Section 1.2: Dihedral Groups

Juan Patricio Carrizales Torres

Feb 13, 2023

One group is known as a Dihedral Group. It's origin can be traced to the study of the symmetries of geometric entities known as n-gons. Hand-wavy explained, a symmetry is a rigid motion of all points in the n-gon such that the resulting copy can be placed over the original one, namely, points of some "nature" lay on top of points of the same nature. Then, the Dihedral group, also represented by D_{2n}, is the set of symmetries of the n-gon. Clearly, we must first represent them by appropiate mathematical objects. Thus, symmetries can be defined as functions $f : V \to V$, where V is the set of vertices of the $n - gon$. This has to do with the fact that the position of the vertices determine the position of all points (particularly, due to the "symmetric" shape of n-gons, one must only know the distance from two points to characterize all points on the n-gon [for an elaborated argument about this fact check "Dihedral Groups" by Keith Conrad]). Thus, the identity e function leaves vertices intact, the inverse of the symmetry "reverses" the rigid motion (brings vertices to the position they were at before the application of the symmetry), and the permutations are defined by the operation of composition of functions, which is associative.

For n-gons, two basic symmetries are the $2\pi/n$ rotation r applied to vertex some vertex labelled as 1 and the reflection s about the line of symmetry of 1 and the center of the n-gon. This is not enough to show that they are the only ones, there could be more. However, one can show the limit $|D_{2n}| \leq 2n$ and construct $2n$ symmetries by permutations of s and r.

To construct the $2n$ symmetries, We show the following useful properties of the Dihedral Group:

(a) $r^n \neq r^m$ such that $n \neq m$ and $n, m \in \{0, 1, \ldots, n-1\}$.

Proof. Consider the vertex labeled by 1, which is at some position $i \in \{1, \ldots, n\}$. Note that r maps vertex 1 from position $\bar{i}$ to position $\overline{i+1}$ and $r^0 = e$ (we use the n residue classes to account the cyclic nature of the permutation of symmetries on n-gons, where each vertex can be represented by the class and labeled by the representative number of that class). Thus, $r(r) : \overline{i+1} \to \overline{i+2}$ and so, by induction, $r^m : \bar{i} \to \overline{i+m}$ for $m \in \{0, \ldots, n-1\}$. Clearly, if $m, k < n$ and $m \neq k$, then $\bar{m} \neq \bar{k}$ and so $r^m \neq r^k$. Furthermore, $r^n : \bar{i} \to \overline{i+n} = e : \bar{i} \to \bar{i}$. Therefore, $|r| = n$. □

(b) $|s| = 2$

Proof. We know that $s : \overline{1+i} \to \overline{1-i}$ for all $0 \leq i \leq n-1$ and $s^0 = e$. Note that $\overline{1-1} = \overline{0} = \overline{1+(n-1)}$ and so $s(s) : \overline{1+(n-1)} \to \overline{-n+2}$. Because $\overline{-n+2} = \overline{2}$, it follows that s^2 brings the point initially at vertex $\overline{2}$ back to $\overline{2}$. Furthermore, by definition, the vertex at position $\overline{1}$ remains intact. Thus, since the position of two adjacent vertices determines the position of the other points on the n-gon, $s^2 = e$. □

(c) $s \neq r^i$ for any nonnegative integer i.

Proof. We know that s mantain one point ate vertex $\overline{1}$ and moves the position of the point at vertex $\overline{i+1}$. Also, any permutation of r either changes the position of all points or keeps them intact r^e. Therefore, $s \neq r^i$ for any nonnegative i. □

(d) $sr^i \neq sr^i$ for $0 \leq i \neq j < n$.

Proof. Since $\overline{i} \neq \overline{j}$ for $0 \leq i, j < n$, it follows that $r^i \neq r^j$. Therefore, they have at least on vertex with different points and so $sr^i \neq sr^j$. □

(e) $rs = r^{-1}s$

Proof. Note that s moves points 1 and 2 to vertices $\overline{1}$ and $\overline{n}$, respectively. Then rs moves points 1 and 2 to vertices $\overline{2}$ and $\overline{1}$, respectively.

Now, r^{-1} brings point 1 and 2 to vertices $\overline{n}$ and $\overline{1}$, respectively. Then, sr^{-1} moves points 1 and 2 to vertices $\overline{2}$ and $\overline{1}$.

Thus, $rs = sr^{-1}$. □

(f) $r^i s = sr^{-i}$ for any i.

Proof. It suffices to show that $r^i s = s^{-i}$ for any nonegative integer i.Clearly, $r^0 s = sr^{-0} = s$. Now, we proceed by induction. We know that $rs = sr^{-1}$. Now, assume that $r^k s = sr^{-k}$ for any $1 \leq k$. Then,

$$\begin{aligned} r^{k+1}s &= r(r^k s) = r(sr^{-k}) \\ &= (rs)r^{-k} = sr^{-1}r^{-k} = sr^{-(k+1)}. \end{aligned}$$

□

Note that (6) is a relation that (6) is a commutative relation, which show a way to move powers of an element of a binary operation to the opposite side. Furthermore, any permutation can be reduced to $s^k r^i$, where $k \in \{0, 1\}$ and $i \in \{0, \ldots, n-1\}$, with relations (1), (2) and (6).

Furthermore, there are two important concepts. A **generator** is any set $S \subset G$ of some group G, such that every element in G can be expressed as a finite product of elements and their inverses of S. This set comes with **Relations** between its elements, there can be many, however, the idea is to look for the lowest quantity of relations to reduce any product of G to a finite product of the elements and their inverses in S. Thus, any group can have a representation

$$G =< S|R_1, R_2, \ldots, R_n > .$$

Its important to note that the choice of representation for a group is important, because, depending on the relations chosen, they can be interwined in such a way that a lot of collapsing occurs. BY collapsing, I believe, the authour means that at first it gives an impression of a limit of elements in the group just to end up realizing that a lot of them can be reduced, lowering the limit.

In the following excercises, D_{2n} has the usual presentation $D_{2n} =< r, s|r^n = s^2 = 1, rs = sr^{-1} >$.

Problem 2. Use the generators and relations above to show that if x is any element of D_{2n}, which is not a power of r, then $rx = xr^{-1}$.

Proof. If x is not a power of r, then $x = sr^k$ for some $k \in \mathbb{Z}$. Then,

$$\begin{aligned} rx &= r\left(sr^k\right) = (rs)\, r^k \\ &= sr^{-1}r^k = sr^{k-1} = sr^k r^{-1} = xr^{-1}. \end{aligned}$$

□

Problem 3. Every element of D_{2n}, which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both having order 2.

Proof. First, we show that every element of D_{2n} that is not a power of r has order 2. Any such element can be reduced to the general expression $sr^k \neq e$ for $k \in \{0, 1, \ldots, n-1\}$. Then,

$$\begin{aligned} (sr^k)^2 &= (sr^k)(sr^k) = (sr^k)(r^{-k}s) \\ &= s(r^k r^{-k})s = s^2 = e. \end{aligned}$$

Now, we proove that every element of D_{2n} can be expressed as a finite product of the elements s and sr, including their inverses. First, consider any product of r. Then,

$$r^k = (s \cdot sr)^k$$

and so

$$sr^k = s(s \cdot sr)^k.$$

Using (4) one can conclude that all elements of D_{2n} can be reduced to powers of r and these multiplied by s. Thus, $S = \{s, sr\}$ generates D_{2n}. □

Problem 4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.

Proof. First we show the following Lemma,

Lemma C. onsidering elements of D_{2n}, any nonidentity power of r^k $(1 \leq k \leq n-1)$ commutes with some nonpower of r if and only if $r^k = r^{-k}$.

Proof. If $r^k = r^{-k}$, it follows that $|r^k| = 2$. Furthermore, every nonpower of r has order 2 and so any nonpower of r commutes with r^k.
For the converse, assume that r^k $(1 \leq k \leq n-1)$ commutes with any nonpower of r. Then, for any $0 \leq i \leq n-1$,

$$\begin{aligned} r^k(sr^i) = (sr^i)r^k \implies sr^{-k}r^i = (sr^i)r^k \implies \\ sr^{i-k} = sr^{i+k} \implies r^{-k}r^i = r^k r^i \implies r^{-k} = r^k. \end{aligned}$$

□

By the relations of the D_{2n} group, we know that $|r| = n = 2k$. Then, $|r^k| = 2$ and so it is the only nonidentity power of r with order 2 (Recall the bijection from $\mathbb{N}$ to the even integers). Then, it is the only nonidentity power of r that is equal to its inverse. Thus, by Lemma, r^k is the only nonidentity power of r such that every nonpower of r commutes with. Therefore, r^k is the only nonidentity element that commutes with all elements. □

Problem 5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

Proof. Since n is odd, it follows that $2 \mid n$ and so there is no nonidentity power of r such that its order is 2. Thus, by Lemma, every nonidentity power of r does not commute with every nonpower of r. Therefore, the identity is the only element in this D_{2n} which commutes with all elements. □

Problem 6. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$. (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Proof. Let x and y be elements of order 2. Thus,

$$\begin{aligned} tx &= (xy)x = x(yx) \\ &= xy^{-1}x^{-1} = x(xy)^{-1} = xt^{-1} = xt. \end{aligned}$$

□

Problem 7. Show that $\langle a, b | a^2 = b^2 = (ab)^n = 1 \rangle$ gives a representation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Excercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]

Proof. Clearly, $a^2 = s^2 = 1 \iff |s| = 2$ and $(ab)^n = (ssr)^n = 1 \iff |r| = n$. Now, $b^2 = 1 \implies sr = (sr)^{-1} = r^{-1}s^{-1} = r^{-1}s$ and $sr = r^{-1}s = (sr)^{-1} \implies |sr| = 2$. □

Problem 8. Find the order of the cyclic subgroup of D_{2n} generated by r.

Proof. We know that for some x such that $|x| = k$, $H = \{x^n : n \in \mathbb{Z}\}$ is a cyclic group of order k. Then, $G_c = \{r^n : n \in \mathbb{Z}\}$ is a cyclic group of order n since $|r| = n$. Thanks to the relation $|r| = n$, the multiplicities and inverses of r can be reduced to n distinct elements. □

1 Permutations

Symmetric group on a set Ω.

(a) S_Ω set of all functions $\sigma : \Omega \to \Omega$.

(b) The binary operation $\circ$ on S_Ω is the associative function composition.

(c) $i(a) = a$ is the identity function.

(d) If $\sigma \in S_\Omega$, then the inverse function $\sigma^{-1} \in S_\Omega$ and so $\sigma \circ \sigma^{-1} = i$.

Every element of S_Ω is a permutation of σ. A permutation $\sigma$of a finite set Ω, is an injective function $\sigma : \Omega \to \Omega$.

(a) S_n is the symmetric group of $\Omega = \{1, 2, \ldots, n\}$ of degree n. Clearly, $|S_n| = n!$.

(b) Each element of S_n can be represented as a cycle decomposition of k cycles. A cycle is a string of integers $(a_1, a_2, \ldots, a_m)$ that represents the permutation that sends a_i to a_{i+1} for all $1 \leq i < m$ and $a_m \to a_1$.

(c) Cycle decomposition is the unique way to express a symmetric group of degree n as an arrengement of disjoint cycles.

Problem a. Show that the order of a permutation represented by a single cycle σ of n integers is n.

Proof. Each position in the string (cycle) can be represented by the residue class $\overline{i}$. Hence, the permutation "transforms" integer at $\overline{i}$ to the integer at position $\overline{i+1}$. It's easy to show that σ^m transforms integers at $\overline{i}$ into the integers at $\overline{i+m}$ (i.e. by induction). Since $\overline{i}$ are residue classes, it follows that $\overline{i+cn} = \overline{i}$ if and only if $c \in \mathbb{Z}$. Therefore, the smallest nonzero nonnegative multiple of n is itself, and so $|\sigma| = n$. Note that this proof considers any cycle represented by a string of n positions with any elements. □

Problem b. Prove that the order of any cyclic decomposition σ is the lowest common multiple of the orders of its disjoint cycles.

Proof. Note that a cyclic decomposition of one cycle one permutes the integers in this cycle while leaving the others alone. Hence, a function f with cyclic decomposition $\sigma_1\sigma_2\ldots\sigma_k$ can be expressed as the product of the separate cycles, namely, $\sigma_1\sigma_2\ldots\sigma_k = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$. Furthermore, the order of the factors does not matter since the product of disjoint cycles is commutative. Therefore, assuming that p is the lowest common multiple of the orders of each cycle,

$$\begin{aligned}(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k)^p &= \sigma_1^{|\sigma_1|c_1} \circ \cdots \circ \sigma_k^{|\sigma_k|c_2},\ c_1, c_2 \in \mathbb{N} \\ &= \left(\sigma_1^{|\sigma_1|}\right)^{c_1} \circ \cdots \circ \left(\sigma_k^{|\sigma_k|}\right)^{c_2} \\ &= 1.\end{aligned}$$

Hence, $|\sigma_1\ldots\sigma_k| \leq p$. Clearly, the previous integer is the lowest common multiple and so any nonzero positive integer lower than it is not a common multiple of the orders of the cycles. Hence, this lower integer k would not be a multiple of at least one $|\sigma_m|$ and so $\sigma_m^k \neq 1$. Therefore, the order of the permutation f is p. □

Problem c. Let σ be a cycle of n positions and k be a positive integer, σ^k can be represented by a single cycle of n positions if and only if k is relative prime to n

Proof. A characteristic that distinguishes a cycle with n positions from other smaller or bigger cycles, is that its order of permutation is n (As we showed in **Problem a**). Furthermore, any σ^k can be reduced to σ^m for some integer $0 \leq m < n$.
Suppose that $n > k \geq 0$ is relative prime to n. Then, the greatest common factor of n and k is 1. Thus, n is the smallest integer such that kn is a multiple of n and so the order of permutation of σ^k is n $\left(\left(\sigma^k\right)^c = \sigma^{c\cdot k} = i(a)\right)$. Thus σ^k can be represented by a single cycle of n positions.
For the converse, assume that σ^k can be represented by a single cycle of n positions. Then, its permutation order is n, which means that n is the smallest nonzero positive integer such that $k \cdot n > n$ is a multiple of n. Therefore, k is relative prime to n. □

Corollary a1. Let σ be a cycle with a prime n number of positions. For any positive integer k that is not a multiple of n, σ^k can be respresented as a cycle of n positions.

Proof. Since n is prime, it follows that any integer not multiple of n is relative prime to n. □

2 Excercises

Problem 12. (a) If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is a n-cycle $\sigma(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

Solution Yep, there is. Consider the 10-cycle $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10)$. Then, $\sigma^5 = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$. It seems that if k is not relative prime to n, then σ^k has a cycle decomposition of $m = \text{gcf}(k, n)$ disjoint cycles each with r elements, where $n = m \cdot r$.

(b) If $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n-cycle $\sigma (n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

Solution There is no such cycle. (I will prove that for any n-cycle σ, σ^k has a cycle decomposition of disjoint cycles of same length).

Lemma A. Consider some n-cycle σ. σ^k can be represented by a cycle decomposition of $m = \text{gcf}(k, n)$ disjoint cycles each with r elements, where $n = m \cdot r$.

Proof. Consider some n-cycle σ and let $m = \text{gcf}(k, n)$, where $k \in \mathbb{N}$. Then, $k = mb$ and $n = mr$ for some $b, r \in \mathbb{N}$. Thus, r is the lowest integer such that $n | r \cdot k$. Now consider the elements at the first m positions. We show that they lie in different r-cycles in the cycle decomposition of σ^k.
First, we show for any $0 \leq i, j < m$ that if $i \neq j$, then $\overline{i + c_1 k} \neq \overline{j + c_2 k}$, where c_1, c_2 are nonnegative integers. Observe that $\overline{i + c_1 k} = \overline{i + c_1 mb}$ and $\overline{j + c_2 k} = \overline{j + c_2 bm}$. Because $i \neq j$ and $0 \leq i, j < m$, it follows that $i + c_1 mb$ and $j + c_2 mb$ are not congruent modulo m. This implies that $m \nmid |(i + c_1 mb) - (j + c_2 mb)|$ and so $rm \nmid |(i + c_1 mb) - (j + c_2 mb)|$. Therefore, $\overline{i + c_1 k} \neq \overline{j + c_2 k}$ for any nonegative integers c_1, c_2.
This means that the elements at the first m positions lie at disjoint cycles in the cycle decomposition of σ^k. Furthermore, at each disjoint cycle, σ^k brings the element at position $\bar{i}$ to its initial position after r iterations. Hence, each cycle has an order of r. Hence, σ^k has a cycle decomposition of m disjoint cycles of length r, which gives a total of $r \cdot m = n$ positions. □