Math 403 Chapter 5 Permutation Groups:

---

1. **Introduction:** We now jump in some sense from the simplest type of group (a cylic group) to the most complicated.

2. **Definition:** Given a set A, a *permutation* of A is a function $f : A \to A$ which is 1-1 and onto. A *permutation group* of A is a set of permutations of A that forms a group under function composition.

3. **Note:** We'll focus specifically on the case when $A = \{1, ..., n\}$ for some fixed integer n. This means each group element will permute this set. For example if $A = \{1, 2, 3\}$ then a permutation α might have $\alpha(1) = 2$, $\alpha(2) = 1$, and $\alpha(3) = 3$. We can write this as:

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

   We will eventually have a better way to write these but this suffices for now.

4. **The Symmetric Groups $\mathbf{S_n}$**

   (a) **Definition:** The *symmetric group* S_n is the group of all permutations of the set $\{1, 2, ..., n\}$.
   Example: The group S_3 consists of six elements. There are 6 because there are 3 choices as to where to send 1 and 2 choices as to where to send 2 and 1 choices as to where to send 3. These six elements are:

$$S_3 = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$$

   When we compose elements we read the permutations from right to left. For example if α is the second element above and if β is the third element above then:

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

   So notice that this group is not Abelian.

   (b) **Cycle Notation:** We now write down a more compact notation for S_n. Consider the following element in S_7:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 4 & 7 & 6 & 2 \end{bmatrix}$$

   What is going on here is:

$$\begin{gathered} 1 \to 3 \to 1 \\ 2 \to 5 \to 7 \to 2 \\ 4 \to 4 \\ 6 \to 6 \end{gathered}$$

We write:

$$\alpha = (1\,3)(2\,5\,7)$$

notice that each parenthetical closes up as a cycle (a loop) and neither 4 nor 6 are mentioned because they are left alone. Within each cycle we read from left-to-right and then cycle back to the start.

Using this notation we can write:

$$S_3 = \{(), (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$$

The notation is not unique, for example $(2\,1) = (2\,1)$ and $(1\,2\,3) = (2\,3\,1) = (3\,1\,2)$.

The inverse of such an element can be obtained simply by reversing each of the disjoint cycles, for example:

$$((1\,5\,3\,2)(4\,7\,6))^{-1} = (2\,3\,5\,1)(6\,7\,4)$$

When we compose elements in this notation we could just put them adjacent but the goal is to get them in *disjoint cycle form*, meaning rewritten as a product of cycles within no overlap.

For example suppose $\alpha = (1\,2)(4\,5)$ and $\beta = (1\,5\,3)(2\,4)$. Suppose we wish to find $\alpha\beta$. We know $\alpha\beta = (1\,2)(4\,5)(1\,5\,3)(2\,4)$ but we'd like to write this in disjoint cycle form.

First we start with 1 and trace it through the element taking the cycles from right-to-left but within each cycle working left-to-right:

$$\underbrace{\overleftarrow{\underbrace{(1\,2)}_{4\to4}\,\underbrace{(4\,5)}_{5\to4}\,\underbrace{(1\,5\,3)}_{1\to5}\,\underbrace{(2\,4)}_{1\to1}}}_{1\to4}$$

Then since we ended with 4 we trace that through:

$$\underbrace{\overleftarrow{\underbrace{(1\,2)}_{2\to1}\,\underbrace{(4\,5)}_{2\to2}\,\underbrace{(1\,5\,3)}_{2\to2}\,\underbrace{(2\,4)}_{4\to2}}}_{4\to1}$$

Since $1 \to 4 \to 1$ we have $(1\,4)$ so far. Then we do the same with the next smallest number (or any number) which we haven't checked yet. If we try 2 we find $2 \to 5 \to 3 \to 2$ and so we have $(2\,5\,3)$. There are no numbers left so we are done.

Thus:

$$\alpha\beta = (1\,2)(4\,5)(1\,5\,3)(2\,4) = (1\,4)(2\,5\,3)$$

Similarly we have:

$$\beta\alpha = (1\,5\,3)(2\,4)(1\,2)(4\,5) = (1\,4\,3)(2\,5)$$

5. **Properties of Permutations:**

   (a) **Theorem:** Every permutation in S_n may be written as a cycle or as a product of disjoint cycles.

   Outline of Proof: The general idea is to formalize the process we just did. $\mathcal{QED}$

(b) **Theorem:** Disjoint cycles commute.
Outline of Proof: If cycles are disjoint they do not affect any common numbers. Consequently it does not matter the order in which we do them. $\mathcal{QED}$

(c) **Theorem:** If $\alpha \in S_n$ then the order of α is the least common multiple of the lengths of the cycles when written in disjoint cycle form.
Outline of Proof: Clearly the we achieve the identity when the power of the element is a multiple of the lengths of the cycles and hence the lcm will achieve $e = ()$. Showing that nothing smaller works takes a bit more work. $\mathcal{QED}$
Example: In S_{10} we have $|(1\,5\,10\,2)(3\,9\,8\,4\,7\,6)| = \text{lcm}\,(4, 6) = 12$.
Note: If the element is not in disjoint cycle form then we must rewrite it, otherwise the order is not at all obvious.

(d) **Theorem:** Every permutation in S_n is a product of 2-cycles.
Proof: Notice that for a cycle:

$$(a_1\,a_2\,a_3\,...\,a_n) = (a_1\,a_n)(a_1\,a_{n-1})...(a_1\,a_3)(a_1\,a_2)$$

Products of cycles are just then products of 2-cycles. $\mathcal{QED}$
Example: We have $(1\,5\,3\,7)(2\,6\,4) = (1\,7)(1\,3)(1\,5)(2\,4)(2\,6)$.

(e) **Theorem:** If $() = \alpha_1\alpha_2...\alpha_r$ where the α_i are 2-cycles then r is even.
Proof: If $r = 1$ then we cannot have $() = \alpha_1$, a single 2-cycle. Thus assume

$$() = \alpha_1...\alpha_r$$

for $r \geq 2$. Consider $\alpha_{r-1}\alpha_r$. This can have only one of the following forms: $(a\,b)(a\,b)$ or $(a\,c)(a\,b)$ or $(b\,c)(a\,b)$ or $(c\,d)(a\,b)$. Focusing on the a, each of these forms can be rewritten:

$$\begin{aligned}(a\,b)(a\,b) &= ()\\(a\,c)(a\,b) &= (a\,b)(b\,c)\\(b\,c)(a\,b) &= (a\,c)(c\,b)\\(c\,d)(a\,b) &= (a\,b)(c\,d)\end{aligned}$$

In the first case we delete the final two 2-cycles and start the process again at the right end.

In the other three cases notice that the a has moved from the final 2-cycle to the one before. We then repeat the procedure with $\alpha_{k-1}\alpha_k$ until either we get cancelation case (and we start the process again at the right end) or else we get an a in the first 2-cycle but nowhere else. However this cannot happen since then this element would not fix a and would not be $()$. $\mathcal{QED}$

(f) **Theorem:** Given $\alpha \in S_n$. If we write α as a product of 2-cycles then whether the number of 2-cycles is even or odd depends only on α and not on how we write it. In other words a given α can either be done only using an odd number of 2-cycles or only using an even number of 2-cycles.
Proof: Suppose $\alpha = A = B$ where A is a product of an even number of 2-cycles and B is a product of an odd number of 2-cycles. Then $AB^{-1} = ()$, a contradiction. $\mathcal{QED}$

(g) **Definition:** An element $\alpha \in S_n$ is *even* if it can be written using an even number of 2-cycles and *odd* if it can be written using an odd number of 2-cycles.
Example: The element $(1\,5\,3\,7)(2\,6\,4)$ is odd because

$$(1\,5\,3\,7)(2\,6\,4) = (1\,7)(1\,3)(1\,5)(2\,4)(2\,6)$$

and this is an odd number of 2-cycles.

(h) **Definition/Theorem:** The set $A_n = \{\{\alpha \in S_n \,|\, \alpha \text{is even}\}$ forms a subgroup of S_n called the *alternating group on n elements*.

Outline of Proof: This is fairly straightfoward just looking at the requirements of a group. $\mathcal{QED}$

Note: The odd permutations do not form a subgroup not least because the identity is not in the set because the identity is even.

6. **Closing Note:** We can think of symmetric groups as "complicated" because there is a lot going on inside them. For example it turns out (and we will prove this) that every group basically sits inside a symmetric group, where "sits inside" means "is structurally equivalent to a subgroup of". For example consider $\mathbb{Z}_6$. This is a cyclic group of order 6. Well in S_6 we have $\langle(1\,2\,3\,4\,5\,6)\rangle$ which is a cyclic subgroup of S_6 of order 6 so we can think of "something that looks like $\mathbb{Z}_6$" sitting inside S_6.