Dihedral groups revisited

Let us determine the subgroup structure of dihedral groups. First we recall the definition.

Definition 1. The dihedral group D_{2n} is generated by a *rotation* a and a *reflexion* b with relations

$$a^n = e$$
$$b^2 = e$$
$$ab = b^{-1}a.$$

Elements of the form a^k are called *rotations*. Elements of the form $a^k b$ are called *reflexions*.

Note that we have

$$a^k b = ba^{n-k}$$

Any element of the dihedral group can be written a^k or $a^k b$ for $0 \leq k < n$.

Normal subgroups of dihedral groups

We identify the normal subgroups. Note that the subgroup generated by a is normal since it has index 2. Let N denote the normal subgroup we are trying to track down.

Case: n is odd

For $n = 2k + 1$, the conjugacy classes are:

$$\{e\}, \{a, a^{n-1}\}, \{a^2, a^{n-2}\} \ldots \{a^k, a^{k+1}\} \quad \text{and} \quad \{a^i b \mid 0 \leq i < n\}.$$

Recall that an equivalent definition for a normal subgroup is one that is a union of conjugacy classes.

If a single reflexion is in N, then they all are. Even worse, that conjugacy class is not a subgroup – so to contain this class, you need that class and more. That means N is more than half the group, so indeed, that would require N to be the whole group.

So the *only* normal subgroups that are not the whole D_{2n} are contained in $\langle a \rangle$, the cyclic group generated by a which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. We know the subgroups of that are of the form $\langle a^d \rangle$. For each divisor d of n, we get a different normal subgroup.

So the normal subgroups are:

$$\begin{aligned}
&\langle a^0 \rangle = e, \\
&\langle a^d \rangle \quad \forall d(d \leq n, d|n), \\
&D_{2n}
\end{aligned}$$

And that's all. Pretty simple.

Case: n is even

The even case is harder. Say $n = 2k$.

First of all, there is actually a centre to this group:

$$Z(D_{2n}) = \{e, a^k\}.$$

That is a normal subgroup already that we would have gotten by our previous argument – since it's inside $\langle a \rangle$. So far then, nothing unknown. But what are the conjugacy classes? They are not the same.

They are the following:

$$\begin{aligned}
&\{e\}, \{a, a^{n-1}\}, \{a^2, a^{n-2},\} \ldots, \{a^{k-1}, a^{k+1}\}, \{a^k\} \\
&\text{and} \quad \{a^{2i}b, 0 \leq i \leq k\}, \quad \text{the even reflexions} \\
&\text{and} \quad \{a^{2i+1}b, 0 \leq i \leq k\}, \quad \text{the odd reflexions.}
\end{aligned}$$

So we can definitely still get all of the subgroups of $\langle a \rangle$.

What else can we get? Well, we have our unknown normal subgroup N. If N contains any reflexions, it has at least one quarter of G – so it's pretty big. Assume it contains $a^j b$. If j is even, then N contains b and $a^2 b$, and thus it contains a^2.

If j is odd, then N contains ab and $a^3 b$, so it contains $a^2 = a^3 bab$.

So in fact, N contains even more of G – half of it in fact. It must contain $\langle a^2 \rangle$, which is a quarter of G, and one of the conjugacy classes – either the odd reflexions, or the even ones. And of course, we don't want to include anything more – or else $N = G$.

So in the end, we get the following normal subgroups:

$$\begin{aligned}
&\langle a^0 \rangle = e \\
&\langle a^d \rangle \quad 0 < d \leq n, d \mid n, \\
&\langle a^2, b \rangle \\
&\langle a^2, ab \rangle \\
&D_{2n}
\end{aligned}$$

So in the even case, there are precisely two extra normal subgroups.

Subgroups of dihedral groups

We identify the whole subgroups of dihedral groups, regardless of whether they are normal or not, by following Stephan A. Cavior.

Definition 2. Let $n \geq 1$ be an integer. The number of divisors of n is denoted by $\tau(n)$. Also the sum of divisors of n is denoted by $\sigma(n)$.

Example 3. $\sigma(8) = 1 + 2 + 4 + 8 = 15$ and $\tau(8) = 4$.

We will prove that if $n \geq 3$, then number of subgroups of D_{2n} is $\tau(n) + \sigma(n)$.

Lemma 4. *The number of subgroups of a cyclic group of order $n \geq 1$ is $\tau(n)$.*

Proof. Let G be a cyclic group of order n. Then $G \cong \mathbb{Z}/n\mathbb{Z}$. A subgroup of $\mathbb{Z}/n\mathbb{Z}$ is in the form $d\mathbb{Z}/n\mathbb{Z}$ where $d\mathbb{Z} \supseteq n\mathbb{Z}$. The condition $d\mathbb{Z} \supseteq n\mathbb{Z}$ is obviously equivalent to $d \mid n$. $\square$

Lemma 5. *Let b be an element of order n in D_{2n} and let H be any subgroup of D_{2n}. Then either $H \subseteq \langle b \rangle$ or $|H \cap \langle b \rangle| = d$ and $|H| = 2d$ for some $d \mid n$.*

Proof. Let $N = \langle b \rangle$. Clearly N is a normal subgroup of D_{2n} because $[D_{2n} \colon N] = 2$. Thus HN is a subgroup of D_{2n} and hence

$$|HN| \mid 2n. \tag{6}$$

On the other hand,

$$|HN| = \frac{|H| \cdot |N|}{|H \cap N|} = \frac{n|H|}{|H \cap N|}.$$

Therefore, by (6), $\frac{|H|}{|H \cap N|} \mid 2$. Hence either $|H| = |H \cap N|$ or $|H| = 2|H \cap N|$. If $|H| = |H \cap N|$, then $H = H \cap N$ and thus $H \subseteq N$. If $|H| = 2|H \cap N|$, then let $|H \cap N| = d$ and so $|H| = 2d$. Clearly $d \mid n$ because $H \cap N$ is a subgroup of N and $|N| = n$. $\square$

Lemma 7. *Given $d \mid n$, let $m = n/d$. For every $0 \leq i < n$ let $A(i, d) = \{ab^{i+km} \mid 0 \leq k < d\}$. Let $B(i, d) = A(i, d) \cup \langle b^m \rangle$. Then $B(i, d)$ is a subgroup of D_{2n} and $|B(i, d)| = 2d$. We also have $|\{B(i, d) \mid 0 \leq i < n\}| = m$.*

Proof. If $ab^{i+km} = ab^{i+rm}$, for some $0 \leq k, r < d$, then $b^{(k-r)m} = 1$ and thus $d \mid (k - r)$, because $\text{ord}(b) = n = md$. Therefore $k = r$ because $0 \leq k, r < d$. So $|A(i, d)| = d$. Clearly $A(i, d) \cap \langle b^m \rangle = \varnothing$ and $|\langle b^m \rangle| = d$, because $\text{ord}(b) = n$. Thus $|B(i, d)| = |A(i, d)| + |\langle b^m \rangle| = 2d$. Proving that $B(i, d)$ is a subgroup of D_{2n} is easy. Just note that every element of $A(i, d)$ is the inverse of itself (because they all have order two) and also note that $ab^s = b^{-s}a$ for all s, because $ab = b^{-1}a$. Finally, the set $\{B(i, d) \mid 0 \leq i < n\}$ has m elements because clearly $B(i, d) = B(j, d)$ if and only if $A(i, d) = A(j, d)$ if and only if $i \equiv j \bmod m$. $\square$

Theorem 8 (Stephan A. Cavior, 1975)**.** *If $n \geq 3$, then the number of subgroups of D_{2n} is $\tau(n) + \sigma(n)$.*

Proof. Suppose that H is a subgroup of D_{2n}. There are two cases to consider.

Case 1 . $H \subseteq \langle b \rangle$. By Lemma 4, the number of these subgroups is $\tau(n)$.

Case 2 . In this case, by Lemma 5, we have $|H| = 2d$ and $|H \cap \langle b \rangle| = d$, for some $d \mid n$. Let $n = md$. Since $H \cap \langle b \rangle$ is a subgroup of $\langle b \rangle$, which is a cyclic group of order n, we have

$$H \cap \langle b \rangle = \langle b^m \rangle. \tag{9}$$

Let $A(i, d)$ and $B(i, d)$ be as they were defined in Lemma 7. Now, since H is not contained in $\langle b \rangle$, there exists some $0 \le i < n$ such that $ab^i \in H$. Then, since H is a subgroup, we must have $ab^i b^{km} \in H$, for all k. Thus $ab^{i+km} \in H$ and so $A(i, d) \subseteq H$ and therefore, by (9), we have $B(i, d) \subseteq H$. Thus, since $|H| = |B(i, d)| = 2d$, we must have $H = B(i, d)$. The converse obviously holds: given $d \mid n$ and $0 \le i < n$, $B(i, d)$ is a subgroup of D_{2n}, by Lemma 7, and $B(i, d) \nsubseteq \langle b \rangle$ because it contains $A(i, d)$. So the subgroups in this case are exactly the ones in the form $B(i, d)$, where $0 \le i < n$ and $d \mid n$. Thus, by Lemma 7, the number of subgroups in this case is

$$\sum_{d|n} |\{B(i, d) \mid \ 0 \le i < n\}| = \sum_{d|n} n/d = \sum_{d|n} d = \sigma(n).$$

So, by case 1 and case 2, the number of subgroups of D_{2n} is $\tau(n) + \sigma(n)$. □

Note that we did not just find the number of subgroups of D_{2n}. We also found all the subgroups.

Example 10. Let us find all subgroups of D_{12}.

By Theorem 8, there are $\tau(6) + \sigma(6) = 4 + 12 = 16$ subgroups. Four of them are obtained from case 1 in the proof of the theorem. They are the subgroups of $\langle b \rangle$. Since $\mathrm{ord}(b) = 6$, the subgroups in this case are $\{1\}, \langle b \rangle, \langle b^2 \rangle$ and $\langle b^3 \rangle$. There are 12 subgroups left and they are in the form $B(i, d)$, where $0 \le i < 6$ and $d \mid 6$. So $d = 1, 2, 3$ or 6. Also, by the proof of the last part of Lemma 7, $B(i, d) = B(j, d)$ if and only if $i \equiv j \mod 6/d$. So those 12 subgroups are:

$$B(0,1), B(1,1), B(2,1), B(3,1), B(4,1), B(5,1),$$
$$B(0,2), B(1,2), B(2,2), B(0,3), B(1,3), B(0,6).$$

Note that $B(0, 6) = D_{12}$.