are m subgroups of D_n with index m.*
- *If m is even and m doesn't divide n then there is one subgroup of D_n with index m.*
- *If m is even and $m \mid n$ then there are $m+1$ subgroups of D_n with index m.*

Proof. Check $n = 1$ and $n = 2$ separately first. We now assume $n \ge 3$.

If n is odd then the odd divisors of $2n$ are the divisors of n and the even divisors of $2n$ are of the form $2d$, where $d \mid n$. From the list of subgroups of D_n in Theorem 3.1, each subgroup with odd index is dihedral and each subgroup with even index is inside $\langle r\rangle$ (since n is odd). A subgroup with odd index m is $\langle r^m, r^i s\rangle$ for a unique i from 0 to $m-1$, so there are m such subgroups. A subgroup with even index m must be $\langle r^{m/2}\rangle$ by Theorem 3.1.

If n is even and m is an odd divisor of $2n$, so $m \mid n$, the subgroups of D_n with index m are $\langle r^m, r^i s\rangle$ where $0 \leq i \leq m-1$. When m is an even divisor of $2n$, so $(m/2) \mid n$, $\langle r^{m/2}\rangle$ has index m. If m does not divide n then $\langle r^{m/2}\rangle$ is the only subgroup of index m. If m divides n then the other subgroups of index m are $\langle r^m, r^i s\rangle$ where $0 \leq i \leq m-1$. $\square$

From knowledge of all subgroups of D_n we can count conjugacy classes of subgroups.

Theorem 3.3. *Let n be odd and $m \mid 2n$. If m is odd then all m subgroups of D_n with index m are conjugate to $\langle r^m, s\rangle$. If m is even then the only subgroup of D_n with index m is $\langle r^{m/2}\rangle$. In particular, all subgroups of D_n with the same index are conjugate to each other.*

Let n be even and $m \mid 2n$.

- *If m is odd then all m subgroups of D_n with index m are conjugate to $\langle r^m, s\rangle$.*
- *If m is even and m doesn't divide n then the only subgroup of D_n with index m is $\langle r^{m/2}\rangle$.*
- *If m is even and $m \mid n$ then every subgroup of D_n with index m is $\langle r^{m/2}\rangle$ or is conjugate to exactly one of $\langle r^m, s\rangle$ or $\langle r^m, rs\rangle$.*

In particular, the number of conjugacy classes of subgroups of D_n with index m is 1 *when m is odd,* 1 *when m is even and m doesn't divide n, and* 3 *when m is even and $m \mid n$.*

Proof. As usual, check $n = 1$ and $n = 2$ separately first. We now assume $n \geq 3$.

When n is odd and m is odd, $m \mid n$ and every subgroup of D_n with index m is some $\langle r^m, r^i s\rangle$. Since n is odd, $r^i s$ is conjugate to s in D_n. The only conjugates of r^m in D_n are $r^{\pm m}$, and every conjugation sending s to $r^i s$ turns $\langle r^m, s\rangle$ into $\langle r^{\pm m}, r^i s\rangle = \langle r^m, r^i s\rangle$. When n is odd and m is even, the only subgroup of D_n with even index m is $\langle r^{m/2}\rangle$ by Theorem 3.1.

If n is even and m is an odd divisor of $2n$, so $m \mid n$, a subgroup of D_n with index m is some $\langle r^m, r^i s\rangle$ where $0 \leq i \leq m-1$. Since $r^i s$ is conjugate to s or rs (depending on the parity of i), and the only conjugates of r^m are $r^{\pm m}$, $\langle r^m, r^i s\rangle$ is conjugate to $\langle r^m, s\rangle$ or $\langle r^m, rs\rangle$. Note $\langle r^m, s\rangle = \langle r^m, r^m s\rangle$ and $r^m s$ is conjugate to rs (because m is odd), Every conjugation sending $r^m s$ to rs turns $\langle r^m, s\rangle$ into $\langle r^m, rs\rangle$.

When m is an even divisor of $2n$, so $(m/2) \mid n$, Theorem 3.1 tells us $\langle r^{m/2}\rangle$ has index m. Every other subgroup of index m is $\langle r^m, r^i s\rangle$ for some i, and this occurs only when $m \mid n$, in which case $\langle r^m, r^i s\rangle$ is conjugate to one of $\langle r^m, s\rangle$ and $\langle r^m, rs\rangle$. It remains to show $\langle r^m, s\rangle$ and $\langle r^m, rs\rangle$ are nonconjugate subgroups of D_n. Since m is even, the reflections in $\langle r^m, s\rangle$ are of the form $r^i s$ with even i and the reflections in $\langle r^m, rs\rangle$ are of the form $r^i s$ with odd i. Therefore no reflection in one of these subgroups has a conjugate in the other subgroup, so the two subgroups are not conjugate. $\square$

Example 3.4. For odd prime p, the only subgroup of D_p with index 2 is $\langle r\rangle$ and all p subgroups with index p (hence order 2) are conjugate to $\langle r^p, s\rangle = \langle s\rangle$.

Example 3.5. In D_6, the subgroups of index 2 are $\langle r\rangle$, $\langle r^2, s\rangle$, and $\langle r^2, rs\rangle$, which are nonconjugate to each other. All 3 subgroups of index 3 are conjugate to $\langle r^3, s\rangle$. The only subgroup of index 4 is $\langle r^2\rangle$. A subgroup of index 6 is $\langle r^3\rangle$ or is conjugate to $\langle s\rangle$ or $\langle rs\rangle$.

Example 3.6. In D_{10} the subgroups of index 2 are $\langle r\rangle$, $\langle r^2, s\rangle$, and $\langle r^2, rs\rangle$, which are nonconjugate. The only subgroup of index 4 is $\langle r^2\rangle$, all 5 subgroups with index 5 are conjugate to $\langle r^5, s\rangle$, and a subgroup with index 10 is $\langle r^5\rangle$ or is conjugate to $\langle r^{10}, s\rangle$ or $\langle r^{10}, rs\rangle$.

Example 3.7. When $k \geq 3$, the dihedral group D_{2^k} has three conjugacy classes of subgroups with each index $2, 4, \ldots, 2^{k-1}$.

We now classify the normal subgroups of D_n, using a method that does not rely on our listing of all subgroups or all conjugacy classes of subgroups.

Theorem 3.8. *In D_n, every subgroup of $\langle r\rangle$ is a normal subgroup of D_n; these are the subgroups $\langle r^d\rangle$ for $d \mid n$ and have index $2d$. This describes all proper normal subgroups of D_n when n is odd, and the only additional proper normal subgroups when n is even are $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$ with index 2.*

In particular, there is at most one normal subgroup per index in D_n except for three normal subgroups $\langle r\rangle$, $\langle r^2, s\rangle$, and $\langle r^2, rs\rangle$ of index 2 when n is even.

Proof. We leave the cases $n = 1$ and $n = 2$ to the reader, and take $n \geq 3$.

Since $\langle r\rangle$ is a *cyclic* normal subgroup of D_n all of its subgroups are normal in D_n, and by the structure of subgroups of cyclic groups these have the form $\langle r^d\rangle$ where $d \mid n$.

It remains to find the proper normal subgroups of D_n that are not inside $\langle r\rangle$. Every subgroup of D_n not in $\langle r\rangle$ must contain a reflection.

First suppose n is odd. All the reflections in D_n are conjugate, so a normal subgroup containing one reflection must contain all n reflections, which is half of D_n. The subgroup also contains the identity, so its size is over half of the size of D_n, and thus the subgroup is D_n. So every proper normal subgroup of D_n is contained in $\langle r\rangle$.

Next suppose n is even. The reflections in D_n fall into two conjugacy classes of size $n/2$, represented by r and rs, so a proper normal subgroup N of D_n containing a reflection will contain half the reflections or all the reflections. A proper subgroup of D_n can't contain all the reflections, so N contains exactly $n/2$ reflections. Since N contains the identity, $|N| > n/2$, so $[D_n : N] < (2n)/(n/2) = 4$. A reflection in D_n lying outside of N has order 2 in D_n/N, so $[D_n : N]$ is even. Thus $[D_n : N] = 2$, and conversely every subgroup of index 2 is normal. Since D_n/N has order 2 we have $r^2 \in N$. The subgroup $\langle r^2\rangle$ in D_n is normal with index 4, so the subgroups of index 2 in D_n are obtained by taking the inverse image in D_n of subgroups of index 2 in $D_n/\langle r^2\rangle = \{\overline{1}, \overline{r}, \overline{s}, \overline{rs}\} \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$:

- the inverse image of $\{\overline{1}, \overline{r}\}$ is $\langle r\rangle$,
- the inverse image of $\{\overline{1}, \overline{s}\}$ is $\langle r^2, s\rangle$,
- the inverse image of $\{\overline{1}, \overline{rs}\}$ is $\langle r^2, rs\rangle$. □

Example 3.9. For an odd prime p, the only nontrivial proper normal subgroup of D_p is $\langle r\rangle$, with index 2.

Example 3.10. In D_6, the normal subgroups of index 2 are $\langle r\rangle$, $\langle r^2, s\rangle$, and $\langle r^2, rs\rangle$. The normal subgroup of index 4 is $\langle r^2\rangle$ and of index 6 is $\langle r^3\rangle$. There is no normal subgroup of index 3.

Example 3.11. The normal subgroups of D_{10} of index 2 are $\langle r\rangle$, $\langle r^2, s\rangle$, and $\langle r^2, rs\rangle$. The normal subgroup of index 4 is $\langle r^2\rangle$ and of index 10 is $\langle r^5\rangle$. There is no normal subgroup of index 5.

Example 3.12. When $k \geq 3$, the dihedral group D_{2^k} has one normal subgroup of each index except for three normal subgroups of index 2.

The "exceptional" normal subgroups $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$ in D_n for even $n \geq 4$ can be realized as kernels of explicit homomorphisms $D_n \to \mathbf{Z}/(2)$. In $D_n/\langle r^2, s\rangle$ we have $r^2 = 1$ and $s = 1$, so $r^a s^b = r^a$ with a only mattering mod 2. In $D_n/\langle r^2, rs\rangle$ we have $r^2 = 1$ and $s = r^{-1} = r$, so $r^a s^b = r^{a+b}$, with the exponent only mattering mod 2. Therefore two homomorphisms $D_n \to \mathbf{Z}/(2)$ are $r^a s^b \mapsto a \bmod 2$ and $r^a s^b \mapsto a + b \bmod 2$. These functions are well-defined since n is even and their respective kernels are $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$.

We can also see that these functions are homomorphisms using the general multiplication rule in D_n:

$$r^a s^b \cdot r^c s^d = r^{a+(-1)^b c} s^{b+d}.$$

We have $a + (-1)^b c \equiv a + c \bmod 2$ and $a + (-1)^b c + b + d \equiv (a + b) + (c + d) \bmod 2$.

4. An infinite dihedral-like group

In Theorem 2.1, the group is assumed to be finite. This finiteness is used in the proof to be sure that xy has a finite order. It is reasonable to ask if the finiteness assumption can be removed: after all, could a nonabelian group generated by two elements of order 2 really be infinite? Yes! In this appendix we construct such a group and show that there is only one such group up to isomorphism.

Our group will be built out of the linear functions $f(x) = ax + b$ where $a = \pm 1$ and $b \in \mathbf{Z}$, with the group law being composition. For instance, the inverse of $-x$ is itself and the inverse of $x + 5$ is $x - 5$. This group is called the *affine group* over $\mathbf{Z}$ and is denoted $\mathrm{Aff}(\mathbf{Z})$. The label "affine" is just a fancy name for "linear function with a constant term." In linear algebra, the functions that are called linear all send 0 to 0, so $ax + b$ is not linear in that sense (unless $b = 0$). Calling a linear function "affine" avoids confusion with the more restricted linear algebra sense of the term "linear function."

Since polynomials $ax + b$ compose in the same way that the matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ multiply, we can consider such matrices, with $a = \pm 1$ and $b \in \mathbf{Z}$, as another model for the group $\mathrm{Aff}(\mathbf{Z})$. We will adopt this matrix model for the practical reason that it is simpler to write down products and powers with matrices rather than compositions with polynomials.

Theorem 4.1. *The group* $\mathrm{Aff}(\mathbf{Z})$ *is generated by* $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

In the polynomial model for $\mathrm{Aff}(\mathbf{Z})$, the generators in Theorem 4.1 are $-x$ and $x + 1$.

Proof. The elements of $\mathrm{Aff}(\mathbf{Z})$ have the form

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \tag{4.1}$$

or

$$\begin{pmatrix} -1 & \ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^\ell \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{4.2}$$

so all matrices in $\mathrm{Aff}(\mathbf{Z})$ are products of $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. $\square$

While $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order. The group $\mathrm{Aff}(\mathbf{Z})$ can be generated by two elements of order 2.

Corollary 4.2. *The group* $\mathrm{Aff}(\mathbf{Z})$ *is generated by* $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, *which each have order* 2.

Proof. Check $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$ has order 2. By Theorem 4.1, it now suffices to show $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ can be generated from $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$. It is their product, taken in the right order: $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. □

In the polynomial model for $\mathrm{Aff}(\mathbf{Z})$, the two generators of order 2 in Corollary 4.2 are $-x$ and $-x-1$. These are reflections across 0 and across $-1/2$ (solve $-x = x$ and $-x-1 = x$). In Figure 3, we color integers the same when they are paired together by the reflection.

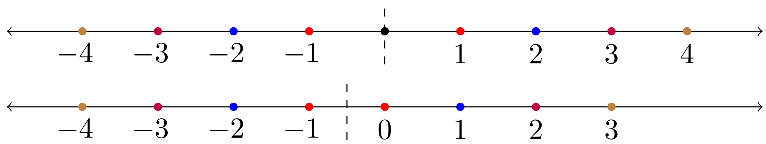

FIGURE 3. The reflections $-x$ and $-x-1$ on $\mathbf{Z}$.

Corollary 4.3. *The matrices* $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$ *are not conjugate in* $\mathrm{Aff}(\mathbf{Z})$ *and do not commute with a common element of order* 2 *in* $\mathrm{Aff}(\mathbf{Z})$.

Proof. Every conjugate of $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ in $\mathrm{Aff}(\mathbf{Z})$ has the form $\left(\begin{smallmatrix}-1 & 2b\\ 0 & 1\end{smallmatrix}\right)$ for $b \in \mathbf{Z}$, and $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$ does not have this form. Thus, the matrices are not conjugate. In $\mathrm{Aff}(\mathbf{Z})$, $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ commutes only with the identity and itself. □

Corollary 4.2 shows $\mathrm{Aff}(\mathbf{Z})$ is an example of an infinite group generated by two elements of order 2. Are there other such groups, not isomorphic to $\mathrm{Aff}(\mathbf{Z})$? No.

Theorem 4.4. *Every infinite group generated by two elements of order* 2 *is isomorphic to* $\mathrm{Aff}(\mathbf{Z})$.

Proof. Write such a group as G and its two generators of order 2 as x and y. Since G is infinite, x and y do not commute. (Otherwise $\langle x, y\rangle = \{1, x, y, xy\}$ has only 4 elements.) Since $x^{-1} = x$ and $y^{-1} = y$, we do not need to use exponents on x and y when writing products. The elements of G are strings of x's and y's, such as $xyyxxyxyxyxyxyxxy$. The relations $x^2 = 1$ and $y^2 = 1$ let us cancel all pairs of adjacent x's or y's, so $xyyxxyxyxyxyxyxxy$ can be simplified to

$$xyxyxyxyx = (xy)^4x.$$

Also, the inverse of such a string is again a string of x's and y's.

Every element of G can be written as a product of alternating x's and y's, so there are four kinds of elements, depending on the starting and ending letter: start with x and end with y, start with y and end with x, or start and end with the same letter. These four types of strings can be written as

$$(xy)^k, \quad (yx)^k, \quad (xy)^kx, \quad (yx)^ky, \tag{4.3}$$

where k is a non-negative integer.

Before we look more closely at these products, let's indicate how the correspondence between G and $\mathrm{Aff}(\mathbf{Z})$ is going to work out. We want to think of x as $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and y as $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$. Therefore the product xy should correspond to $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, and in particular have infinite order. Does xy really have infinite order? Yes, because if xy has finite order, the proof of Theorem 2.1 shows $G = \langle x, y\rangle$ is a finite group. (The finiteness hypothesis on the group in the statement of Theorem 2.1 was only used in its proof to show

xy has finite order; granting that xy has finite order, the rest of the proof of Theorem 2.1 shows $\langle x, y\rangle$ has to be a finite group.)

The proof of Theorem 4.1 shows each element of $\mathrm{Aff}(\mathbf{Z})$ is $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)^k$ or $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)^k\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$ for some $k \in \mathbf{Z}$. This suggests we should show each element of G has the form $(xy)^k$ or $(xy)^k x$.

Let $z = xy$, so $z^{-1} = y^{-1}x^{-1} = yx$. Also $xzx^{-1} = yx$, so

$$xzx^{-1} = z^{-1}. \tag{4.4}$$

The elements in (4.3) have the form $z^k, z^{-k}, z^k x$, and $z^{-k}y$, where $k \geq 0$. Therefore elements of the first and second type are just integral powers of z. Since $z^{-k}y = z^{-k}yxx = z^{-k-1}x$, elements of the third and fourth type are just integral powers of z multiplied on the right by x.

Now we make a correspondence between $\mathrm{Aff}(\mathbf{Z})$ and $G = \langle x, y\rangle$, based on the formulas in (4.1) and (4.2). Let $f \colon \mathrm{Aff}(\mathbf{Z}) \to G$ by

$$f\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix} = z^k, \quad f\begin{pmatrix}-1 & \ell\\ 0 & 1\end{pmatrix} = z^\ell x.$$

This function is onto, since we showed each element of G is a power of z or a power of z multiplied on the right by x. The function f is one-to-one, since z has infinite order (and, in particular, no power of z is equal to x, which has order 2). By taking cases, the reader can check $f(AB) = f(A)f(B)$ for all A and B in $\mathrm{Aff}(\mathbf{Z})$. Some cases will need the relation $xz^n = z^{-n}x$, which follows from raising both sides of (4.4) to the n-th power. $\square$

Remark 4.5. The abstract group $\langle x, y\rangle$ from this proof is the set of all words in x and y (like $xyxyx$) subject only to the relation that all pairs of adjacent x's or adjacent y's can be cancelled (*e.g.*, $xyxxxy = xyxy$). Because the only relation imposed (beyond the group axioms) is that xx and yy are the identity, this group is called a *free group* on two elements of order 2.

Corollary 4.6. *Every nontrivial quotient group of* $\mathrm{Aff}(\mathbf{Z})$ *is isomorphic to* $\mathrm{Aff}(\mathbf{Z})$ *or to* D_n *for some* $n \geq 1$*.*

Proof. Since $\mathrm{Aff}(\mathbf{Z})$ is generated by two elements of order 2, each nontrivial quotient group of $\mathrm{Aff}(\mathbf{Z})$ is generated by two elements that have order 1 or 2, and not both have order 1. If one of the generators has order 1 then the quotient group is isomorphic to $\mathbf{Z}/(2) = D_1$. If both generators have order 2 then the quotient group is isomorphic to $\mathrm{Aff}(\mathbf{Z})$ if it is infinite, by Theorem 4.4, and it is isomorphic to some D_n if it is finite since the finite groups generated by two elements of order 2 are the dihedral groups. $\square$

Every dihedral group arises as a quotient of $\mathrm{Aff}(\mathbf{Z})$. For $n \geq 3$, reducing matrix entries modulo n gives a homomorphism $\mathrm{Aff}(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/(n))$ whose image is the matrix group $\widetilde{D}_n$ from (1.3), which is isomorphic to D_n. The map $\left(\begin{smallmatrix}a&b\\0&1\end{smallmatrix}\right) \mapsto (a, b \bmod 2)$ is a homomorphism from $\mathrm{Aff}(\mathbf{Z})$ onto $\{\pm 1\} \times \mathbf{Z}/(2) \cong D_2$ and the map $\left(\begin{smallmatrix}a&b\\0&1\end{smallmatrix}\right) \mapsto a$ is a homomorphism from $\mathrm{Aff}(\mathbf{Z})$ onto $\{\pm 1\} \cong D_1$. Considering the kernels of these homomorphisms for $n \geq 3$, $n = 2$, and $n = 1$ reveals that we can describe all of these maps onto dihedral groups in a uniform way: for all $n \geq 1$, $\langle\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)\rangle \lhd \mathrm{Aff}(\mathbf{Z})$ and $\mathrm{Aff}(\mathbf{Z})/\langle\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)\rangle \cong D_n$. This common pattern is another justification for our definition of the dihedral groups D_1 and D_2.