PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 4

INSTRUCTOR: ARUNDHATHI KRISHNAN

5. Permutation Groups

5.1. **Basic Definitions.** A function on a set A which is one-to-one (injective) and onto (surjective) will be called a bijective function. Recall from Subsection 1.3 that given a set A, we can consider the set $\{\alpha : A \to A \mid \alpha \text{ is bijective}\}$ which has a product on it given by composition of functions. This set equipped with this product is then a group. We will henceforth call bijective functions on a non-empty set "permutations".

Definition 5.1.1. Let A be a (non-empty) set. A permutation of A is a bijective function from A to A. A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Let us look at some elementary examples of permutations. The set A can be *any* set, but our focus will be on finite sets.

Example 5.1.2. Let $A = \{1, 2, 3, 4\}$. Define $\alpha : A \to A$ as

$$\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \alpha(4) = 4.$$

This can also be written in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Let us see how to compose two functions on A in this representation. Let $\beta(1) = 2, \beta(2) = 1, \beta(3) = 4, \beta(4) = 3$. Then

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

The products $\beta\alpha$ and $\alpha\beta$ are given by $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}$ and $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$. We note straightaway that the product given by function composition is not commutative.

We now give an example of a permutation group.

Example 5.1.3. Let S_3 denote the set of *all* bijective functions from $\{1, 2, 3\}$ to itself. Then it is an easy computation to see that the cardinality of S_3 is $3! = 6$. We list the elements out explicitly, using the same array form as above.

$$S_3 = \Big\{\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$
$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}\Big\}.$$

Here ε denotes the identity permutation. Note that $\alpha^3 = \varepsilon = \beta^2$ and that $\beta\alpha = \alpha^2\beta$.

The permutation group S_3 is called the symmetric group of degree 3.

Definition 5.1.4. Let $A = \{1, 2, \ldots, n\}$ and S_n denote the group of all permutations of A, equipped with function composition. Elements of S_n have the following array form

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}.$$

S_n is called the symmetric group of degree n.

It is clear that $|\, S_n \,| = n!$.

Exercise 5.1.5. For $n \geq 3$, S_n is non-Abelian.

5.2. **Cycle Notation.** Let $\alpha \in S_6$ be given by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}.$$

We can write α as products of so-called *cycles* in the following way:

$$(1,\, 2)(3,\, 4,\, 6)(5).$$

An expression of the form $(a_1,\, a_2,\, \ldots, a_m)$ is called a cycle of length m or an m-cycle.

The permutation $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$ can be expressed as $(1,\, 5,\, 2,\, 3)(4,\, 6)$.

It is easily checked that $\alpha\beta = (1,\, 5)(2,\, 4,\, 3)(6)$ and $\beta\alpha = (1,\, 3,\, 6)(2,\, 5)(4)$.

Often, a cycle with a single entry is omitted and it is understood that the point in question is fixed (for example, 6 in $\alpha\beta$ and 4 in $\beta\alpha$). The identity ε is often written as a single cycle, say (1).

5.3. **Properties of Permutations.** We now formally show that any finite permutation can be written as a product of disjoint cycles.

Theorem 5.3.1. *Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.*

Proof. Let α be a permutation on $A = \{1, 2, \ldots, n\}$. Choose $a_1^1 \in A$ and let $a_2^1 = \alpha(a_1^1), a_3^1 = \alpha(a_2^1) = \alpha^2(a_1^1), \ldots$ until we arrive at $a_1^1 = \alpha^{m_1}(a_1^1)$ for some m_1. Such an m_1 must surely exist as the sequence $a_1^1, \alpha(a_1^1), \ldots$ takes values in the finite set A. To be precise, we must have $i < j \in \mathbb{N}_0$ such that $\alpha^i(a_1^1) = \alpha^j(a_1^1)$, so that $a_1^1 = \alpha^{j-i}(a_1^1)$. We express this relationship among $a_1^1, \ldots, a_{m_1}^1$ as the cycle $(a_1^1,\, \ldots, a_{m_1}^1)$ and write $\alpha = (a_1^1,\, \ldots, a_{m_1}^1)\cdots$. If all the entries of A are not exhausted, select $a_1^2 \in A$ such that a_1^2 does not belong to the cycle already considered. Repeat the same process as before to get a cycle $(a_1^2, \ldots, a_{m_2}^2)$. We claim that this cycle and the previously constructed cycle have no elements in common. Indeed, if $\alpha^i(a_1^1) = \alpha^j(a_1^2)$ for some $i, j \in \mathbb{N}_0$, then $\alpha^{i-j}(a_1^1) = a_1^2$, which contradicts the criterion for choosing a_1^2. We continue building disjoint cycles in this manner until the (finitely many) elements of A run out, so that we get for some $k \in \mathbb{N}$ and $m_1, \ldots, m_k \in \mathbb{N}$,

$$\alpha = (a_1^1,\, \ldots, a_{m_1}^1)(a_1^2,\, \ldots, a_{m_2}^2)\cdots(a_1^k,\, \ldots, a_{m_k}^k).$$

□

We next show that disjoint cycles commute.

Theorem 5.3.2. *If the pair of cycles $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.*

Proof. Suppose α and β are permutations of $S = \{a_1 \ldots, a_m, b_1, \ldots, b_n, c_1 \ldots, c_s\}$ where the c_i-s are left fixed by α and β. We will show that $\alpha\beta(x) = \beta\alpha(x)$ for all $x \in S$.

First, suppose $x = c_i$ for some i. Then $\alpha\beta(c_i) = \alpha(c_i) = c_i = \beta(c_i) = \beta\alpha(c_i)$.

If $x = a_i$ for some i, then $\alpha\beta(a_i) = \alpha(a_i) = a_{i+1} = \beta(a_{i+1}) = \beta\alpha(a_i)$, with the understanding that $a_{m+1} = a_1$. Similarly, $\alpha\beta(b_i) = \alpha(b_{i+1}) = b_{i+1} = \beta(b_i) = \beta\alpha(b_i)$ with the understanding that $b_{n+1} = b_1$. □

We now show that the order of a permutation can be determined from the lengths of disjoint cycles whose product is the permutation.

Theorem 5.3.3. *The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

Proof. Note that any cycle of length n has order n. We will call the elements $c_1, \ldots, c_s$ that appear in a permutation $\gamma = (c_1, \ldots, c_s)$ *symbols*. Suppose that α and β are disjoint cycles of length m and n, and let $k = \text{lcm}(m, n)$. Then $\alpha^k = \varepsilon = \beta^k$. Now $(\alpha\beta)^k = \alpha^k\beta^k = \varepsilon$ as α and β commute by Theorem 5.3.2. Let t be the order of $\alpha\beta$. By Corollary 4.1.5, t divides k. Now, $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, so $\alpha^t = \beta^{-t}$. As α and β are disjoint cycles, there is no common symbol that appears in both. Hence, the same is true of α^t and β^{-t} as raising a cycle to a power does not introduce any new symbols. Hence the equality of α^t and β^{-t} means that we must have $\alpha^t = \varepsilon = \beta^{-t}$, so that m and n both divide t, by another application of Corollary 4.1.5. Hence, the least common multiple k of m and n also divides t so that $k = t$. That is, $|\,\alpha\beta\,| = \text{lcm}(m, n)$. The argument can now be extended to any finite product of disjoint cycles. □

2-cycles, which are also called transpositions, are of particular importance.

Theorem 5.3.4. *Every permutation in S_n for $n \geq 2$ is a product of 2-cycles.*

Proof. The identity can be written as $\varepsilon = (1, 2)(2, 1)$. By Theorem 5.3.1, we know that every permutation can be written as a product of disjoint cycles as follows:

$$(a_1, \ldots, a_m)(b_1, \ldots, b_n) \cdots (c_1, \ldots, c_s).$$

It is easily verified that this can be written as

$$(a_1, a_m)(a_1, a_{m-1}) \cdots (a_1, a_2)(b_1, b_n)(b_1, b_{n-1}) \cdots (b_1, b_2) \cdots (c_1, c_s)(c_1, c_{s-1}) \cdots (c_1 c_2).$$

□

It is worth noting that the decomposition above is not unique. For example, the cycle $(1, 2, 3, 4, 5)$ can be expressed as both $(1, 5)(1, 4)(1, 3)(1, 2)$ and $(5, 4)(5, 2)(2, 1)(2, 5)(2, 3)(1, 3)$.

Lemma 5.3.5. *If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where the β_i-s are 2-cycles, then r is even.*

Proof. Clearly, $r \neq 1$ as a 2-cycle cannot be the identity ε. If $r = 2$, we are done. Let us thus suppose that $r > 2$ and assume that the result is true for all $s < r$. Suppose the rightmost 2-cycle is (a, b). The product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms for some symbols c, d in the set on which the permutation is considered. For each of the cases below, we express the product of cycles on the left hand side as a product of cycles on the right hand side in such a way that a does not occur in the rightmost cycle.

$$(a,b)(a,b) = \varepsilon$$
$$(a,c)(a,b) = (a,b)(b,c)$$
$$(b,c)(a,b) = (a,c)(c,b)$$
$$(c,d)(a,b) = (a,b)(c,d).$$

In the first case, we can delete the terms $\beta_{r-1}\beta r$ so that $\varepsilon = \beta_1 \cdots \beta_{r-2}$ and then $r-2$ is even by the induction hypothesis, so r is even.

In all the other cases, we replace the form of $\beta_{r-1}\beta_r$ by what is given on the right hand side above. Repeat the same process for the pair of terms $\beta_{r-2}\beta_{r-1}$ so that we either get a product of $(r-2)$ cycles equal to ε or the rightmost occurrence of a in the 2-cycles is in the third-last term. We can now continue this process to arrive at the situation that either an $(r-2)$ product of 2-cycles is the identity, or that the only occurrence of a is in the left-most cycle. The latter is impossible, as the identity fixes a. Hence only the former is possible, namely that a product of $(r-2)$ cycles is equal to ε. Hence, by (strong) induction, $r-2$ is even, and r is even.

□

Theorem 5.3.6. *If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (respectively, odd) number of 2-cycles.*

Proof. Suppose $\alpha = \beta_1 \cdots \beta_r = \gamma_1 \cdots \gamma_s$ for $r, s \in \mathbb{N}$. Then $\varepsilon = \gamma_1 \cdots \gamma_s \beta_r^{-1} \cdots \beta_1^{-1} = \gamma_1 \cdots \gamma_s \beta_r \cdots \beta_1$. By Lemma 5.3.5, $s+r$ is even, so s, r are both odd or both even. Note that we used here that the inverse of a 2-cycle is itself. □

The above theorem allows us to make the following definition.

Definition 5.3.7. A permutation that can be expressed as a product of an even (odd) number of 2-cycles is called an even (respectively, odd) permutation.

Theorem 5.3.8. *The set of even permutations in S_n forms a subgroup of S_n. It is denoted by A_n and called the alternating group of degree n.*

Proof. The identity ε belongs to A_n by Lemma 5.3.5. It is clear that a 2-cycle is its own inverse. Hence the inverse of an even permutation is also even. Finally, clearly the product of two even permutations is even. □

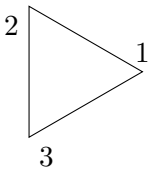
Theorem 5.3.9. *For $n \geq 2$, $|\, A_n \,| = \frac{n!}{2}$.*

Proof. For each odd permutation α, the permutation $(1,2)\alpha$ is even and $(1,2)\alpha \neq (1,2)\beta$ when $\alpha \neq \beta$. Thus the number of even permutations is greater than or equal to the number of odd permutations. Similarly if α is even, the permutation $(1,2)\alpha$ is odd and $(1,2)\alpha \neq (1,2)\beta$ if $\alpha \neq \beta$. Hence the number of odd permutations is greater than or equal to the number of even permutations. So, indeed, these numbers must be equal and each is equal to $\frac{|\, S_n \,|}{2}$. So $|\, A_n \,| = \frac{n!}{2}$.

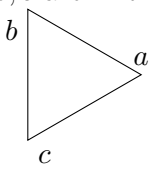
□

5.4. **Dihedral Groups.** We look at a particular type of permutation groups called dihedral groups. We are interested in the so-called *symmetries* of the regular polygon with n sides, $n \geq 3$. These are bijections from the polygon onto itself such that the orientation is preserved. They consist of *rotational* and *reflection* symmetries.

Let us start by considering the example of an equilateral triangle.



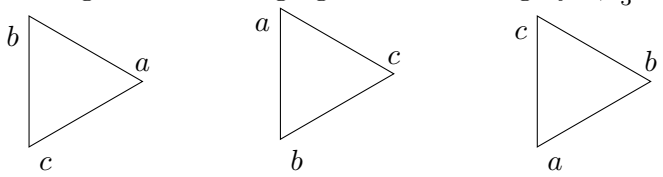
In its resting state, the vertices a, b, c are in the positions $1, 2$, and 3 respectively.



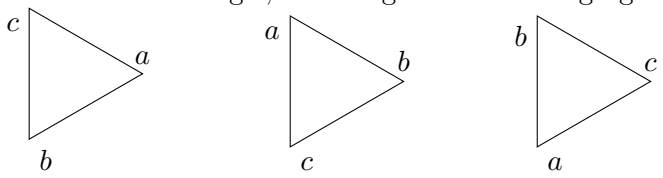
On applying one of our symmetries, the resulting figure must look the same, and only the labels may change. It is clear then that the rotational symmetries are given by rotating (counterclockwise) by $0, \frac{2\pi}{3}$ and $\frac{4\pi}{3}$.

For example, rotating by $\frac{2\pi}{3}$ sends the vertex a to the position 2, vertex b to position 3 and vertex c to position 1.

So we get the resulting figures on rotating by $0, \frac{2\pi}{3}$ and $\frac{4\pi}{3}$ respectively:



What about the reflection symmetries? This is achieved by reflecting about the three bisectors of the triangle, and we get the following figures:



Let us formalize how to write the above symmetries in the array form and cycle form discussed for permutations. For example, we write rotation by $\frac{2\pi}{3}$ as

$$r_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix},$$

as vertex a is now in the 2nd place, vertex b in the 3rd place and vertex c in the 1st place. The first row of the above array records the initial positions of the vertices respectively, and the second row the final positions. In cycle form, clearly $r_1 = (1, 2, 3)$.

Let us now write the permutation given by reflection about the bisector passing through the vertex in the first position:

$$s_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix},$$

as a stays in position 1 and b and c interchange positions. Clearly, in cycle form $s_0 = (2, 3)$.

We now list the above figures in cycle form

$$\{r_0 = (1), r_1 = (1, 2, 3), r_2 = (1, 3, 2), s_0 = (2, 3), s_1 = (1, 2), s_2 = (1, 3)\},$$

and note that there are $6 = 2(3)$ such symmetries. We are now ready to define dihedral groups more formally.

For $n \geq 3$, consider the regular n-polygon in $\mathbb{R}^2$. It has $2n$ symmetries, namely n rotations r_k (counter-clockwise) by $\frac{2\pi k}{n}$ for $k = 0, 2, \ldots, n-1$, and n reflections s_l about the axis passing through $\frac{\pi l}{n}$ for $l = 0, \ldots, n-1$. There are $2n$ such symmetries in total. The key point is that the set $\{r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}\}$ forms a group under the product given by composition of maps.

Let us form the multiplication table for the symmetries of the regular 3-gon, that is, the equilateral triangle considered above.

	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

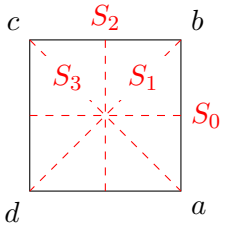
Let us verify this in cycle notation for $r_2 s_1$ for example:

$$r_2 s_1 = (1,3,2)(1,2) = (2,3) = s_0.$$

We will now define the dihedral group D_n of order $2n$ abstractly. It is the set $D_n = \{r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}\}$ with products given by:

$$r_i r_j = r_{(i+j \mod n)}, r_i s_j = s_{(i+j \mod n)}, s_i r_j = s_{(i-j \mod n)}, s_i s_j = r_{(i-j \mod n)}. \tag{1}$$

Let us look briefly at the case $n = 4$, that is, we consider the symmetries of a square.



Then $D_4 = \{r_0, r_1, r_2, r_3, s_0, s_1, s_2, s_3\}$ where r_i denotes the (counter-clockwise) rotation by $\frac{2\pi i}{4}$ and s_i denoted the reflection about the axis passing through $\frac{\pi i}{4}$. The corresponding axes are marked on the figure as S_i.

Let us write the elements of D_4 in array form:

$$r_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = (1) = \varepsilon$$
$$r_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1,2,3,4)$$
$$r_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = (1,3)(2,4)$$
$$r_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = (1,4,3,2)$$
$$s_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (1,2)(3,4)$$
$$s_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = (1,3)$$
$$s_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = (1,4)(2,3)$$
$$s_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} = (2,4)$$

As an exercise, verify that the elements of D_4 as presented in cycle form satisfy the relations of Equation (1).

See below a pictorial representation of the symmetries of a regular octagon.

FIGURE 1. Jim.belk, Public domain, via Wikimedia Commons

As an exercise, write the elements of D_8 and find their array and cycle forms too.

REFERENCES

[1] Chapters 2 and 5. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.