Dihedral Groups

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Dihedral groups are the group of symmetries of regular n-sided polygons. The reader should study the cases when $n = 3, 4$ while we look at the general case of n-gon.

We orient the regular n-gons as in Figure 1 (the left column picture) by locating a vertex at the top, labeled as 1. We number the positions of the other vertices in clockwise order. It is intuitively obvious that a symmetry σ is completely determined (1) by the position of the image, $\sigma(1)$, of the vertex at 1 under the symmetry σ, and (2) by the position of the image, $\sigma(2)$, of the vertex at 2 relative to $\sigma(1)$—whether it is clockwise or anti-clockwise of $\sigma(1)$. There are n choices for the vertex at 1 and for each such choice, there are are two choices for the image of the vertex at 2. Thus there are $2n$ symmetries of the regular n-gon.

Let R denote the clockwise rotation by $2\pi/n$ radians. Let ρ denote the reflection about the vertical diameter through the vertex at 1. See Figures 1–2.

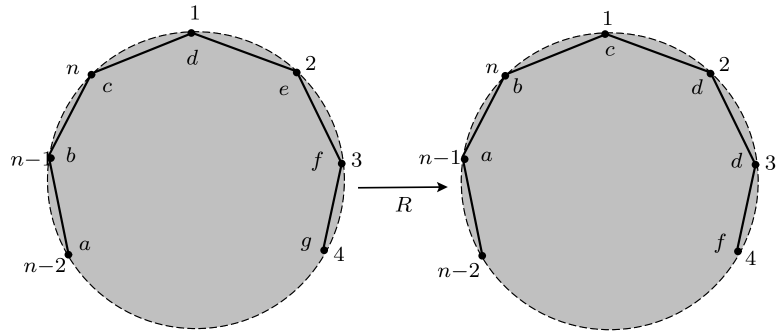


Figure 1: Rotation

The following are the consequences of our (intuitively obvious) observation: Any symmetry can be obtained by

(1) A rotation of $2\pi k/n$ radians. The corresponding group element is R^k for $0 \leq k < n$.

(2) A reflection or no reflection about the vertical diameter. The corresponding group element is ρ^l where $l = 0$ or $l = 1$.

Some typical situations are shown in Figures 1–2. (Keep in mind that the integers 1,2,3 etc., denote the positions of the vertices, not the vertices themselves.) If we denote the

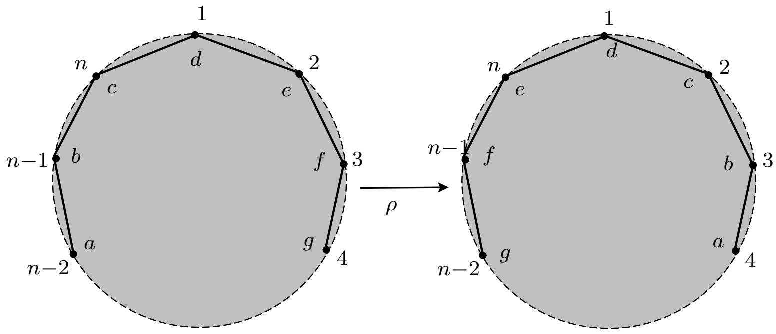


Figure 2: Reflection

identity symmetry by I, we have the relations

$$R^n = I = \rho^2 \text{ and } R\rho = \rho R^{-1} = \rho R^{n-1}. \tag{1}$$

The last relation is visualized in Figure 4. See also Observation 1

We now make three observations.

Observation 1. The symmetries R and ρ induce permutations of the integers $1, 2, \ldots, n$ in terms of the positions assumed by the vertices. Thus R and ρ are represented by the permutations

$$R = \begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix} \text{ and } \rho = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & n & (n-1) & \ldots & 2 \end{pmatrix}. \tag{2}$$

Thus, we have $\rho(j) = n + 2 - j$ if $j \neq 1$ and $\rho(1) = 1$. Using this, it is easy to see that $R\rho = \rho R^{-1}$. (Exercise!)

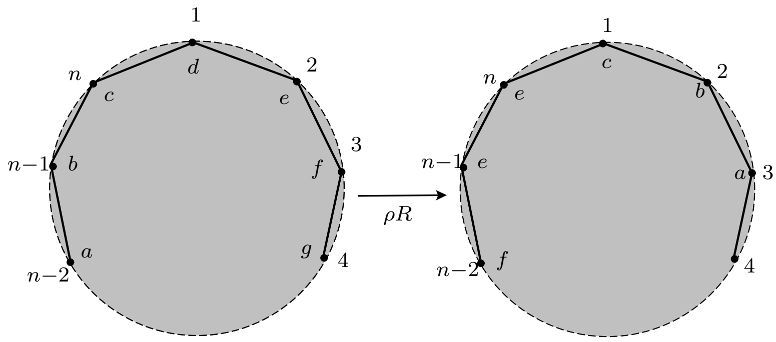


Figure 3: Rotation followed by reflection

Observation 2. From the relation $R\rho = \rho R^{-1}$ we have

$$R^k\rho = \rho R^{-k}, \text{ for } 0 \le k < n. \tag{3}$$

This is seen as follows:

$$R^k\rho = \underbrace{R\cdots R}_{k}\rho = (\underbrace{R\cdots R}_{k-1})(R\rho) = \underbrace{R\cdots R}_{k-1}\rho R^{-1} = \cdots = \rho R^{-k}.$$

Observation 3. Each element of the group is of the form $R^k\rho^l$ where $0 \le k < n$ and $l = 0, 1$. Thus there are $2n$ elements of this form and we must prove that they are all distinct. If $R^k\rho^l = R^r\rho^s$, then we should have $R^{k-r} = \rho^{l-s}$. In geometric language this means that the rotation R^{k-r} must be a reflection ρ^{l-s}. This is impossible, for example, the rotation will have determinant 1 whereas a reflection will have determinant -1.

While this is perfectly a valid argument, we shall prove this purely algebraically using only the relations (1).

Theorem 4. *Let G be a group. Assume that there exist $r, a \in G$ such that, for some fixed integer $n > 2$*

1. *$r^n = 1 = a^2$ and $r^k \neq 1$ if $0 < k < n$, and $a \neq 1$.*
2. *$ra = ar^{-1}$.*

Then G contains at least $2n$ elements of the form $r^k a^l$ where $0 \le k < n$ and $l = 0, 1$. The group multiplication for these elements is given by

$$(r^k a^l)(r^i a^j) = \begin{cases} r^{k+i}a^j, & \text{if } l = 0 \\ r^{k-i}a^{l+j}, & \text{if } l = 1. \end{cases} \tag{4}$$

Proof. As shown in Observation 2, we have

$$r^k a = ar^{-k} \text{ (or equivalently } r^{-k}a = ar^k). \tag{5}$$

The relations in (5) are sufficient to prove those in (4).

The relation (4) is trivial when $l = 0$. If $l = 1$, then

$$(r^k a^l)(r^i a^j) = r^k(a^l r^i)a^j = r^k(r^{-i}a^l)a^j = r^{k-i}a^{l+j}.$$

Relation (4) shows that the set $\{r^k a^l : 0 \le k < n, l = 0, 1\}$ is closed under multiplication and contains the identity $1 = r^0 a^0$. Since this is a finite set, it is a subgroup of G.

Thus to complete the proof, we need only show that the $2n$ elements $r^k a^l$ of the set are all distinct. Suppose that $r^k a^l = r^i a^j$. We first show that this implies that $r^{k-i} = 1$ and that $a^{l-j} = 1$. Multiplying the equation on the left by r^{-i} and on the right by a^{-j}, we obtain

$$r^{k-i}a^{l-j} = 1.$$

To simplify the notation, let $c = k - i$ and $d = l - j$. We therefore want to show that $r^c a^d = 1$ implies that $r^c = 1$ and $a^d = 1$. If $d = 0$,we are done. If $d = \pm 1$, then, since $a^2 = 1$, $a^d = a$ and hence $r^c a^d = 1$ is the same as saying that $r^c a = 1$ or equivalently $r^c = a$. But then $ra = rr^c = r^c r = ar$. By hypothesis, $ra = ar^{-1}$. Hence we conclude that $r = r^{-1}$ or $r^2 = 1$. This contradicts our hypothesis (1). Thus we infer that $d = 0$.

Finally, if $r^c = 1$ for $0 \le c < n$, then $c = 0$, in view of the hypothesis (1). Therefore we conclude that all elements of the form $r^k a^l$ ($0 \le k < n$, $l = 0, 1$) are distinct. □

Corollary 5. *For every integer $n > 2$, there is a group of order $2n$ with properties 1 and 2 of the theorem. This group is unique up to isomorphism and will be denoted by D_{2n}.*

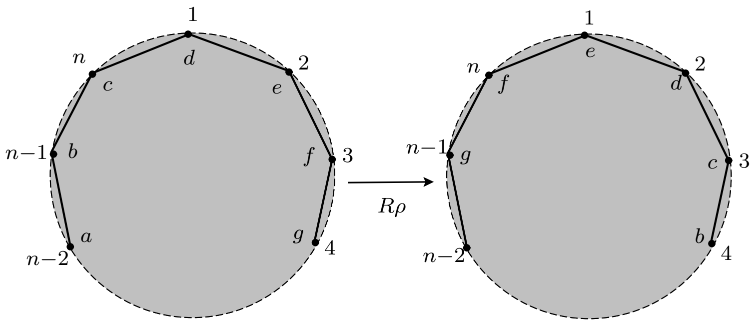
Proof. The existence is given by the groups of symmetries of a regular n-gon. The uniqueness is what Theorem 4 is about. □

Example 6. Consider D_8. Let the generators by r, s with $r^4 = 1 = s^2$ and $rs = sr^{-1}$ as the relations. The elements $s, b := sr$ are of order 2. Also, the subgroup $< s, sr >$ generated by them is D_8, since $r = sb \in < s, sr >$. However, not all elements can be written in the form $s^i b^j$. For there are only four such distinct elements whereas $|D_8| = 8$. In particular, the element sbs cannot be brought into the form $s^i b^j$.

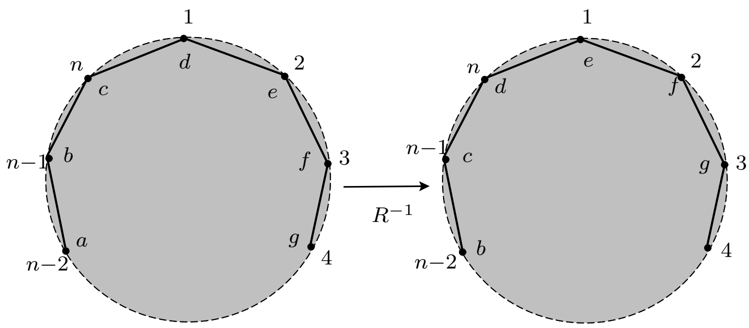
Ex. 7. Let G_n be the subgroup of $GL(2, \mathbb{C})$ generated by the elements

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } B := \begin{pmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{pmatrix}.$$

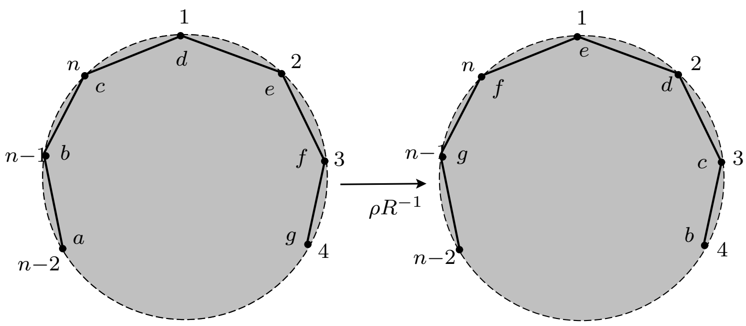
Show that $G_n$is isomorphic to D_{2n}.



Reflection followed by rotation



The inverse of rotation



Inverse of rotation followed by reflection

Figure 4: Some Elements of Dihedral Group