Chapter 5: Permutation Groups

Dr. Jehan Al-bar

December 3, 2010

We study Certain groups of functions, known as permutation groups from a set A to itself.

Definition of Permutation on A, Permutation Group of A.

Definition

A permutation of a set A is a function from A to A that is both one-one and onto. A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Definition of Permutation on A, Permutation Group of A.

In this chapter we consider the set A to be finite, and we set $A = \{1, 2, 3, ..., n\}$ for positive integer n.

Examples

1. A permutation α on the set $\{1,2,3,4\}$ is defined to be $\alpha(1)=2, \alpha(2)=3, \alpha(3)=1, \alpha(4)=4$. We write α in array form

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

2. A permutation β on the set $\{1,2,3,4,5,6\}$ is defined to be $\beta(1)=5, \beta(2)=3, \beta(3)=1, \beta(4)=6, \beta(5)=2$, $\beta(6)=4$, and we write

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

Composition of Permutations

We express the composition of permutations in array notation, and we carry it out from **right to left** going from top to bottom, then again from top to bottom, as we see in the next example.

Composition of Permutations

Example

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$ and $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$ Then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

On the right array we have 2 under 1, and on the left array we have 4 under 2, so in the composition we must have 4 under 1, and so on. in function composition language we write $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$, hence $\gamma\sigma$ sends 1 to 4. Following in this manner we have

$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$

Symmetric Group S_n

Let $A = \{1, 2, 3, ..., n\}$. Then the set of all permutations of A under the function composition is called the *symmetric group of degree n* and is denoted by S_n. Elements of S_n are on the form

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

The order of $S_n = n!$

Symmetric Group S_3

Example

Let S_3 denote the set of all one-one and onto functions from $\{1, 2, 3\}$ to itself. Then S_3 under function composition, is a group with 6 elements. They are

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

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

We note that $\beta\alpha \neq \alpha\beta$, so S_3 is non-Abelian group.

Cycle Notation

The cycle notation is another way to specify permutations. Some important properties of the permutation can easily be determined when cycle notation is used. Let

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

In cycle notation $\alpha = (12)(346)(5)$, and for

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

we have $\beta = (1523)(46)$ or $\beta = (46)(3152)$.
An expression of the form $(a_1, a_2, ..., a_m)$ is called a cycle of length m or an m-cycle.

Multiplication of Cycles

We think of a cycle as a permutation that fixes any symbol not appearing in the cycle. For example, the cycle (46) represents the permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{bmatrix}$.

Bearing this in mind, when multiplying cycles we think of them as permutations given in array form. For example, in S_8, let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$, then $\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$

A disjoint Cycle Form

In this form the various cycles have **no number in common**. Because function composition is done from right to left, and each cycle that does not contain a symbol fixes that symbol, we see that (5) fixes 1, (648) fixes 1, (1237) sends 1 to 2, (8) fixes 2, (456) fixes 2, (27) sends 2 to 7, and (13) fixes 7. So the net effect of $\alpha\beta$ is to send 1 to 7. So $\alpha\beta = (17....)$.
Repeating the process starting with 7, we have
$7 \to 7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3$, so that $\alpha\beta = (173...)$.
Ultimately, we have $\alpha\beta = (1732)(48)(56)$. **The important thing when multiplying cycles is to keep moving from one cycle to the next from right to left.**

A Cycle Notation, Disjoint cycle form

Example

Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$
In cycle notation $\alpha = (12)(3)(45)$ and $\beta = (153)(24)$, and $\alpha\beta = (12)(3)(45)(153)(24)$. In disjoint cycle form, $\alpha\beta = (14)(253)$. To convert $\alpha\beta$ back to array form, we observe that (14) means 1 goes to 4 and 4 goes to 1, (253) means $2 \to 5 \to 3 \to 2$.

It is preferred not to write the cycle with one entry. **The missing element is mapped to itself**. For instance, the previous α cab be written as $\alpha = (12)(45)$

The Identity Permutation in Cycle Form

The identity permutation consists only of cycles with one entry, so we write just one cycle. For example,

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

can be written as $\varepsilon = (5)$ or $\varepsilon = (3)$.
Remember that missing elements are mapped to themselves.