From a group $G$ we can select two elements $a$ and $b$ and form the object

$$\langle a,b \rangle \equiv (ba)^{-1}(ab) = a^{-1}b^{-1}ab$$  \hfill (1)

The set of $\langle a,b \rangle$, together with their products, form an invariant subgroup of $G$ called a derived subgroup called $D$. It is possible for the derived subgroup to contain elements other than those formed by operation $\langle a,b \rangle$, since a product of two of these terms may not have the form $I$.

The inverse of $\langle a,b \rangle$ is found from

$$\langle a,b \rangle^{-1} = [a^{-1}b^{-1}ab]^{-1} = b^{-1}a^{-1}ba = \langle b,a \rangle$$  \hfill (2)

One other thing to note is that if $a$ and $b$ commute, then

$$\langle a,b \rangle = (ba)^{-1}(ab) = (ab)^{-1}(ab) = I$$  \hfill (3)

Thus an abelian group has only one derived subgroup, namely the identity $I$.

We can prove that $D$ is actually an invariant subgroup of $G$ as follows. An invariant subgroup $H$ satisfies the property that if $h \in H$, then $g^{-1}hg \in H$ for all $g \in G$. If $h = \langle a,b \rangle$ then

$$g^{-1} \langle a,b \rangle g = g^{-1}a^{-1}b^{-1}abg$$  \hfill (4)

$$= g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}ag^{-1}bg$$  \hfill (5)

$$= \langle g^{-1}ag,g^{-1}bg \rangle$$  \hfill (6)

where we used the fact that $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$ to get the third line. Thus if $\langle a,b \rangle \in H$, then $\langle g^{-1}ag,g^{-1}bg \rangle \in H$ for any element $g \in G$.

**Example 1.** We’ll find the derived subgroup of the dihedral group, which is the group of rotations and reflections about the medians of an $n$-sided polygon. Recall that this group is generated by a reflection operation $s$ with the property that $s^2 = I$ (since any reflection is its own inverse), and a rotation $r$ by an angle $\frac{2\pi}{n}$, so that $r^n = I$. We saw that the product of two rotations is another rotation, and the product of two reflections is also
a rotation. Since all rotations in 2-d commute, the terms $\langle r^i, r^j \rangle = I$ for all $i, j$. Thus we need to consider only terms such as $\langle sr^i, sr^j \rangle$, since these are the only terms that involve two reflections, or a reflection plus a rotation, and these terms in general do not commute. We have

$$
\langle sr^i, sr^j \rangle = (sr^i)\,^{-1} \, (sr^j)\,^{-1} \, sr^i \, sr^j
$$

(7)

$$
= r^{-i} \, s \, r^{-1} \, s^{-1} \, r \, s \, r^i \, sr^j
$$

(8)

We can now use the property of the dihedral group

$$
sr^i s = r^{-1}
$$

(9)

along with $s^{-1} = s$ to get

$$
\langle sr^i, sr^j \rangle = r^{-i} \, r^j \, r^{-i} \, r^j
$$

(10)

$$
= r^{2(j-i)}
$$

(11)

We can also look at $\langle sr^i, r^j s \rangle$ and we find

$$
\langle sr^i, r^j s \rangle = r^{-i} \, s \, r^{-j} \, s \, r^i \, r^j \, s
$$

(12)

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

(13)

$$
= r^{-2(i+j)}
$$

(14)

In both these formulas, $i$ and $j$ can range over $0, 1, \ldots, n-1$ and the exponent of $r$ in each case is taken mod $n$, since $r^n = I$. Thus the exponents in (11) and (14) actually give the same range of values. The results for the first few dihedral groups are in Table 1.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\mathcal{D}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>${ I, r, r^2 }$</td>
</tr>
<tr>
<td>4</td>
<td>${ I, r^2 }$</td>
</tr>
<tr>
<td>5</td>
<td>${ I, r, r^2, r^3, r^4 }$</td>
</tr>
<tr>
<td>6</td>
<td>${ I, r^2, r^4 }$</td>
</tr>
<tr>
<td>7</td>
<td>${ I, r, r^2, r^3, r^4, r^5, r^6 }$</td>
</tr>
</tbody>
</table>

**Table 1.** Derived subgroups for dihedral groups.
The derived subgroup for $n = 3$ is obtained by setting $j - i$ (or $i + j$) to 0 (giving $I$), 1 (giving $r^2$) or 2 (giving $r^4 = r$) where we’ve taken 4 mod 3 = 1.

For $n = 4$, we have $r^0 = I$, $r^2$, $r^4 = I$, so we have only two members in $D$.

For $n = 5$, we have $r^0 = I$, $r^2$, $r^4$, $r^6 = r$, $r^8 = r^3$, where again we’ve taken exponents larger than 4 to be mod 5. Similar calculations give the groups for $n = 6$ and $n = 7$.

In general, for even $n$, the factor of 2 in the exponent in 11 means that we will have only even powers of $r$ up to $r^n$, so only half the rotations in the dihedral group will appear in the derived group. For odd $n$, we again get all the even powers of $r$ up to $r^n-1$, but once $2(j - i) > n$, the mod $n$ will pick up the odd powers as well, so for odd $n$, the derived subgroup will have $n$ members.

A final note. We recall that $Z_n$ is the group consisting of the $n$th roots of 1 (in the complex plane). For odd $n$ the derived subgroup has the same structure as $Z_n$, in that if we take the $n$th power of any element of the group, we get $I$. For example, for $n = 5$, raise any of the elements in Table 1 to the 5th power and you will get $r^5 = I$ (once you’ve applied the mod 5 operator).

For even $n$, the derived subgroup is isomorphic to $Z_{n/2}$. For example, for $n = 6$, raise any of the group elements to the 3rd power and you will get $r^6 = I$ (again mod 6).