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 \( G \) 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 \( j \in \mathbb{Z} \) (raise both sides to
the \( j \)th power). Since \( y^2 = 1 \), we have for all \( k \in \mathbb{Z} \)
\[
y^k x^j y^{-k} = x^{(-1)^k j}
\]
by considering even and odd \( k \) separately. Thus for all \( j,k \in \mathbb{Z} \),
\[
y^k x^j y^{-k} = x^{(-1)^k j} y^k.
\]
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
\[
G = \langle x,y \rangle
\]
\[
= \{ x^j, x^j y : j \in \mathbb{Z} \}
\]
\[
= \{ 1, x, x^2, \ldots, x^{n-1}, y, xy, x^2 y, \ldots, x^{n-1} y \}.
\]
Thus \( G \) is a finite group 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 \( f : D_n \to G \) defined by
\[
f(r^j s^k) = x^j y^k.
\]
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 \( k \). 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](https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf).
that \( j \) changes mod \( n \) and \( k \) changes mod 2: \( r^j s^k = r^{j'} s^{k'} \Rightarrow r^{j-j'} = s^{k-k} \in \langle r \rangle \cap \langle s \rangle = \{1\} \), so \( j' \equiv j \pmod{n} \) and \( k' \equiv k \pmod{2} \). 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):

\[
f(r^j s^k) f(r^{j'} s^{k'}) = x^j y^k x^{j'} y^{k'}
= x^j x^{(-1)^k j'} y^k y^{k'}
= x^{j+(-1)^k j'} y^{k+k'}
\]

and

\[
f((r^j s^k)(r^{j'} s^{k'})) = f(r^{j+(-1)^k j'} s^{k+k'})
= f(r^j s^k) f(r^{j'} s^{k'})
= x^{j+(-1)^k j'} y^{k+k'}
\]

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 \( |G| = 2n \) then surjectivity of \( f \) implies injectivity, so \( f \) is an isomorphism. \( \square \)

**Remark 1.2.** The homomorphism \( f : D_n \to G \) constructed in the proof is the only one where \( f(r) = x \) and \( f(s) = y \): if there is such a homomorphism then \( f(r^j s^k) = f(r)^j f(s)^k = x^j y^k \). 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 \( yxy^{-1} = x^{-1} \), 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 \( \mathbb{Z}/(n) \) that is isomorphic to \( D_n \) when \( n \geq 3 \). Set

\[(1.3) \quad \widetilde{D}_n = \left\{ \begin{pmatrix} \pm 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbb{Z}/(n) \right\} \]

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

\[
\begin{pmatrix} \pm 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}
= \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix},
\]

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

\[
\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}
= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}.
\]

Thus, by Theorem 1.1, \( \widetilde{D}_n \) is isomorphic to \( D_n \), using \( (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}) \) in the role of \( r \) and \( (\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}) \) in the role of \( s \).
This realization of $D_n$ inside $\text{GL}_2(\mathbb{Z}/(n))$ should not be confused with the geometric realization of $D_n$ in $\text{GL}_2(\mathbb{R})$ using real matrices: $r = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$ and $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

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 $D_n \cong D_{n/2} \times \mathbb{Z}/(2)$.

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

**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 $f: H \times Z \to D_n$ 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. \qed

Figure 1 is a geometric interpretation of the isomorphism $D_6 \cong D_3 \times \mathbb{Z}/(2)$. 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 $\mathbb{Z}/(2)$, 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.](image)

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: $D_n \not\cong D_{n/2} \times \mathbb{Z}/(2)$. That’s because $n$ and $n/2$ are even, so the center of $D_n$ has order 2 while the center of $D_{n/2} \times \mathbb{Z}/(2)$ has order $2 \cdot 2 = 4$. Since the groups $D_n$ and $D_{n/2} \times \mathbb{Z}/(2)$ 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 $n \geq 3$,

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

In particular, the order of $\text{Aut}(D_n)$ 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 $f(r) = ra$ with $(a, n) = 1$, so $f(\langle r \rangle) = \langle r \rangle$. Then $f(s) \notin \langle r \rangle$, so

$$f(r) = ra, \quad f(s) = rb$$

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

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

- $(ra)^n = 1$,
- $(rb)^2 = 1$,
- $(rb)(ra)(rb)^{-1} = r^{-a}$.

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

$$(rb)(ra)(rb)^{-1} = r^{bs}a^{-1}r^{-b} = r^{rb-a}sr^{-b} = r^{rb-a}r^{-b} = r^{-a}.$$  

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

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

and

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

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

$$\text{Aut}(D_n) \to \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (\mathbb{Z}/(n))^\times, b \in \mathbb{Z}/(n) \right\}. \quad \square$$

**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 $f \in \text{Aut}(D_n)$ is determined by $f(r) = ra$ and $f(s) = rb$ where $a \in (\mathbb{Z}/(n))^\times$ and $b \in \mathbb{Z}/(n)$. That $f$ fixes all of $\langle r \rangle$ means $a \equiv 1 \text{ mod } n$. How can we force $f(g) = h$?

Write $g = rs$ and $h = ri$ for some $i$ and $j$ (unique modulo $n$). Then $f(g) = f(r)f(s) = r^{i+bs} = r^{i+b}$, so the condition $f(g) = h$ says $r^{i+b}s = r^{j}s$, or equivalently $b \equiv j - i \text{ mod } n$. Therefore $f_{i,j-i}$ fixes $\langle r \rangle$, maps $g$ to $h$, and is the only such automorphism of $D_n$. \quad \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 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 $\mathbb{R}^2$ 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 $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$,\footnote{We have not yet defined $D_n$ for $n = 2$: $D_2$ is $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. This will be explained after Theorem 2.1.}
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

\[
(2.1) \quad bab^{-1} = yxyy = yx, \quad a^{-1} = y^{-1}x^{-1} = yx,
\]

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 \(\mathbb{Z}/(2) \times \mathbb{Z}/(2)\) or (in the degenerate case that the two generators are the same element) to \(\mathbb{Z}/(2)\). So we can define new dihedral groups of order 2 and 4:

\[
D_1 := \mathbb{Z}/(2), \quad D_2 := \mathbb{Z}/(2) \times \mathbb{Z}/(2).
\]

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 $\text{GL}_2(\mathbb{R})$ 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 $\mathbb{Z}/(n)$ in (1.3) is invalid when $n \leq 2$,
• the matrix model for $\text{Aut}(D_n)$ over $\mathbb{Z}/(n)$ in Theorem 1.4 doesn’t work when $n = 2$: $\text{Aut}(D_2) = \text{GL}_2(\mathbb{Z}/(2))$ 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 $\bar{r}s$ 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 $|D_n/N|$ is even, so $m$ is even. If $\bar{r}s$ 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 $\mathbb{Z}/(2)$ or $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ if $D_n/N$ is abelian, which are also dihedral groups by our convention on the meaning of $D_1$ and $D_2$. If $\bar{r}s$ or $\bar{s}$ have order 1 then only one of them has order 1, which makes $D_n/N \cong \mathbb{Z}/(2) = D_1$. \hfill $\Box$

Example 2.4. For even $n \geq 3$, $Z(D_n) = \{1, \tau^{n/2}\}$, so $D_n/Z(D_n)$ has order $(2n)/2 = n = 2(n/2)$ and is generated by the images $\bar{r}$ (with order $n/2$ in $D_n/Z(D_n)$) and $\bar{s}$ (with order 2), subject to the relation $\bar{r}\bar{s}\bar{s}^{-1} = \bar{r}^{-1}$. Therefore $D_n/Z(D_n) \cong D_{n/2}$. Note for $n = 4$ that we are using the definition $D_2 := \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. (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 $\langle \tau^2 \rangle$, 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 $\bar{r}$ and $\bar{s}$, where $\bar{s}$ has order 2. For odd $n$, $\bar{s}$ is trivial so $D_n/[D_n, D_n] = \langle \bar{s} \rangle \cong \mathbb{Z}/(2)$. For even $n$, $\bar{s}$ has order 2 and doesn’t equal $\bar{r}$, so $D_n/[D_n, D_n] \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. 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 $0 \leq i \leq d - 1$, with index $d$.

Every subgroup of $D_n$ occurs exactly once in this listing.

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 $H \subseteq \langle r \rangle$ 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 $H \not\subseteq \langle r \rangle$, 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 $h \not\in \langle r \rangle$ 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 $h = r^i s = r^{dk}s = (r^d)^ks \in \langle r^d, s \rangle$, so $H \subseteq \langle r^d, s \rangle$.

Consider now the case where $H \not\subseteq \langle r \rangle$ 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 $j \equiv i \mod d$, we can adjust $i \mod d$ without affecting $\langle r^d, r^i s \rangle$ and thus write $H = \langle r^d, r^i s \rangle$ where $0 \leq i \leq d - 1$.

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 $(r^i s)^r = r^{-k}(r^i s)$, all elements of $\langle r^d, r^i s \rangle$ that are not powers of $r$ have the form $(r^d)^k(r^i s) = r^d r^i s$. 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 $|H| = 2|\langle r^d \rangle| = 2n/(n/d)$, 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 $\{0, \ldots, d - 1\}$. Then $r^i s \in \langle r^d, r^i s \rangle = \langle r^d \rangle \cup \langle r^d \rangle r^i s$, so $r^i s = r^{dk+i}$ for some $k \in \mathbb{Z}$. Therefore $j \equiv dk + i \mod n$. We can reduce both sides mod $d$, since $d \mid n$, to get $j \equiv i \mod d$. That forces $j = i$ since $0 \leq i, j \leq d - 1$.

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 $n \geq 3$.

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 \( 0 \leq i \leq m-1 \).

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 \( \langle r^{m}, r^i s \rangle = \langle r^m, r^i s \rangle \). 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 \( \langle r^m, s \rangle = \langle r^m, r^i s \rangle \) 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.

**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 \( D_{2k} \) 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 \( D_n/\langle r^2 \rangle = \{1, r, s, rs\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \):

- the inverse image of \( \{1, r\} \) is \( \langle r \rangle \),
- the inverse image of \( \{1, s\} \) is \( \langle r^2, s \rangle \),
- the inverse image of \( \{1, rs\} \) 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 \( D_{2k} \) 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 \( D_n \to \mathbb{Z}/(2) \). 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 \( D_n \to \mathbb{Z}/(2) \) are \( r^a s^b \mapsto a \) mod 2 and \( r^a s^b \mapsto a+b \) mod 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 \( a + (-1)^b c \equiv a + c \mod 2 \) and \( a + (-1)^b c + b + d \equiv (a + b) + (c + d) \mod 2 \).

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 \( b \in \mathbb{Z} \), 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 \( \mathbb{Z} \) and is denoted \( \text{Aff}(\mathbb{Z}) \). 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 \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \) multiply, we can consider such matrices, with \( a = \pm 1 \) and \( b \in \mathbb{Z} \), as another model for the group \( \text{Aff}(\mathbb{Z}) \). 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 \( \text{Aff}(\mathbb{Z}) \) is generated by \( \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \).

In the polynomial model for \( \text{Aff}(\mathbb{Z}) \), the two generators in Theorem 4.1 are the functions \(-x\) and \( x + 1 \).

**Proof.** The elements of \( \text{Aff}(\mathbb{Z}) \) have the form

\[
\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k
\]

or

\[
\begin{pmatrix} -1 & \ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^\ell \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.
\]

While \( \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \) has order 2, \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) has infinite order. The group \( \text{Aff}(\mathbb{Z}) \) can be generated by two elements of order 2.

**Corollary 4.2.** The group \( \text{Aff}(\mathbb{Z}) \) is generated by \( \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \) and \( \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \), which each have order 2.
Proof. Check \((-1,-1)\) has order 2. By Theorem 4.1, it now suffices to show \((1,1)\) can be generated from \((-1,0)\) and \((-1,-1)\). It is their product, taken in the right order: 
\[
(-1,0)(-1,-1) = (1,1).
\]

In the polynomial model for \(\text{Aff}(\mathbb{Z})\), 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 \(\mathbb{Z}\).](image)

**Corollary 4.3.** The matrices \((-1,0)\) and \((-1,-1)\) are not conjugate in \(\text{Aff}(\mathbb{Z})\) and do not commute with a common element of order 2 in \(\text{Aff}(\mathbb{Z})\).

**Proof.** Every conjugate of \((-1,0)\) in \(\text{Aff}(\mathbb{Z})\) has the form \((-1,2b)\) for \(b \in \mathbb{Z}\), and \((-1,-1)\) does not have this form. Thus, the matrices are not conjugate. In \(\text{Aff}(\mathbb{Z})\), \((-1,0)\) commutes only with the identity and itself. □

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

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

**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 
\[x^{-1} = x\text{ and } y^{-1} = y,\]
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 \(x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y\). The relations 
\[x^2 = 1\text{ and } y^2 = 1\]
let us cancel all pairs of adjacent \(x\)'s or \(y\)'s, so \(x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y x y\) can be simplified to 
\[x y x y x y x y = (x y)^4 x.
\]
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 
\[(xy)^k, \ (yx)^k, \ (xy)^k x, \ (yx)^k y, \]
where \(k\) is a non-negative integer.

Before we look more closely at these products, let's indicate how the correspondence between \(G\) and \(\text{Aff}(\mathbb{Z})\) is going to work out. We want to think of \(x\) as \((-1,0)\) and \(y\) as \((-1,-1)\). Therefore the product \(x y\) should correspond to \((-1,0)(-1,-1) = (1,1)\), 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...
xy has finite order; granting that xy has finite order, the rest of the proof of Theorem 2.1 shows \((x,y)\) has to be a finite group.)

The proof of Theorem 4.1 shows each element of \(\text{Aff}(\mathbb{Z})\) is \((\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\)^k or \((\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})\)(−1 0) for some \(k \in \mathbb{Z}\). This suggests we should show each element of \(G\) has the form \((xy)^k\) or \((xy)^kx\).

Let \(z = xy\), so \(z^{-1} = y^{-1}x^{-1} = yx\). Also \(xx^{-1} = yx\), so
\[
xx^{-1} = z^{-1}. 
\]
(4.3)
The elements in (4.2) have the form \(z^k, xz^{-k}, xz^{-k}x,\) and \(z^{-k}y\), where \(k \geq 0\). Therefore elements of the first and second type are just integral powers of \(z\). Since \(z^{-k}y = z^{-k}yx = z^{-k-1}x\), 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 \(\text{Aff}(\mathbb{Z})\) and \(G = \langle x, y \rangle\), based on the formulas in (4.1) and (4). Let \(f: \text{Aff}(\mathbb{Z}) \rightarrow G\) by
\[
f \left( \begin{array}{cc} 1 & k \\ 0 & 1 \end{array} \right) = z^k, \quad f \left( \begin{array}{cc} -1 & k \\ 0 & 1 \end{array} \right) = z^kx.
\]
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 \(\text{Aff}(\mathbb{Z})\). Some cases will need the relation \(xx^n = z^{-n}x\), which follows from raising both sides of (4.3) 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., \(xyxyxy = xyxy\)). 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 \(\text{Aff}(\mathbb{Z})\) is isomorphic to \(\text{Aff}(\mathbb{Z})\) or to \(D_n\) for some \(n \geq 1\).

**Proof.** Since \(\text{Aff}(\mathbb{Z})\) is generated by two elements of order 2, each nontrivial quotient group of \(\text{Aff}(\mathbb{Z})\) 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 \(\mathbb{Z}/(2) = D_1\). If both generators have order 2 then the quotient group is isomorphic to \(\text{Aff}(\mathbb{Z})\) 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 \(\text{Aff}(\mathbb{Z})\). For \(n \geq 3\), reducing matrix entries modulo \(n\) gives a homomorphism \(\text{Aff}(\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/(n))\) whose image is the matrix group \(D_n\) from (1.3), which is isomorphic to \(D_n\). The map \((\begin{smallmatrix} a \\ b \\ 0 & 1 \end{smallmatrix}) \mapsto (a, b \text{ mod } 2)\) is a homomorphism from \(\text{Aff}(\mathbb{Z})\) onto \(\{\pm 1\} \times \mathbb{Z}/(2) \cong D_2\) and the map \((\begin{smallmatrix} a \\ b \\ 0 & 1 \end{smallmatrix}) \mapsto a\) is a homomorphism from \(\text{Aff}(\mathbb{Z})\) onto \{±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 \(n \geq 1\), \((\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})\) \(\triangleleft \text{Aff}(\mathbb{Z})\) and \(\text{Aff}(\mathbb{Z})/(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})) \cong D_n\). This common pattern is another justification for our definition of the dihedral groups \(D_1\) and \(D_2\).