# 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 $s r s^{-1}=r^{-1}$. 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 $G$ be generated by elements $x$ and $y$ where $x^{n}=1$ for some $n \geq 3$, $y^{2}=1$, and $y x y^{-1}=x^{-1}$. There is a surjective homomorphism $D_{n} \rightarrow G$, and if $G$ has order $2 n$ 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 $y x y^{-1}=x^{-1}$ (take $x$ and $y$ to be the identity).
Proof. The equation $y x y^{-1}=x^{-1}$ implies $y x^{j} y^{-1}=x^{-j}$ for all $j \in \mathbf{Z}$ (raise both sides to the $j$ th 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 $j, k \in \mathbf{Z}$,

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

This shows each product of $x$ 's and $y$ 's (like $y^{5} x^{-7} y^{3} x^{2} y^{-4} x^{21}$ ) 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 $x^{a} y^{b}$. Taking into account that $x^{n}=1$ and $y^{2}=1$, we can say

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

Thus $G$ is a finite group with $|G| \leq 2 n$.
To write down an explicit homomorphism from $D_{n}$ onto $G$, the equations $x^{n}=1, y^{2}=1$, and $y x y^{-1}=x^{-1}$ suggest we should be able send $r$ to $x$ and $s$ to $y$ by a homomorphism. This suggests the function $f: D_{n} \rightarrow G$ defined by

$$
f\left(r^{j} s^{k}\right)=x^{j} y^{k} .
$$

This equation defines $f$ on all of $D_{n}$ since all elements of $D_{n}$ have the form $r^{j} s^{k}$ for some $j$ and $k .{ }^{1}$ To see $f$ is well-defined, the only ambiguity in writing an element of $D_{n}$ as $r^{j} s^{k}$ is

[^0]that $j$ changes mod $n$ and $k$ changes mod 2: $r^{j} s^{k}=r^{j^{\prime}} s^{k^{\prime}} \Rightarrow r^{j-j^{\prime}}=s^{k^{\prime}-k} \in\langle r\rangle \cap\langle s\rangle=\{1\}$, so $j^{\prime} \equiv j \bmod n$ and $k^{\prime} \equiv k \bmod 2$. Such changes to $j$ and $k$ have no effect on $x^{j} y^{k}$ since $x^{n}=1$ and $y^{2}=1$.

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

$$
\begin{aligned}
f\left(r^{j} s^{k}\right) f\left(r^{j^{\prime}} s^{k^{\prime}}\right) & =x^{j} y^{k} x^{j^{\prime}} y^{k^{\prime}} \\
& =x^{j} x^{(-1)^{k} j^{\prime}} y^{k} y^{k^{\prime}} \\
& =x^{j+(-1)^{k} j^{\prime}} y^{k+k^{\prime}}
\end{aligned}
$$

and

$$
\begin{aligned}
f\left(\left(r^{j} s^{k}\right)\left(r^{j^{\prime}} s^{k^{\prime}}\right)\right) & =f\left(r^{j} r^{(-1)^{k} j^{\prime}} s^{k} s^{k^{\prime}}\right) \\
& =f\left(r^{j+(-1)^{k} j^{\prime}} s^{k+k^{\prime}}\right) \\
& =x^{j+(-1)^{k} j^{\prime}} y^{k+k^{\prime}} .
\end{aligned}
$$

The results agree, so $f$ is a homomorphism from $D_{n}$ to $G$. It is onto since every element of $G$ has the form $x^{j} y^{k}$ and these are all values of $f$ by the definition of $f$.

If $|G|=2 n$ then surjectivity of $f$ implies injectivity, so $f$ is an isomorphism.
Remark 1.2. The homomorphism $f: D_{n} \rightarrow G$ constructed in the proof is the only one where $f(r)=x$ and $f(s)=y$ : if there is such a homomorphism then $f\left(r^{j} s^{k}\right)=f(r)^{j} f(s)^{k}=$ $x^{j} y^{k}$. 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 $y x y^{-1}=x^{-1}$, there is a unique homomorphism $D_{n} \rightarrow G$ 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

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

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

$$
\begin{aligned}
\left(\begin{array}{cc} 
\pm 1 & c \\
0 & 1
\end{array}\right) & =\left(\begin{array}{ll}
1 & c \\
0 & 1
\end{array}\right)\left(\begin{array}{cc} 
\pm 1 & 0 \\
0 & 1
\end{array}\right) \\
& =\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)^{c}\left(\begin{array}{cc} 
\pm 1 & 0 \\
0 & 1
\end{array}\right),
\end{aligned}
$$

so $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ and $\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)$ generate $\widetilde{D}_{n}$. Moreover, $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ and $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)^{-1}$ are conjugate by $\left(\begin{array}{cc}-1 & 1 \\ 0 & 1\end{array}\right)$ :

$$
\begin{aligned}
\left(\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array}\right)\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array}\right)^{-1} & =\left(\begin{array}{cc}
1 & -1 \\
0 & 1
\end{array}\right) \\
& =\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)^{-1} .
\end{aligned}
$$

Thus, by Theorem 1.1, $\widetilde{D}_{n}$ is isomorphic to $D_{n}$, using $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ in the role of $r$ and $\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)$ 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: $r=\left(\begin{array}{c}\cos (2 \pi / n) \\ \sin (2 \pi / n)\end{array} \sin (2 \pi / n)\right.$ cos $(2 \pi / n)$ and $s=\left(\begin{array}{cc}1 & 0 \\ 0 & -1\end{array}\right)$.

For even $n, D_{n}$ has a nontrivial center $\left\{1, r^{n / 2}\right\}$, 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 $H=\left\langle r^{2}, s\right\rangle$, where $r$ and $s$ are taken from $D_{n}$. Then $\left(r^{2}\right)^{n / 2}=1, s^{2}=1$, and $s r^{2} s^{-1}=r^{-2}$, so Theorem 1.1 tells us there is a surjective homomorphism $D_{n / 2} \rightarrow H$. Since $r^{2}$ has order $n / 2,|H|=2(n / 2)=n=\left|D_{n / 2}\right|$, so $D_{n / 2} \cong H$.

Set $Z=\left\{1, r^{n / 2}\right\}$, the center of $D_{n}$. The elements of $H$ commute with the elements of $Z$, so the function $f: H \times Z \rightarrow D_{n}$ by $f(h, z)=h z$ is a homomorphism. Writing $n=2 k$ where $k=2 \ell+1$ is odd, we get $f\left(\left(r^{2}\right)^{-\ell}, r^{n / 2}\right)=r^{-2 \ell+k}=r$ 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: $D_{n} \neq D_{n / 2} \times \mathbf{Z} /(2)$. 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 $n \geq 3$,

$$
\operatorname{Aut}\left(D_{n}\right) \cong\left\{\left(\begin{array}{ll}
a & b \\
0 & 1
\end{array}\right): a \in(\mathbf{Z} /(n))^{\times}, b \in \mathbf{Z} /(n)\right\} .
$$

In particular, the order of $\operatorname{Aut}\left(D_{n}\right)$ 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

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

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

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

We have shown $\operatorname{Aut}\left(D_{n}\right)$ is parametrized by pairs $(a, b)$ in $(\mathbf{Z} /(n))^{\times} \times \mathbf{Z} /(n)$ : for each $(a, b)$, there is a unique $f_{a, b} \in \operatorname{Aut}\left(D_{n}\right)$ 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 $D_{n}$,

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

and

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

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

$$
\operatorname{Aut}\left(D_{n}\right) \rightarrow\left\{\left(\begin{array}{ll}
a & b \\
0 & 1
\end{array}\right): a \in(\mathbf{Z} /(n))^{\times}, b \in \mathbf{Z} /(n)\right\}
$$

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 $f \in \operatorname{Aut}\left(D_{n}\right)$ 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 $D_{n}$.

## 2. Dihedral groups and generating elements of order 2

Since $D_{n}=\langle r, s\rangle=\langle r s, s\rangle, D_{n}$ is generated by the two reflections $s$ and rs. The reflections $s$ and $r s$ fix lines separated by an angle $2 \pi /(2 n)$, as illustrated in Figure 2 for $3 \leq n \leq 6$. A nice visual demonstration that $s$ and $r s$ 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 $G=\{1, x, y, x y\}$. This has size 4 provided $x \neq y$. Then we see $G$ behaves just like the group $\mathbf{Z} /(2) \times \mathbf{Z} /(2)$,

[^1]

Figure 2. The reflections $s$ and $r s$ 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: $x y \neq y x$.

The product $x y$ has some finite order, since we are told that $G$ is a finite group. Let the order of $x y$ be denoted $n$. Set $a=x y$ and $b=y$. (If we secretly expect $x$ is like $r s$ 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 $G=\langle x, y\rangle=\langle x y, y\rangle$ is generated by $a$ and $b$, where $a^{n}=1$ and $b^{2}=1$. Since $a$ has order $n, n| | G \mid$. Since $b \notin\langle a\rangle,|G|>n$, so $|G| \geq 2 n$.

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

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

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

$$
\begin{equation*}
b a b^{-1}=y x y y=y x, \quad a^{-1}=y^{-1} x^{-1}=y x \tag{2.1}
\end{equation*}
$$

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

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,

- $\left|D_{n}\right|=2 n$ 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 $Z\left(D_{n}\right)=D_{n}$ 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 $\operatorname{Aut}\left(D_{n}\right)$ over $\mathbf{Z} /(n)$ in Theorem 1.4 doesn't work when $n=2$ : $\operatorname{Aut}\left(D_{2}\right)=\mathrm{GL}_{2}(\mathbf{Z} /(2))$ 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 $N \triangleleft D_{n}$ 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 $\overline{r s}$ and $\bar{s}$, 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 $\left|D_{n} / N\right|$ is even, so $m$ is even. If $\overline{r s}$ and $\bar{s}$ 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 $\overline{r s}$ or $\bar{s}$ have order 1 then only one of them has order 1 , which makes $D_{n} / N \cong \mathbf{Z} /(2)=D_{1}$.

Example 2.4. For even $n \geq 3, Z\left(D_{n}\right)=\left\{1, r^{n / 2}\right\}$, so $D_{n} / Z\left(D_{n}\right)$ has order $(2 n) / 2=n=$ $2(n / 2)$ and is generated by the images $\bar{r}$ (with order $n / 2$ in $D_{n} / Z\left(D_{n}\right)$ ) and $\bar{s}$ (with order 2), subject to the relation $\bar{s} \bar{r} \bar{s}^{-1}=\bar{r}^{-1}$. Therefore $D_{n} / Z\left(D_{n}\right) \cong D_{n / 2}$. Note for $n=4$ that we are using the definition $D_{2}:=\mathbf{Z} /(2) \times \mathbf{Z} /(2)$. (For odd $n \geq 3, Z\left(D_{n}\right)=\{1\}$ so $D_{n} / Z\left(D_{n}\right)=D_{n}$, which is boring.)
Example 2.5. For $n \geq 3$, the commutator subgroup $\left[D_{n}, D_{n}\right]$ is $\left\langle r^{2}\right\rangle$, which is $\langle r\rangle$ for odd $n$, so $D_{n} /\left[D_{n}, D_{n}\right]$ has order $(2 n) / 2 n=2$ for odd $n$ and order $2 n /(n / 2)=4$ for even $n$. The group $D_{n} /\left[D_{n}, D_{n}\right]$ is abelian and is generated by the images $\bar{r}$ and $\bar{s}$. where $\bar{s}$ has order 2 . For odd $n, \bar{r}$ is trivial so $D_{n} /\left[D_{n}, D_{n}\right]=\langle\bar{s}\rangle \cong \mathbf{Z} /(2)$. For even $n, \bar{r}$ has order 2 and doesn't equal $\bar{s}$, so $D_{n} /\left[D_{n}, D_{n}\right] \cong \mathbf{Z} /(2) \times \mathbf{Z} /(2)$. These formulas for $\left.\left.D_{n} /\right] D_{n}, D_{n}\right]$ 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) $\left\langle r^{d}\right\rangle$, where $d \mid n$, with index $2 d$,
(2) $\left\langle r^{d}, r^{i} s\right\rangle$, where $d \mid n$ and $0 \leq i \leq d-1$, 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: $\left\langle r^{d}\right\rangle \cong \mathbf{Z} /(n / d)$ and $\left\langle r^{d}, r^{i} s\right\rangle \cong D_{n / d}$.
Proof. It is left to the reader to check $n=1$ and $n=2$ separately. We now assume $n \geq 3$.
Let $H$ be a subgroup of $D_{n}$. Since $\langle r\rangle$ is cyclic of order $n$, if $H \subset\langle r\rangle$ then $H=\left\langle r^{d}\right\rangle$ where $d \mid n$ (and $d>0$ ). The order of $\left\langle r^{d}\right\rangle$ is $n / d$, so its index in $D_{n}$ is $2 n /(n / d)=2 d$.

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

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 $f\left(r^{i} s\right)=s$. Then $f(H)$ is a subgroup of $D_{n}$ containing $s$, so by the previous paragraph $f(H)=\left\langle r^{d}, s\right\rangle$ where $d \mid n$ (and $d>0$ ). Then $H=f^{-1}\left(\left\langle r^{d}, s\right\rangle\right)=$ $\left\langle f^{-1}(r)^{d}, f^{-1}(s)\right\rangle=\left\langle r^{d}, r^{i} s\right\rangle$. Since $\left\langle r^{d}, r^{i} s\right\rangle=\left\langle r^{d}, r^{j} s\right\rangle$ when $j \equiv i \bmod d$, we can adjust $i \bmod d$ without affecting $\left\langle r^{d}, r^{i} s\right\rangle$ and thus write $H=\left\langle r^{d}, r^{i} s\right\rangle$ where $0 \leq i \leq d-1$.

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

It remains to show the subgroups in the theorem have no duplications. First let's show the two lists are disjoint. Everything in $\left\langle r^{d}\right\rangle$ commutes with $r$ while $\left\langle r^{d}, r^{i} s\right\rangle$ 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 $\left\langle r^{d}\right\rangle$ determines $d$ when $d$ is a positive divisor of $n$ : it has index $2 d$. If two subgroups of the second type are equal, then they have equal index in $D_{n}$, say $d$, so they must be $\left\langle r^{d}, r^{i} s\right\rangle$ and $\left\langle r^{d}, r^{j} s\right\rangle$ where $i$ and $j$ are in $\{0, \ldots, d-1\}$. Then $r^{j} s \in\left\langle r^{d}, r^{i} s\right\rangle=\left\langle r^{d}\right\rangle \cup\left\langle r^{d}\right\rangle r^{i} s$, so $r^{j} s=r^{d k+i} s$ for some $k \in \mathbf{Z}$. Therefore $j \equiv d k+i \bmod n$. We can reduce both sides $\bmod d$, since $d \mid n$, to get $j \equiv i \bmod d$. That forces $j=i$ since $0 \leq i, j \leq d-1$.
Corollary 3.2. Let $n$ be odd and $m \mid 2 n$. 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 $m \mid 2 n$.

- 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 $n \geq 3$.
If $n$ is odd then the odd divisors of $2 n$ are the divisors of $n$ and the even divisors of $2 n$ are of the form $2 d$, 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 $\left\langle r^{m}, r^{i} s\right\rangle$ for a unique $i$ from 0 to $m-1$, so there are $m$ such subgroups. A subgroup with even index $m$ must be $\left\langle r^{m / 2}\right\rangle$ by Theorem 3.1.

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

From knowledge of all subgroups of $D_{n}$ we can count conjugacy classes of subgroups.
Theorem 3.3. Let $n$ be odd and $m \mid 2 n$. If $m$ is odd then all $m$ subgroups of $D_{n}$ with index $m$ are conjugate to $\left\langle r^{m}, s\right\rangle$. If $m$ is even then the only subgroup of $D_{n}$ with index $m$ is $\left\langle r^{m / 2}\right\rangle$. In particular, all subgroups of $D_{n}$ with the same index are conjugate to each other.

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

- If $m$ is odd then all $m$ subgroups of $D_{n}$ with index $m$ are conjugate to $\left\langle r^{m}, s\right\rangle$.
- If $m$ is even and $m$ doesn't divide $n$ then the only subgroup of $D_{n}$ with index $m$ is $\left\langle r^{m / 2}\right\rangle$.
- If $m$ is even and $m \mid n$ then every subgroup of $D_{n}$ with index $m$ is $\left\langle r^{m / 2}\right\rangle$ or is conjugate to exactly one of $\left\langle r^{m}, s\right\rangle$ or $\left\langle r^{m}, r s\right\rangle$.
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 $\left\langle r^{m}, r^{i} s\right\rangle$. 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 $\left\langle r^{m}, s\right\rangle$ into $\left\langle r^{ \pm m}, r^{i} s\right\rangle=\left\langle r^{m}, r^{i} s\right\rangle$. When $n$ is odd and $m$ is even, the only subgroup of $D_{n}$ with even index $m$ is $\left\langle r^{m / 2}\right\rangle$ by Theorem 3.1.

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

When $m$ is an even divisor of $2 n$, so $(m / 2) \mid n$, Theorem 3.1 tells us $\left\langle r^{m / 2}\right\rangle$ has index $m$. Every other subgroup of index $m$ is $\left\langle r^{m}, r^{i} s\right\rangle$ for some $i$, and this occurs only when $m \mid n$, in which case $\left\langle r^{m}, r^{i} s\right\rangle$ is conjugate to one of $\left\langle r^{m}, s\right\rangle$ and $\left\langle r^{m}, r s\right\rangle$. It remains to show $\left\langle r^{m}, s\right\rangle$ and $\left\langle r^{m}, r s\right\rangle$ are nonconjugate subgroups of $D_{n}$. Since $m$ is even, the reflections in $\left\langle r^{m}, s\right\rangle$ are of the form $r^{i} s$ with even $i$ and the reflections in $\left\langle r^{m}, r s\right\rangle$ 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.
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 $\left\langle r^{p}, s\right\rangle=\langle s\rangle$.
Example 3.5. In $D_{6}$, the subgroups of index 2 are $\langle r\rangle,\left\langle r^{2}, s\right\rangle$, and $\left\langle r^{2}, r s\right\rangle$, which are nonconjugate to each other. All 3 subgroups of index 3 are conjugate to $\left\langle r^{3}, s\right\rangle$. The only subgroup of index 4 is $\left\langle r^{2}\right\rangle$. A subgroup of index 6 is $\left\langle r^{3}\right\rangle$ or is conjugate to $\langle s\rangle$ or $\langle r s\rangle$.
Example 3.6. In $D_{10}$ the subgroups of index 2 are $\langle r\rangle,\left\langle r^{2}, s\right\rangle$, and $\left\langle r^{2}, r s\right\rangle$, which are nonconjugate. The only subgroup of index 4 is $\left\langle r^{2}\right\rangle$, all 5 subgroups with index 5 are
conjugate to $\left\langle r^{5}, s\right\rangle$, and a subgroup with index 10 is $\left\langle r^{5}\right\rangle$ or is conjugate to $\left\langle r^{10}, s\right\rangle$ or $\left\langle r^{10}, r s\right\rangle$.
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 $\left\langle r^{d}\right\rangle$ for $d \mid n$ and have index $2 d$. 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 $\left\langle r^{2}, s\right\rangle$ and $\left\langle r^{2}, r s\right\rangle$ with index 2.

In particular, there is at most one normal subgroup per index in $D_{n}$ except for three normal subgroups $\langle r\rangle,\left\langle r^{2}, s\right\rangle$, and $\left\langle r^{2}, r s\right\rangle$ 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 $\left\langle r^{d}\right\rangle$ 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 $r s$, 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 $\left[D_{n}: N\right]<(2 n) /(n / 2)=4$. A reflection in $D_{n}$ lying outside of $N$ has order 2 in $D_{n} / N$, so $\left[D_{n}: N\right]$ is even. Thus $\left[D_{n}: N\right]=2$, and conversely every subgroup of index 2 is normal. Since $D_{n} / N$ has order 2 we have $r^{2} \in N$. The subgroup $\left\langle r^{2}\right\rangle$ 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 $D_{n} /\left\langle r^{2}\right\rangle=\{\overline{1}, \bar{r}, \bar{s}, \overline{r s}\} \cong \mathbf{Z} /(2) \times \mathbf{Z} /(2)$ :

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

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 $\langle r\rangle,\left\langle r^{2}, s\right\rangle$, and $\left\langle r^{2}, r s\right\rangle$. The normal subgroup of index 4 is $\left\langle r^{2}\right\rangle$ and of index 6 is $\left\langle r^{3}\right\rangle$. There is no normal subgroup of index 3.

Example 3.11. The normal subgroups of $D_{10}$ of index 2 are $\langle r\rangle,\left\langle r^{2}, s\right\rangle$, and $\left\langle r^{2}, r s\right\rangle$. The normal subgroup of index 4 is $\left\langle r^{2}\right\rangle$ and of index 10 is $\left\langle r^{5}\right\rangle$. 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 $\left\langle r^{2}, s\right\rangle$ and $\left\langle r^{2}, r s\right\rangle$ in $D_{n}$ for even $n \geq 4$ can be realized as kernels of explicit homomorphisms $D_{n} \rightarrow \mathbf{Z} /(2)$. In $D_{n} /\left\langle r^{2}, s\right\rangle$ we have $r^{2}=1$ and $s=1$, so $r^{a} s^{b}=r^{a}$ with $a$ only mattering $\bmod 2$. In $D_{n} /\left\langle r^{2}, r s\right\rangle$ 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 $D_{n} \rightarrow \mathbf{Z} /(2)$ 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 $\left\langle r^{2}, s\right\rangle$ and $\left\langle r^{2}, r s\right\rangle$.

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 $x y$ 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 $f(x)=a x+b$ 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 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 $a x+b$ 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 $a x+b$ compose in the same way that the matrices $\left(\begin{array}{ll}a & b \\ 0 & 1\end{array}\right)$ multiply, we can consider such matrices, with $a= \pm 1$ and $b \in \mathbf{Z}$, as another model for the group $\operatorname{Aff}(\mathbf{Z})$. 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 $\operatorname{Aff}(\mathbf{Z})$ is generated by $\left(\begin{array}{rl}-1 & 0 \\ 0 & 1\end{array}\right)$ and $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$.
In the polynomial model for $\operatorname{Aff}(\mathbf{Z})$, the two generators in Theorem 4.1 are the functions $-x$ and $x+1$.

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

$$
\left(\begin{array}{cc}
1 & k  \tag{4.1}\\
0 & 1
\end{array}\right)=\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)^{k}
$$

or

$$
\left(\begin{array}{cc}
-1 & \ell \\
0 & 1
\end{array}\right)=\left(\begin{array}{ll}
1 & \ell \\
0 & 1
\end{array}\right)\left(\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array}\right)=\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)^{\ell}\left(\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array}\right)
$$

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

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

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

In the polynomial model for $\operatorname{Aff}(\mathbf{Z})$, 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 $\left(\begin{array}{rr}-1 & 0 \\ 0 & 1\end{array}\right)$ and $\left(\begin{array}{rr}-1 & -1 \\ 0 & 1\end{array}\right)$ are not conjugate in $\operatorname{Aff}(\mathbf{Z})$ and do not commute with a common element of order 2 in $\mathrm{Aff}(\mathbf{Z})$.
Proof. Every conjugate of $\left(\begin{array}{rr}-1 & 0 \\ 0 & 1\end{array}\right)$ in $\operatorname{Aff}(\mathbf{Z})$ has the form $\left(\begin{array}{cc}-1 & 2 b \\ 0 & 1\end{array}\right)$ for $b \in \mathbf{Z}$, and $\left(\begin{array}{cc}-1 & -1 \\ 0 & 1\end{array}\right)$ does not have this form. Thus, the matrices are not conjugate. In $\operatorname{Aff}(\mathbf{Z}),\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)$ commutes only with the identity and itself.

Corollary 4.2 shows $\operatorname{Aff}(\mathbf{Z})$ is an example of an infinite group generated by two elements of order 2. Are there other such groups, not isomorphic to $\operatorname{Aff}(\mathbf{Z})$ ? No.
Theorem 4.4. Every infinite group generated by two elements of order 2 is isomorphic to 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 $\langle x, y\rangle=\{1, x, y, x y\}$ 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 $x y y x x y x y x y x y x y x x y$ can be simplified to

$$
x y x y x y x y x=(x y)^{4} x .
$$

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

$$
\begin{equation*}
(x y)^{k}, \quad(y x)^{k}, \quad(x y)^{k} x, \quad(y x)^{k} y \tag{4.2}
\end{equation*}
$$

where $k$ is a non-negative integer.
Before we look more closely at these products, let's indicate how the correspondence between $G$ and $\operatorname{Aff}(\mathbf{Z})$ is going to work out. We want to think of $x$ as $\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)$ and $y$ as $\left(\begin{array}{cc}-1 & -1 \\ 0 & 1\end{array}\right)$. Therefore the product $x y$ should correspond to $\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)\left(\begin{array}{cc}-1 & -1 \\ 0 & 1\end{array}\right)=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$, and in particular have infinite order. Does $x y$ really have infinite order? Yes, because if $x y$ 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
$x y$ has finite order; granting that $x y$ 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 $\operatorname{Aff}(\mathbf{Z})$ is $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)^{k}$ or $\left(\begin{array}{cc}1 & 1 \\ 0 & 1\end{array}\right)^{k}\left(\begin{array}{cc}-1 & 0 \\ 0 & 1\end{array}\right)$ for some $k \in \mathbf{Z}$. This suggests we should show each element of $G$ has the form $(x y)^{k}$ or $(x y)^{k} x$.

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

$$
\begin{equation*}
x z x^{-1}=z^{-1} \tag{4.3}
\end{equation*}
$$

The elements in (4.2) 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 $z^{-k} y=z^{-k} y x x=z^{-k-1} x$, 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 $\operatorname{Aff}(\mathbf{Z})$ and $G=\langle x, y\rangle$, based on the formulas in (4.1) and (4). Let $f: \operatorname{Aff}(\mathbf{Z}) \rightarrow G$ by

$$
f\left(\begin{array}{cc}
1 & k \\
0 & 1
\end{array}\right)=z^{k}, \quad f\left(\begin{array}{cc}
-1 & \ell \\
0 & 1
\end{array}\right)=z^{\ell} x .
$$

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 $f(A B)=f(A) f(B)$ for all $A$ and $B$ in $\operatorname{Aff}(\mathbf{Z})$. Some cases will need the relation $x z^{n}=z^{-n} x$, which follows from raising both sides of (4.3) to the $n$-th power.

Remark 4.5. The abstract group $\langle x, y\rangle$ from this proof is the set of all words in $x$ and $y$ (like $x y x y x$ ) subject only to the relation that all pairs of adjacent $x$ 's or adjacent $y$ 's can be cancelled (e.g., $x y x x x y=x y x y$ ). Because the only relation imposed (beyond the group axioms) is that $x x$ and $y y$ are the identity, this group is called a free group on two elements of order 2 .
Corollary 4.6. Every nontrivial quotient group of $\operatorname{Aff}(\mathbf{Z})$ is isomorphic to $\operatorname{Aff}(\mathbf{Z})$ or to $D_{n}$ for some $n \geq 1$.
Proof. Since $\operatorname{Aff}(\mathbf{Z})$ is generated by two elements of order 2, each nontrivial quotient group of $\operatorname{Aff}(\mathbf{Z})$ 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 $\operatorname{Aff}(\mathbf{Z})$ 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.

Every dihedral group arises as a quotient of $\operatorname{Aff}(\mathbf{Z})$. For $n \geq 3$, reducing matrix entries modulo $n$ gives a homomorphism $\operatorname{Aff}(\mathbf{Z}) \rightarrow \mathrm{GL}_{2}(\mathbf{Z} /(n))$ whose image is the matrix group $\widetilde{D}_{n}$ from (1.3), which is isomorphic to $D_{n}$. The map $\left(\begin{array}{c}a \\ a \\ 0\end{array} 1\right) \mapsto(a, b \bmod 2)$ is a homomorphism from $\operatorname{Aff}(\mathbf{Z})$ onto $\{ \pm 1\} \times \mathbf{Z} /(2) \cong D_{2}$ and the map $\left(\begin{array}{cc}a & b \\ 0 & 1\end{array}\right) \mapsto a$ is a homomorphism from $\operatorname{Aff}(\mathbf{Z})$ 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 $n \geq 1,\left\langle\left(\begin{array}{cc}1 & n \\ 0 & 1\end{array}\right)\right\rangle \triangleleft \operatorname{Aff}(\mathbf{Z})$ and $\operatorname{Aff}(\mathbf{Z}) /\left\langle\left(\begin{array}{ll}1 & n \\ 0 & 1\end{array}\right)\right\rangle \cong D_{n}$. This common pattern is another justification for our definition of the dihedral groups $D_{1}$ and $D_{2}$.


[^0]:    ${ }^{1}$ See Theorem 2.5 in https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf.

[^1]:    ${ }^{2}$ We have not yet defined $D_{n}$ for $n=2: \quad D_{2}$ is $\mathbf{Z} /(2) \times \mathbf{Z} /(2)$. This will be explained after Theorem 2.1.

