DIHEDRAL GROUPS II

KEITH CONRAD

1. Conjugacy classes

Theorem 1.1. *The conjugacy classes in D_n are as follows, depending on the parity of n.*

(1) *Odd n:* $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(n-1)/2}\}, \{r^i s : 0 \leq i \leq n-1\}$.
(2) *Even n:* $\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(\frac{n}{2}-1)}\}, \{r^{\frac{n}{2}}\}, \{r^{2i} s : 0 \leq i \leq \frac{n}{2}-1\}$, *and* $\{r^{2i+1} s : 0 \leq i \leq \frac{n}{2}-1\}$.

In words, a rotation is conjugate only to its inverse (which is a different rotation except for 1 and, for even n, $r^{n/2}$) and the set of reflections falls into either one or two conjugacy classes depending on whether or not n is odd or even. It makes sense geometrically that all reflections in D_n are conjugate for odd n but they break into two conjugacy classes for even n: for odd n every reflection has the same kind of geometric description (a reflection across a line linking a vertex to the midpoint of the opposite side), while for even n the reflections are of two kinds: across a line through opposite vertices or across a line bisecting opposite edges. These two types of reflections are the two conjugacy classes of reflections in D_n for even n.

Proof. Every rotation is conjugate to its inverse, since

$$sr^j s^{-1} = r^{-j}.$$

More generally, the formulas

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

as i varies show the only conjugates of r^j in D_n are r^j and r^{-j}.

To find the conjugacy class of s, we compute

$$r^i s r^{-i} = r^{2i} s, \quad (r^i s) s (r^i s)^{-1} = r^{2i} s.$$

As i varies, $r^{2i}s$ runs through the reflections in which r occurs with an exponent divisible by 2. If n is odd then every integer modulo n is a multiple of 2 (since 2 is invertible mod n so we can solve $a \equiv 2x \bmod n$ given a). Therefore

$$\{r^{2i} s : i \in \mathbf{Z}\} = \{r^i s : i \in \mathbf{Z}\},$$

so every reflection in D_n is conjugate to s for odd n. When n is even, however, we only get half the reflections as conjugates of s. The other half are conjugate to rs:

$$r^i (rs) r^{-i} = r^{2i+1} s, \quad (r^i s)(rs)(r^i s)^{-1} = r^{2i-1} s.$$

As i varies, this gives us $\{rs, r^3 s, \ldots, r^{n-1} s\}$. □

In the following two tables, the first row gives a representative element from each conjugacy class in D_n and the second row gives the size of the conjugacy class of that element. In the tables, r^k is a rotation with $1 \leq k < n/2$. Thus, there are $(n-1)/2$ pairs of conjugate rotations for odd n (exclude the identity) and $n/2 - 1$ pairs of conjugate rotations for even

n (exclude the identity and $r^{n/2}$). In both cases, whether n is even or odd, check the sum of the sizes of the conjugacy classes in D_n equals $2n$.

Rep.	1	r	r^2	$\cdots$	$r^{(n-1)/2}$	s
Size	1	2	2	$\cdots$	2	n

TABLE 1. Conjugacy class representatives in D_n for n odd

Rep.	1	r	r^2	$\cdots$	$r^{n/2-1}$	$r^{n/2}$	s	rs
Size	1	2	2	$\cdots$	2	1	$n/2$	$n/2$

TABLE 2. Conjugacy class representatives in D_n for n even

Theorem 1.2. *When $n \geq 3$ is odd, the center of D_n is trivial. When $n \geq 3$ is even, the center of D_n is $\{1, r^{n/2}\}$.*

Proof. This is immediate from the tables, since the center is the set of elements which are in conjugacy classes of size 1. □

Example 1.3. The group D_3 has trivial center. The group D_4 has center $\{1, r^2\}$.

Corollary 1.4. *If $n \geq 6$ is twice an odd number then $D_n \cong D_{n/2} \times \mathbf{Z}/(2)$.*

Proof. Let $H = \langle r^2, s\rangle \cong D_{n/2}$ and $Z = \{1, r^{n/2}\}$. Then $Z \lhd D_n$, so HZ is a subgroup of D_n and the elements of H commute with the elements of Z.

Let $f\colon H \times Z \to D_n$ by $f(h, z) = hz$. This is a homomorphism since Z is the center of D_n. The kernel is $H \cap Z$, which is trivial. That is, $r^{n/2} \notin H$. Indeed, if $r^{n/2} \in H$ then either $r^{n/2} = r^{2k}$ or $r^{n/2} = r^{2k}s$ for some k. The first condition implies $n/2 \equiv 2k \bmod n$, which is impossible since $2k$ and the modulus n are even but $n/2$ is odd. The second condition is impossible since it implies s is a power of r.

Since f is injective and $\#(H \times Z) = 2n = \#D_n$, f is an isomorphism. □

There is no isomorphism as in Corollary 1.4 when n is divisible by 4: since n and $n/2$ are even the center of D_n is cyclic of size 2 and the center of $D_{n/2} \times \mathbf{Z}/(2)$ is a direct product of two cyclic groups of size 2. Therefore the centers are not isomorphic, so $D_n \ncong D_{n/2} \times \mathbf{Z}/(2)$.

Theorem 1.5. *The commutator subgroup of D_n is $\langle r^2\rangle$.*

Proof. The commutator $[r, s]$ is $rsr^{-1}s^{-1} = rrss^{-1} = r^2$, so r^2 is a commutator and thus $\langle r^2\rangle$ is in the commutator subgroup.

To show the commutator subgroup is in $\langle r^2\rangle$, it suffices to show every commutator is in $\langle r^2\rangle$. There are two ways to do this: tediously and conceptually. The tedious way is to calculate a general commutator and see it is a power of r^2. Let's do that, just to appreciate the second way that will be shown.

Since $s^j r^i = r^{(-1)^j i} s^j$, a general commutator in D_n is (ready?)

$$\begin{aligned}
[r^i s^j, r^{i'} s^{j'}] &= (r^i s^j)(r^{i'} s^{j'})(r^i s^j)^{-1}(r^{i'} s^{j'})^{-1} \\
&= r^i r^{(-1)^j i'} s^j s^{j'} s^{-j} r^{-i} s^{-j'} r^{-i'} \\
&= r^{i+(-1)^j i'} s^{j'} r^{-i} r^{(-1)^{-j'}(-i')} s^{-j'} \\
&= r^{i+(-1)^j i'} s^{j'} r^{-i+(-1)^{j'+1} i'} s^{-j'} \\
&= r^{i+(-1)^j i' r^{(-1)^{j'}(-i+(-1)^{j'+1} i')} s^{j'} s^{-j'}} \\
&= r^{i+(-1)^j i'+(-1)^{j'+1} i+(-1)^{j'+j'+1} i'}.
\end{aligned}$$

That exponent looks like (well, it is) a mess, but it is even since modulo 2 the exponent is $i + i' + i + i' \equiv 0 \bmod 2$, Therefore a general commutator in D_n is a power of r^2, because we actually computed it.

Now we will show any commutator is a power of r^2 by a method using our brains. If we can find a quotient group D_n/N which is abelian, then all commutators in D_n are trivial in D_n/N, and hence all commutators in D_n lie in N. Very well then, let's try $N = \langle r^2 \rangle$. First of all, is this subgroup normal? Yes, because the conjugates of a power of r^2 are the power itself and its inverse, which both are in N. Next, is the group D_n/N abelian? Yes: it has size 4 and in fact is represented by $\{\overline{1}, \overline{r}, \overline{s}, \overline{rs}\}$ with $sr \equiv rs \bmod N$ because $r \equiv r^{-1} \bmod N$ (after all, $r^2 \in N$). Thus D_n/N is abelian, so all commutators in D_n are in $\langle r^2 \rangle$. □

When n is odd, r and r^2 generate the same cyclic subgroup, so we can say D_n has commutator subgroup $\langle r \rangle$. However, $\langle r \rangle$ is not the commutator subgroup of D_n for even n.

2. Abstract characterization of D_n

Abstracting the relation $srs^{-1} = r^{-1}$ between r and s leads us to see that any group with properties resembling D_n is a homomorphic image of D_n, and is isomorphic to D_n if it has the same size.

Theorem 2.1. *Let G be generated by elements a and b where $a^n = 1$ for some $n \geq 3$, $b^2 = 1$, and $bab^{-1} = a^{-1}$. There is a surjective homomorphism $D_n \to G$, and if $\#G = 2n$ then this homomorphism is an isomorphism.*

The hypotheses $a^n = 1$ and $b^2 = 1$ do *not* mean a has order n and b has order 2, only that their orders divide n and divide 2. For instance, the trivial group has the form $\langle a, b \rangle$ where $a^n = 1$, $b^2 = 1$, and $bab^{-1} = a^{-1}$ (take a and b to be the identity). The trivial group is a homomorphic image of D_n.

Proof. The conjugation relation $bab^{-1} = a^{-1}$ implies $ba^j b^{-1} = a^{-j}$ for any $j \in \mathbf{Z}$. Conjugating by b repeatedly gives

$$b^k a^j b^{-k} = a^{(-1)^k j},$$

so

$$b^k a^j = a^{(-1)^k j} b^k. \tag{2.1}$$

Thus, any product of a's and b's can have all the a's brought to one side and all the b's brought to the other side (either side). This shows, taking into account that $a^n = 1$ and

$b^2 = 1$, that

$$\begin{aligned} G &= \langle a, b\rangle \\ &= \{a^j, a^j b : j \in \mathbf{Z}\} \\ &= \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}. \end{aligned} \tag{2.2}$$

Thus G is a finite group with $\#G \leq 2n$.

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

$$f(r^j s^k) = a^j b^k.$$

This function makes sense, since the only ambiguity in writing an element of D_n as $r^j s^k$ is that j can change modulo n and k can change modulo 2. This has no effect on the right side, since $a^n = 1$ and $b^2 = 1$.

To check f is a homomorphism, we use (2.1):

$$\begin{aligned} f(r^j s^k)f(r^{j'} s^{k'}) &= a^j b^k a^{j'} b^{k'} \\ &= a^j a^{(-1)^k j'} b^k b^{k'} \\ &= a^{j+(-1)^k j'} b^{k+k'} \end{aligned}$$

and

$$\begin{aligned} f((r^j s^k)(r^{j'} s^{k'})) &= f(r^j r^{(-1)^k j'} s^k s^{k'}) \\ &= f(r^{j+(-1)^k j'} s^{k+k'}) \\ &= a^{j+(-1)^k j'} b^{k+k'}. \end{aligned}$$

The results agree, so f is a homomorphism from D_n to G. It is onto since its image is a subgroup of G containing $a = f(r)$ and $b = f(s)$, which generate G by hypothesis. (Alternatively, from (2.2) every element of G has the form $a^j b^k$ for some j and k, so f is onto by its defining formula.)

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

Remark 2.2. The homomorphism $f\colon D_n \to G$ constructed in the proof is the only one where $f(r) = a$ and $f(s) = b$: if there is any such homomorphism then $f(r^j s^k) = f(r)^j f(s)^k = a^j b^k$. So a more precise formulation of Theorem 2.1 is this: for any group $G = \langle a, b\rangle$ where $a^n = 1$ for some $n \geq 3$, $b^2 = 1$, and $bab^{-1} = a^{-1}$, there is a *unique* homomorphism $D_n \to G$ sending r to a and s to b. 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 2.1.

As an application of Theorem 2.1, we can write down a 2×2 matrix group over $\mathbf{Z}/(n)$ which is isomorphic to D_n when $n \geq 3$. Set

$$\widetilde{D}_n = \left\{ \begin{pmatrix} \pm 1 & c \\ 0 & 1 \end{pmatrix} : c \in \mathbf{Z}/(n) \right\}. \tag{2.3}$$

This is a subgroup of $\mathrm{GL}_2(\mathbf{Z}/(n))$; it can also be described as the linear polynomials on $\mathbf{Z}/(n)$ of the form $f(x) = \varepsilon x + c$, where $\varepsilon = \pm 1$ and c vary. The composition of such linear polynomials matches the multiplication of the corresponding 2×2 matrices over $\mathbf{Z}/(n)$.

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

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

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

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

Thus, by Theorem 2.1, $\widetilde{D}_n$ is isomorphic to D_n, using $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in the role of r and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in the role of s. This algebraic realization of D_n inside $\mathrm{GL}_2(\mathbf{Z}/(n))$ should not be confused with the geometric realization of D_n as a subgroup of $\mathrm{GL}_2(\mathbf{R})$ in terms of rigid motions of $\mathbf{R}^2$ by real matrices ($r = \left(\begin{smallmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{smallmatrix}\right)$ and $s = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$).

3. Dihedral groups and reflections

In D_n, we can obtain r from s and rs (just multiply: $rs \cdot s = rs^2 = r$), so we can use the reflections rs and s as generators for D_n:

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

In group-theoretic terms, D_n is generated by two elements of order 2. They do not commute: $rs \cdot s = r$ and $s \cdot rs = srs = r^{-1}ss = r^{-1}$.

What 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 additive group $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$, 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, it turns out that G is essentially a dihedral group!

Theorem 3.1. *Let G be a finite non-abelian 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 non-abelian 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.) 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, $n | \#G$. Since $b \notin \langle a \rangle$, $\#G > n$, so $\#G \geq 2n$.

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

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

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

$$bab^{-1} = yxyy = yx, \quad a^{-1} = y^{-1}x^{-1} = yx, \tag{3.1}$$

where the last equation is due to x and y having order 2, we obtain $bab^{-1} = a^{-1}$. By Theorem 2.1, there is a surjective homomorphism $D_n \to G$, so $\#G \leq 2n$. We saw before that $\#G \geq 2n$, so $\#G = 2n$ and $G \cong D_n$. □

Theorem 3.1 says we know all the finite *non-abelian* 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 3.1. Such a group is isomorphic to $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ or (in the degenerate case that the two generators are equal) to $\mathbf{Z}/(2)$. So we can define new dihedral groups

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

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

- $\#D_n = 2n$ for every $n > 0$,
- the dihedral groups are precisely the finite groups generated by two elements of order 2,
- Theorems 1.1 and 1.5 are true for all $n > 0$,
- for even $n > 0$, Corollary 1.4 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 $n > 0$.

However, D_1 and D_2 don't satisfy all previous properties of dihedral groups. For example,

- Theorem 1.2 is false when $n \leq 2$,
- the matrix model for D_n over $\mathbf{Z}/(n)$ doesn't work when $n \leq 2$,
- D_n can't be viewed as a subgroup of S_n for $n \leq 2$ since $2n > n!$ for these n.

Remark 3.2. Unlike finite groups generated by two elements of order 2, there is no elementary description of all finite groups generated by two elements with equal order > 2.

The following corollary of Theorem 3.1 applies our knowledge of dihedral groups to elements of order 2 in any finite group.

Corollary 3.3. *In any finite group with two elements x and y of order 2, either x is conjugate to y or x and y commute with a common element of order 2.*

Proof. If x and y commute, the second case occurs. Now assume x and y do not commute. Then Theorem 3.1 says the subgroup $\langle x, y \rangle$ is isomorphic to a dihedral group D_n, where $n \geq 3$. If $\langle x, y \rangle$ is isomorphic to D_n for odd n, then all order 2 elements in $\langle x, y \rangle$ are conjugate to each other (recall the description of the conjugacy classes of dihedral groups in Section 1), so x and y are conjugate. If $\langle x, y \rangle$ is isomorphic to D_n for even n, then the center of $\langle x, y \rangle$ contains an element of order 2 (use the classification of the center of dihedral groups in Theorem 1.2), so x and y commute with some element of order 2. □

Theorem 3.4. *Any nontrivial homomorphic image of a dihedral group is dihedral.*

Proof. A dihedral group is generated by two elements of order equal to 2. Any homomorphic image is a group generated by two elements of order dividing 2. If those two elements have order 2, the image is dihedral (possibly D_1 or D_2). If one of the elements has order 1 then the image is cyclic of order 2, and thus dihedral since $D_1 = \mathbf{Z}/(2)$. □

A converse of Theorem 3.4 is true: every dihedral group is the homomorphic image of a dihedral group (with nontrivial kernel). For even $n \geq 4$, $Z(D_n) = \{1, r^{n/2}\}$, so $D_n/Z(D_n)$ has order $(2n)/2 = n = 2(n/2)$ and is generated by the images $\overline{r}$ (with order $n/2$ in $D_n/Z(D_n)$) and $\overline{s}$ (with order 2), subject to the relation $\overline{srs}^{-1} = \overline{r}^{-1}$. Therefore $D_n/Z(D_n) \cong D_{n/2}$ and $\#D_{n/2} = 2(n/2) = n$. The group $D_1 = \mathbf{Z}/(2)$ is isomorphic to $D_n/\langle r\rangle$ for any $n \geq 3$.

4. Subgroups of D_n

We will list all the subgroups of D_n and then collect them into conjugacy classes. Our results are valid even in the special cases $n = 1$ 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 4.1. *Every subgroup of D_n is cyclic or dihedral. A complete listing of the subgroups are as follows:*

1. *cyclic subgroups $\langle r^d\rangle$, where $d|n$, with index $2d$,*
2. *dihedral subgroups $\langle r^d, r^i s\rangle$, where $d|n$ and $0 \leq i \leq d-1$, with index d.*

Every subgroup of D_n occurs exactly once in this listing.

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

Let H be a subgroup of D_n. The composite homomorphism $H \hookrightarrow D_n \to D_n/\langle r\rangle$ to a group of order 2 is either trivial or onto. Its kernel is $H \cap \langle r\rangle$.

If the homomorphism is trivial then $H = H \cap \langle r\rangle$, so $H \subset \langle r\rangle$, which means $H = \langle r^d\rangle$ for a unique $d|n$. The order of $\langle r^d\rangle$ is n/d and its index is $2n/(n/d) = 2d$.

If the homomorphism $H \to D_n/\langle r\rangle$ is onto then $H/(H \cap \langle r\rangle)$ has order 2, so $H \cap \langle r\rangle$ has index 2 in H. Set $H \cap \langle r\rangle = \langle r^d\rangle$, so $[H : \langle r^d\rangle] = 2$. Since $\langle r^d\rangle$ has order n/d, $\#H = 2n/d$ and $[D_n : H] = 2n/\#H = d$. Choosing $h \in H$ with $h \notin \langle r^d\rangle$, we know h is not a power of r since $\langle r^d\rangle = H \cap \langle r\rangle$, so h is a reflection. Write $h = r^i s$. Then H contains

$$\left\{r^{dk}, r^{dk+i}s : 0 \leq k \leq \frac{n}{d} - 1\right\},$$

which is already $2(n/d)$ terms, so $H = \langle r^d, r^i s\rangle$. Multiplying $r^i s$ by an appropriate power of r^d will produce an $r^j s$ where $0 \leq j \leq d-1$, and we can replace $r^i s$ with this $r^j s$ in the generating set. So we may assume $0 \leq i \leq d-1$. The subgroup $\langle r^d, r^i s\rangle$ is dihedral since it is nontrivial and is generated by two elements of order 2 ($r^i s$ and $r^d \cdot r^i s$). Since r^d has order n/d, the order of $\langle r^d, r^i s\rangle$ is $2(n/d) = 2n/d$, whose index in D_n is d.

To check the two lists of subgroups in the theorem have no duplications, first we show the lists are disjoint. The only dihedral groups which are cyclic are groups of order 2, and $\langle r^d, r^i s\rangle$ has order 2 only when $d = n$. The subgroup $\langle r^n, r^i s\rangle = \langle r^i s\rangle$ has order 2 and $r^i s$ is not a power of r, so this subgroup is not on the first list.

The first list of subgroups has no duplications since the order of $\langle r^d\rangle$ changes when we change d (among positive divisors of n). If the second list of subgroups has a duplication, say $\langle r^d, r^i s\rangle = \langle r^e, r^j s\rangle$, then computing the index in D_n shows $d = e$. The reflections in $\langle r^d, r^i s\rangle$ are all $r^{dk+i}s$, so $r^j s = r^{dk+i}s$ for some k. Therefore $j \equiv dk + i \bmod n$, and from $d|n$ we further get $j \equiv i \bmod d$. That forces $j = i$, since $0 \leq i, j \leq d-1$. □

Corollary 4.2. *Let n be odd and $m|2n$. 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 $m|2n$.

- *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 $m|n$ 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 $d|n$. From the list of subgroups of D_n in Theorem 4.1, any subgroup with odd index is dihedral and any subgroup with even index is inside $\langle r\rangle$. 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. The only subgroup with even index m is $\langle r^{m/2}\rangle$ by Theorem 4.1.

If n is even and m is an odd divisor of $2n$, so $m|n$, 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 $(m/2)|n$, $\langle r^{m/2}\rangle$ 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 our knowledge of all subgroups of D_n we can count the conjugacy classes of subgroups.

Theorem 4.3. *Let n be odd and $m|2n$. 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 $m|2n$.

- *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 $m|n$ then any 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 $m|n$.

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, $m|n$ and any 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 any conjugation sending s to $r^i s$ turns $\langle r^m, s\rangle$ into $\langle r^{\pm m}, r^i s\rangle = \langle r^m, r^i s\rangle$. When n is odd and m is even, the only subgroup of D_n with even index m is $\langle r^{m/2}\rangle$ by Theorem 4.1.

If n is even and m is an odd divisor of $2n$, so $m|n$, a subgroup of D_n with index m is some $\langle r^m, r^i s\rangle$ where $0 \leq i \leq m-1$. Since $r^i s$ is conjugate to s or rs (depending on the parity of i), and the only conjugates of r^m are $r^{\pm m}$, $\langle r^m, r^i s\rangle$ is conjugate to $\langle r^m, s\rangle$ or $\langle r^m, rs\rangle$. Note $\langle r^m, s\rangle = \langle r^m, r^m s\rangle$ and $r^m s$ is conjugate to rs (because m is odd), Any 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 $(m/2)|n$, Theorem 4.1 tells us $\langle r^{m/2}\rangle$ has index m. Any other subgroup of index m is $\langle r^m, r^i s\rangle$ for some i, and this occurs only when $m|n$, 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 4.4. The only subgroup of D_5 with index 2 is $\langle r\rangle$ and all 5 subgroups with index 5 are conjugate to $\langle r^5, s\rangle$.

Example 4.5. 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 4.6. 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 4.7. When $k \geq 3$, the dihedral group D_{2^k} has three conjugacy classes of subgroups with each index $2, 4, \ldots, 2^{k-1}$.

Corollary 4.8. *When n is odd, the proper normal subgroups of D_n are $\langle r^d\rangle$ for $d|n$; these are the subgroups with even index.*

When n is even, the proper normal subgroups of D_n are $\langle r^d\rangle$ with index d when $d|n$ and $\langle r^2, s\rangle$ 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. This is left to the reader. □

Example 4.9. The only nontrivial proper normal subgroup of D_5 is $\langle r\rangle$, with index 2.

Example 4.10. 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 4.11. 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 4.12. When $k \geq 3$, the dihedral group D_{2^k} has one normal subgroup of each index except for three normal subgroups of index 2.

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

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

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

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

Appendix A. An infinite dihedral-like group

In Theorem 3.1, 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 non-abelian group generated by two elements of order 2 really be infinite? Yes! In this appendix we construct such a group and show that there is only one such group up to isomorphism.

Our group will be built out of the linear functions $f(x) = ax + b$ where $a = \pm 1$ and $b \in \mathbf{Z}$, with the group law being composition. For instance, the inverse of $-x$ is itself and the inverse of $x + 5$ is $x - 5$. This group is called the *affine group* over $\mathbf{Z}$ and is denoted $\mathrm{Aff}(\mathbf{Z})$. The label "affine" is just a fancy name for "linear function with a constant term." In linear algebra, the functions which 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 any confusion with the more restricted linear algebra sense of the term "linear function."

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

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

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

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

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

or

$$\begin{pmatrix} -1 & \ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^\ell \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{A.2}$$

□

While $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order. However, we can also generate $\mathrm{Aff}(\mathbf{Z})$ by two matrices of order 2.

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

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

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

The next corollary shows Corollary 3.3 need not hold if x and y lie in an infinite group.

Corollary A.3. *The matrices* $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ *are not conjugate in* $\mathrm{Aff}(\mathbf{Z})$ *and do not commute with a common element of order* 2 *in* $\mathrm{Aff}(\mathbf{Z})$*.*

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

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

Theorem A.4. *Any infinite group generated by two elements of order* 2 *is isomorphic to* $\mathrm{Aff}(\mathbf{Z})$*.*

Proof. Write such a group as G and its two generators of order 2 as x and y. Since G is infinite, x and y do not commute. (Otherwise $\langle x, y\rangle = \{1, x, y, xy\}$ has only 4 elements.) Since $x^{-1} = x$ and $y^{-1} = y$, we do not need to use any 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 any pair of adjacent x's or y's, so $xyyxxyxyxyxyxyxxy$ can be simplified to

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

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

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

$$(xy)^k, \quad (yx)^k, \quad (xy)^kx, \quad (yx)^ky, \tag{A.3}$$

where k is a non-negative integer.

Before we look more closely at these products, let's indicate how the correspondence between G and $\mathrm{Aff}(\mathbf{Z})$ is going to work out. We want to think of x as $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and y as $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. Therefore the product xy should correspond to $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and in particular have infinite order. Does xy really have infinite order? Yes, because if xy has finite order, the proof of Theorem 3.1 shows $G = \langle x, y\rangle$ is a finite group. (The finiteness hypothesis on the group in the statement of Theorem 3.1 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 3.1 shows $\langle x, y\rangle$ has to be a finite group.)

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

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

$$xzx^{-1} = z^{-1}. \tag{A.4}$$

The elements in (A.3) have the form z^k, z^{-k}, z^kx, and $z^{-k}y$, where $k \geq 0$. Therefore elements of the first and second type are just integral powers of z. Since $z^{-k}y = z^{-k}yxx = z^{-k-1}x$, elements of the third and fourth type are just integral powers of z multiplied on the right by x.

Now we make a correspondence between $\mathrm{Aff}(\mathbf{Z})$ and $G = \langle x, y\rangle$, based on the formulas in (A.1) and (A.2). Let $f\colon \mathrm{Aff}(\mathbf{Z}) \to G$ 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 $f(AB) = f(A)f(B)$ for any A and B in $\mathrm{Aff}(\mathbf{Z})$. Some cases will need the relation $xz^n = z^{-n}x$, which follows from raising both sides of (A.4) to the n-th power. □

Remark A.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 any pair of adjacent x's or adjacent y's can be cancelled (*e.g.*, $xyxxxy = xyxy$). Because the only relation imposed (beyond the group axioms) is that xx and yy are the identity, this group is called a *free group* on two elements of order 2.

Corollary A.6. *Every quotient group of* $\mathrm{Aff}(\mathbf{Z})$ *is isomorphic to* $\mathrm{Aff}(\mathbf{Z})$ *or to* D_n *for some* $n \geq 1$.

Proof. Any quotient of $\mathrm{Aff}(\mathbf{Z})$ is a group generated by two elements of order 2. If the quotient is infinite then it is isomorphic to $\mathrm{Aff}(\mathbf{Z})$ by Theorem A.4. If the quotient is finite then it is isomorphic to some D_n since the finite groups generated by two elements of order 2 are the dihedral groups. □

Every dihedral group arises as a quotient of $\mathrm{Aff}(\mathbf{Z})$. For $n \geq 3$, reducing matrix entries modulo n gives a homomorphism $\mathrm{Aff}(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/(n))$ whose image is the matrix group $\widetilde{D}_n$ from (2.3), which is isomorphic to D_n. The map $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto (a, b \bmod 2)$ is a homomorphism from $\mathrm{Aff}(\mathbf{Z})$ onto $\{\pm 1\} \times \mathbf{Z}/(2) \cong D_2$ and the map $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto a$ is a homomorphism from $\mathrm{Aff}(\mathbf{Z})$ onto $\{\pm 1\} \cong D_1$. Considering the kernels of these homomorphisms for $n \geq 3$, $n = 2$, and $n = 1$ reveals that we can describe all of these maps onto dihedral groups in a uniform way: for any $n \geq 1$, $\langle \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \rangle \lhd \mathrm{Aff}(\mathbf{Z})$ and $\mathrm{Aff}(\mathbf{Z})/\langle \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \rangle \cong D_n$. This common pattern is another justification for our definition of the dihedral groups D_1 and D_2.