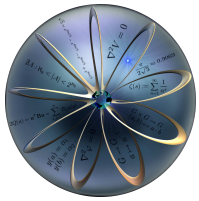

planetmath.org

Math for the people, by the people.

dihedral group properties

Canonical name	DihedralGroupProperties
Date of creation	2013-03-22 16:06:35
Last modified on	2013-03-22 16:06:35
Owner	Algeboy (12884)
Last modified by	Algeboy (12884)
Numerical id	10
Author	Algeboy (12884)
Entry type	Topic
Classification	msc 20F55
Related topic	GeneralizedQuaternionGroup

1 Properties of Dihedral Groups

A group generated by two involutions is a dihedral group. When the group is finite it is possible to show that the group has order $2n$ for some $n > 0$ and takes the presentation

$$D_{2n} = \langle a, b \mid a^n = 1, b^2 = 1, a^b = a^{-1} \rangle.$$

Remark 1. *Contemporary group theorists prefer D_{2n} over D_n as the notation for the dihedral group of order $2n$. Although this notation is overly explicit, it does help to resolve the ambiguity with the Lie type D_l which corresponds to the orthogonal group $\Omega^+(2l, q)$. However, introductory texts in algebra still make use of the more appropriate D_n notation to emphasize the connection to the symmetries of a regular n-gon (n-sided polygon).*

$D_2 \cong \mathbb{Z}_2$, $D_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ are the two abelian examples of dihedral groups. They can be considered as dihedral groups of the respective order because they satisfy the relations, though the geometric interpretations are slightly modified. Often D_2 can be termed the symmetries of a line segment, and the D_4 the symmetries of a non-square rectangle, as the symmetry groups of each of these object is isomorphic to D_2 and D_4 respectively. These exceptions cause problems for most theorems on dihedral groups so it is convenient to insist that $n > 2$ for theorems.

Proposition 2.

$$D_{2n} = \{a^i \mid i \in \mathbb{Z}_n\} \sqcup \{a^i b \mid i \in \mathbb{Z}_n\}$$

is a irredundant list of the elements of D_{2n}. Moreover the conjugacy classes of D_{2n} are $\{a^i, a^{-i}\}$ for all $i \in \mathbb{Z}_n$ and

- *$2|n$, $\{a^{2i}b \mid i \in \mathbb{Z}_n\}$ and $\{a^{2i+1}b \mid i \in \mathbb{Z}_n\}$*
- *$2 \nmid n$, $\{a^i b \mid i \in \mathbb{Z}_n\}$.*

Consequently when $n > 2$ the center of D_{2n} is 1 when $2 \nmid n$ and $Z(D_{2n}) = \langle a^{n/2} \rangle$ when $2|n$. Furthermore $C_n := \langle a \rangle$ is a characteristic subgroup of D_{2n}, provided $n \neq 2$.

Proof. The conjugation relation $a^b = a^{-1}$ allows us to place every element in the normal form $a^i b^j$. If $a^i b^j = a^k b^l$ then $a^{i-k} = b^{l-j}$. Yet $\langle a \rangle \cap \langle b \rangle = 1$ so

$i - k \equiv 0 \pmod{n}$ and $l - j \equiv 0 \pmod{2}$. Thus we have and irredundant list as required.

For the conjugacy classes note that $(a^i)^{a^j b} = (a^i)^b = a^{-i}$ so that these conjugacy classes are established. Next

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

for all $i \in \mathbb{Z}$. When $2 \nmid n$ we have $(2, n) = 1$ so 2 is invertible modulo n. We let $j = 2^{-1}(k - i)$ for any $k \in \mathbb{Z}$ and we see that $a^i b$ is conjugate to any $a^k b$. However, when $2|n$ we have a parity constraint that so far creates the two classes. We need to also verify conjugation by $a^j b$ does not fuse the two classes. Indeed

$$(a^i b)^{a^j b} = (a^{-2j+i} b)^b = b a^{-2j+i} b = a^{2j-i} b,$$

thus we retain two conjugacy classes amongst the reflections.

Finally, the order of the elements $(a^i b)$ is 2 – a fact used already. Thus the only cyclic subgroup of order n, when $n > 2$, is C_n and thus by its uniqueness it is characteristic. □

Proposition 3. *The maximal subgroups of D_{2n} are dihedral or cyclic. In particular, the unique maximal cyclic group is $C_n = \langle a \rangle$ and the maximal dihedral groups are those of the form $\langle a^{n/p}, a^i b \rangle$ for primes p dividing n.*

We will prove this with a more general claim. First we pause to note that as a corollary to these two propositions we can determine the entire lattice of normal and characteristic subgroups of a dihedral group.

Corollary 4. *A proper subgroup H of D_{2n} is normal in D_{2n} if and only if $H \leq \langle a \rangle$ or $2|n$, and H is one the following two maximal subgroups of index 2:*

$$M_1 = \langle a^2, b \rangle, \qquad M_2 = \langle a^2, ab \rangle.$$

The proper characteristic subgroups of D_{2n} are all the subgroups of $\langle a \rangle$.

Proof. If H is normal and contains an element of the form $a^i b$, then it contains the entire conjugacy class of $a^i b$. If n is odd then all reflections are conjugate to $a^i b$ so H contains all reflections of D_{2n} and so H is D_{2n} as the relfections generate D_{2n}.

If instead n is even then H is forced only to contain one of the two conjugacy classes of reflections. If i is even then H contains b and $a^2 b$ so it

contains a^2. If i is odd then H contains ab and a^3b so it contains $a^2 = aba^3b$ (note $n > 3$ as $n > 2$ and $2|n$).

The two maximal subgroups of index 2 which can exist when n is even can be interchanged by an outer automorphism which maps $a \mapsto a^{-1}$ and $b \mapsto ab$ so these two are not characterisitic. The subgroups of a characterisitic cyclic group are necessarily characteristic. □

Proposition 5. *Quotient groups of dihedral groups are dihedral, and subgroups of dihedral groups are dihedral or cyclic.*

Proof. The homomorphic image of a dihedral group has two generators $\hat{a}$ and $\hat{b}$ which satisfy the conditions $\hat{a}^{\hat{b}} = \hat{a}^{-1}$ and $\hat{a}^n = 1$ and $\hat{b}^2 = 1$, therefore the image is a dihedral group.

For subgroups we proceed by induction. When $n = 1$ the result is clear. Now suppose that D_{2n} has some proper subgroup H that is not dihedral or cyclic. H is contained in some maximal subgroup M of D_{2n}. However the maximal subgroups of D_{2n} are cyclic or dihedral so H falls to the induction step for M – together with the fact that subgroups of cyclic groups are cyclic. Thus H must actually be dihedral or cyclic to avoid contradictions. □

Proposition 6. *D_n is nilpotent if and only if $n = 2^i$ for some $i \geq 0$.*

Proposition 7. *D_{2n} is solvable for all $n \geq 1$.*

Proof. When $n = 1$, $D_{2n} \cong \mathbb{Z}_2$ which is nilpotent and so also solvable. Now let $n > 1$. Then $D_{2n}/\langle a \rangle \cong \mathbb{Z}_2$ and $\langle a \rangle \cong \mathbb{Z}_n$. Both $\mathbb{Z}_n$ and $\mathbb{Z}_2$ are nilpotent and so they are both solvable. As extensions of solvable groups are solvable, D_{2n} is solvable for all $n > 0$. □

1.1 Automorphisms of D_{2n}

Theorem 8. *Let $n > 2$. The automorphism group of D_{2n} is isomorphic to $\mathbb{Z}_n^\times \ltimes \mathbb{Z}_n$, with the canonical action of $1 : \mathbb{Z}_n^\times \to \operatorname{Aut} \mathbb{Z}_n = \mathbb{Z}_n^\times$. Explicitly,*

$$\operatorname{Aut} D_{2n} = \{\gamma_{s,t} \mid s \in \mathbb{Z}_n^\times, t \in \mathbb{Z}_n\}$$

with $\gamma_{s,t}$ defined as

$$(a^i)\gamma_{s,t} = \alpha^{is}, \qquad (a^i b)\gamma_{s,t} = a^{is+t}b.$$

Proof. We apply the needle-in-the-haystack heuristic and search first to explain why these are the only possible forms for the automorphisms. We will then prove all such are indeed automorphisms.

Given $\gamma \in \operatorname{Aut} D_{2n}$, we know $\langle a \rangle$ is characteristic in D_{2n} so $a\gamma = a^s$ for some $s \in \mathbb{Z}_n$. But γ is invertible so indeed $(s, n) = 1$ so that $s \in \mathbb{Z}_n^\times$. Next $b\gamma = a^t b$ as b cannot be sent to $\langle a \rangle$.

Now we claim $\gamma = \gamma_{s,t}$.

$$(a^i)\gamma = a^{is} = (a^i)\gamma_{s,t}$$

and

$$(a^i b)\gamma = a^{is}a^t b = a^{is+t}b = (a^i b)\gamma_{s,t}.$$

Now we must show all $\gamma_{s,t}$ are indeed homomorphisms when $s \in \mathbb{Z}_n^\times$ and $t \in \mathbb{Z}_n$. First we note that γ is well-defined as we have an irredundant listing of the elements. Next we verify the homomorphism cases.

$$\begin{aligned}
(a^i a^j)\gamma_{s,t} &= a^{(i+j)s} = a^{is}a^{js} = (a^i)\gamma_{s,t}(a^j)\gamma_{s,t}.\\
(a^i a^j b)\gamma_{s,t} &= a^{(i+j)s+t}b = a^{is}(a^{js+t}b) = (a^i)\gamma_{s,t}(a^i b)\gamma_{s,t}.\\
(a^i b a^j)\gamma_{s,t} &= (a^{i-j}b)\gamma_{s,t} = a^{(i-j)s+t}b = a^{is+t}ba^{js} = (a^i b)\gamma_{s,t}(a^j)\gamma_{s,t}.\\
(a^i b a^j b)\gamma_{s,t} &= (a^{i-j})\gamma_{s,t} = a^{is-js} = a^{is+t-t-is}\\
&= (a^{is+t}b)(ba^{-t-is}) = (a^{is+t}b)(a^{js+t}b) = (a^i b)\gamma_{s,t}(a^j b)\gamma_{s,t}.
\end{aligned}$$

So indeed $\gamma_{s,t}$ is a homomorphism.

Finally, we show the composition of two such maps both to identify the automorphism group and to show that each $\gamma_{s,t}$ is invertible.

$$(a^i b)\gamma_{s,t}\gamma_{u,v} = (a^{is+t}b)\gamma_{u,v} = a^{isu+tu+v}b.$$

Hence, $\gamma_{s,t}\gamma_{u,v} = \gamma_{su,tu+v}$. This agrees on a^i's as well. This reveals the isomorphism desired: $\operatorname{Aut} D_{2n} \to \mathbb{Z}_n^\times \ltimes \mathbb{Z}_n$ by $\gamma_{s,t} \mapsto (s, t)$ where we see the multiplications agree as

$$(s, t)(u, v) = (su, tu + v).$$

In fact this demonstrates that the inverse of $\gamma_{s,t}$ is simply $\gamma_{s^{-1},-ts^-}$ and the identity map is $\gamma_{1,0}$. □