MAT301H5Y

Week 4 Lecture 1: Dihedral groups and permutation groups

Thursday May 30th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Overview

In today's class we covered two new types of groups. Namely, Dihedral groups and symmetry permutation groups.

Dihedral groups

Before understanding what is a dihedral group, let us define P_n.

Definition: P_n polygon shape

P_n is defined as an n-sided regular polygon(usually defined for $n > 2$). A couple examples are as below:

- $n = 3 \ <-> \ P_3$: Equilateral triangle
- $n = 4 \ <-> \ P_4$: Square

Another pre-requisite or "recap" from linear algebra are isometries which will be useful in defining a dihedral group.

Recap: Linear transformations /isometries and orthogonal matrices

A linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is a transformation that "respects" linearity, specifically:

- $T(\vec{a} + \vec{b}) = T(\vec{a}) + T(\vec{b})$ for any $\vec{a}, \vec{b} \in \mathbb{R}^n$.
- $T(k\vec{v}) = kT(\vec{v})$ for any $k \in \mathbb{R}$ and $\vec{v} \in \mathbb{R}^n$.

Remark: Linear transformations can be between any two vectors spaces. We sometimes denote linear transformation $T : V \to W$ as $T \in L(V, W)$

A linear isometry $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation that preserves norm after transformation of a vector from $\mathbb{R}^n$. In specific $\|T(\vec{x})\| = \|\vec{x}\|$ for all $\vec{x} \in \mathbb{R}^n$.

Since linear transformation in $\mathbb{R}^n$ have standard matrices, the set of orthogonal matrices in $\mathbb{R}^2$ which are isometries are denoted by $O(2, \mathbb{R})$ which is a subgroup of $GL(n, \mathbb{R})$ under matrix multiplication which was covered earlier. The definition of $O(n, \mathbb{R})$ is given below as a recap:

$$O(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : A \text{ is invertible and } A^T = A^{-1}\}$$

Since the dihedral group deals with isometries in $\mathbb{R}^2$, it is important to realize that there are a finite number of types isometries in $\mathbb{R}^2$, these are namely rotation by some angle and reflection. Their notations used in this course are given below.

Notation: Reflection and rotation isometries

The following are the only 2 linear isometries in $\mathbb{R}^2$:

- **Rotation**: The rotation transformation by angle θ around the origin counter clockwise denoted by R_θ
- **Reflection**: the reflection of vectors across the line d passing through the origin is denoted by S_d.

Now we can use the above definitions to define the dihedral group D_n.

Definition: Dihedral group D_n

The dihedral group denoted by D_n is given as below under function composition:

$$D_n = \{T \in L(\mathbb{R}^2, \mathbb{R}^2) : T \text{ is an isometry which preserves } P_n\}$$

The matrix equivalent is given as below under matrix multiplication:

$$D_n = \{M \in O(n, \mathbb{R}) : M \text{ preserves } P_n\}$$

Remark: Preserves in this sense means that after applying the transformation of isometry T on P_n(n sided regular polygon), we get back P_n in same coordinates as before transformation. Since the only isometries in $\mathbb{R}^2$ are reflection and rotation, D_n is a subset of all such transformations. There are multiple ways to view and define the dihedral group. We discussed some examples during lecture and the alternative explanations. It is recommended to consult the course notes by Ali(chapter 4.1 examples and explanations) in case the nature/definition of D_n is unclear. How to generally write out the elements of D_n will be covered later in the notes after the below given examples.

To better understand dihedral groups, one of the examples discussed in class was D_4.

Example: D_4

Find the elements of D_4

Solution: D_4 is the group of all linear isometries in $\mathbb{R}^2$ that preserve P_4 as per definition. This means that it is a group of all linear isometries that preserve a square centered at (0,0). Since these isometries can only be rotation or reflections, we start by realizing that a rotation of $\frac{\pi}{2}$ is one such transformation. Therefore $R_{\frac{\pi}{2}} \in D_4$. We further realize that a rotation of $\pi, \frac{3\pi}{2}$ also preserve the square and thus $R_\pi, R_{\frac{3\pi}{2}} \in D_4$ as well. Note that 2π also works, however that is that same as no rotation at all and therefore don't need to include it. We then move on to reflections. Another way to view finding such reflection isometries is finding axes of symmetry of the square, which is the same as finding reflections that preserve the square after reflection across certain axes.

We see that the x axis is one such line which we can denote as d_1(note that d_1 could have also been denoted as the y axis, as long as you clearly define your line) therefore $S_{d_1} \in D_4$. The other possible lines of symmetry are $y = x$, $y = -x$ and the y axis. We can denote these as $S_{d_2}, S_{d_3}, S_{d_4} \in D_4$ respectively. We therefore have D_4 constructed with our isometries as

below(note that ϵ is the identity isometry):

$$D_4 = \{\epsilon, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, S_{d_1}, S_{d_2}, S_{d_3}, S_{d_4}\}$$

Notice that the rotations are multiples of $\frac{\pi}{2} = \frac{2\pi}{4}$. We can therefore generalize D_4 as the below set builder form:

$$D_4 = \{R_{\frac{\pi}{2}k} : 0 \leq k \leq 3, S_{d_k} : 1 \leq k \leq 4\}$$

(Note that it is highly recommended to see examples in Ali's course notes chapter 4.1 for a better visual understanding in case it is hard to follow why these choices are being made in the solution.)

We see that we can generalize this to D_n as below:

$$D_n = \{R_{\frac{2\pi k}{n}} : 0 \leq k \leq n-1\, S_{d_k} : 1 \leq k \leq n\}$$

Where for $k = 0$ we get R_0 which is the identity transformation ϵ. We can now use our knowledge of groups, generators and order to come up with an even more generalized way to construct D_n. Since our dihedral group is a composition of rotations and reflections.

Proposition: reflection and reflections as generator of D_n

For an elementary rotation isometry $r = R_{\frac{2\pi}{n}}$ and an arbitrary reflection across an axis of symmetry $s = S_d$. We have that $D_n = \langle r, s\rangle$ with the following properties:

- $|r| = n$
- $|s| = 2$
- $rs = sr^{-1}$

Proof:

Assuming that $r = R_{\frac{2\pi}{n}}$. We see that in general $r^k = (R_{\frac{2\pi}{n}})^k = R_{\frac{2\pi}{n}} \cdot R_{\frac{2\pi}{n}} \cdot R_{\frac{2\pi}{n}} \ldots R_{\frac{2\pi}{n}}$ k times $= R_{\frac{2\pi k}{n}}$. Using this fact we see $r^n = R_{\frac{2\pi n}{n}} = R_{2\pi} = R_0 = \epsilon$ and thus $|r| = n$.

When it comes to reflection, realize that reflection once and then again is the same as doing no transformation at all which is the identity transformation. Thus $ss = s^2 = \epsilon \implies |s| = 2$.
Geometrically, $rs = sr^{-1}$ is the same observing that reflecting across a line and then rotating by an angle is the same as rotating in the opposite direction and then reflecting and thus $rs = sr^{-1}$.

■

Remark: Notice that $r^{-1} = r^{n-1}$ because rotating in the opposite direction by $\frac{2\pi}{n}$ is the same as rotating in the same direction but by angle $\frac{2\pi(n-1)}{n}$. Using groups we also see that $r^n = \epsilon \implies r^{n-1} = r^{-1}$. In general, $r^{n-k} = r^{-k}$.

Using our observations and the above proposition, we finally generalize the dihedral group that can by written as the following:

Definition: Generalized dihedral group definition

Assuming $r = R_{\frac{2\pi}{n}}$ and s is a reflection across an axis of symmetry of P_n, we can write D_n as below:

$$D_n =< r, s >= \{r, s : |r| = n, |s|, rs = sr^-1\} = \{\epsilon, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

Permutation and symmetry group

Permutation and symmetry groups are special groups that deal with bijections under composition. Recall that $f : A \to B$ is a bijection iff f is both a surjection and an injection. Using this fact, define the permutation group as below:

Definition: Permutation group

The permutation group of some arbitrary set A is given by the set of all bijections from A to A. In other words it the set of all $f : A \to A$ where f is a bijection under function composition.

A specific case where $A = \{1, 2, 3 \ldots n\}$, the permutation group of this form is called a symmetry group defined as below:

Definition: symmetry group

When $A = \{1, 2, \ldots, n\}$, the permutation group of A is denoted by S_n.

Remark: when we say $x \in S_n$, we conventionally call x to be a permutation of S_n. Finding the order of S_n turns out to be an interesting counting problem.

Proposition: Order of S_n

The order of S_n is $n!$

Proof:

We have to show that the total number of bijections from $A = \{1, 2 \ldots, n\}$ is $n!$. First start by assigning a value for x=1 for our permutation f. In other words, choose an output for $f(1)$, we have n total choices. Once done choosing, we move on to choose an output for $f(2)$, note that it cannot be the same as $f(1)$ and therefore we are narrowed down to $n - 1 choices$. Repeating this process till we reach $f(n)$, we see that that the total outcomes/permutations are

$$n(n-1)(n-2)\ldots 3 \cdot 2 \cdot 1 = n! = |S_n|$$

■

We then moved on to m-cycles which are ways to denote cycles within permutations in shorthand as defined below:

Definition: m-cycle

An m-cycle is a tuple of size m written as $(a_1\ a_2\ a_3 \ldots a_{m-1})$ which represents the permutation mapping where $a_i \to a_{i+1}$ for $1 \leq i \leq m-2$ and $a_{m-1} \to a_1$. This means that $f(a_i) = a_{i+1}$ for $1 \leq i \leq m-2$ and $f(a_{m-1}) = a_1$. The rest of mappings are just "fixed", in other words, $f(i) = i$ for all i not in the m-cycle in S_n.

Remark: An m-cycle is still a permutation and thus an element of S_n just with special notation. An example is as below to demonstrate an example of an m-cycle.

Example: 3-cycle

Construct the table for the cycle (1 4 5) in S_5

Solution:

As per the definition of an m-cycle, we have $m = 3$. Our cycle tells us thatt $1 \to 4 \to 5 \to 1$ and we need to "fix" the other remaining positions of S_5 that are not in our cycle. In other words, $f(2) = 2, f(3) = 3$ since $2, 3$ are not in the cycle. The table therefore can be summarized as below

n	1	2	3	4	5
$f(n)$	4	2	3	5	1

We can compose multiple cycles together as they are still technically permutations of the symmetry group as per function composition. We can see the example below:

Example: composition of m-cycles

Construct the table for (1 3)(2 1 4 5) in S_5

Solution:

The two cycles given to us are just permutations which then need to be composed. We apply the same steps as the previous example for the first 5-cycle (which is (2 1 4 5))and then compose the table with the other cycle which is (1 3). This starts with writing out the table with the cycle $2 \to 1 \to 4 \to 5 \to 1$, then fixing 3(because 3 is not in our cycle) as $f(3) = 3$. We then proceed to repeat the process with the other 2 cycle(which is (1 3)) to our previous table. We get our final result as below:

n	1	2	3	4	5
$f(n)$	4	3	1	5	2

Lastly, we define two cycles to be disjoint iff they don't share any elements. For example the two cycles (1 5)(3 2 4) in S_6 are disjoint as they don't share any elements. We covered some special properties of m-cycles in class:

Proposition: properties of m-cycles and permutations

Suppose we denote C_k to be an arbitrary m-cycle(where the size of the cycle could be different for simplicity's sake for some other C_i). Considering the symmetry group S_n, the following properties hold true:

1. $x \in S_n \implies \exists C_1, C_2 \dots C_k$ s.t. $x = C_1C_2C_3 \dots C_k$. (any$x$ can be decomposed into multiple m-cycles)
2. C_1, C_2 being disjoint means they commute i.e. $C_1C_2 = C_2C_1$
3. if C_1 is a k-cycle then $|C_1| = k$
4. Using our decomposition from (1) we see that $|x| = \text{lcm}(|C_1|, |C_2|, |C_3|, \dots, |C_k|)$

Remark: The proofs of these were not covered in class, they are in the course notes. The instructor just gave some examples to intuitively show some of these properties working.