Chapter 5

**Defn.** Let $A$ be a nonempty set.
A permutation of $A$ is a bijection $\alpha: A \to A$.
The permutation group of $A$ is the set of all permutations of $A$ with the binary operation of composition of functions.

We will focus on the case where $A = \{1, 2, 3, \ldots, n\}$ for some $n \in \mathbb{Z}$, $n \geq 1$.

**Defn.** The symmetric group of degree $n$, denoted $S_n$, is the permutation group of $\{1, 2, \ldots, n\}$.
We will denote the identity of $S_n$ by $e$.

**Ex/Defn.** Consider $\alpha \in S_5$ where
$\alpha(1) = 4 \quad \alpha(2) = 3 \quad \alpha(3) = 5 \quad \alpha(4) = 1 \quad \alpha(5) = 2$

We express $\alpha$ in array form by

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

In general, for $\beta \in S_n$ we write

$$
\beta = \begin{bmatrix}
1 & 2 & 3 & \cdots & n \\
\beta(1) & \beta(2) & \beta(3) & \cdots & \beta(n)
\end{bmatrix}
$$
Suppose \( \alpha \in S_5 \) is as above and
\[
\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix}
\]
Then
\[
\alpha \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{bmatrix}
\]
Also
\[
\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}
\]
Note: When building \( \alpha \in S_n \) you have

* \( n \) choices for \( \alpha(1) \)
* \( n-1 \) remaining choices for \( \alpha(2) \)
* \( 2 \) choices for \( \alpha(n-1) \)
* only 1 choice for \( \alpha(n) \)

Therefore \( S_n \) has order \( |S_n| = n! \)

**Cycle Notation**

Every \( \alpha \in S_n \) divides (partitions) \( S_n \) into cycles

Ex: \( \alpha = [4 \, 3 \, 5 \, 1 \, 2] \) as above

\[
\begin{array}{c}
1 \rightarrow 4 \\
2 \rightarrow 3 \\
5 \rightarrow \alpha \\
\alpha \rightarrow \alpha
\end{array}
\]
We therefore write \( \alpha \) in cycle notation as
\[
\alpha = (14)(235)
\]

Note: The cycle notation is not unique. We could also write
\[
\alpha = (235)(14) \text{ or } \\
\alpha = (41)(352) \text{ or } \\
\alpha = (523)(14) \text{ etc.}
\]

Here's another example
\[
\beta = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
4 & 6 & 1 & 3 & 7 & 2 & 5
\end{bmatrix}
\]

Then in cycle notation
\[
\beta = (143)(26)(57)
\]

And another
\[
\gamma = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
6 & 1 & 3 & 2 & 7 & 4 & 5
\end{bmatrix}
\]
\[
\gamma = (1642)(3)(57)
\]

When there are cycles having only one element, it is customary to not write them.
\[
\delta = (1642)(57)
\]
Similarly if
\[ \sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{bmatrix} \]

Then we can write
\[ \sigma = (1 \ 5) \ (2) \ (3) \ (4 \ 7) \ (6) \]
or
\[ \sigma = (1 \ 5) \ (4 \ 7) \]
with the bottom notation being most preferred.

For the identity
\[ e = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix} \]
we can write
\[ e = (1) \text{ or } e = (2) \text{ or } \ldots \text{ or } e = (7) \]

**Defn.** A permutation of the form \((a_1, a_2, \ldots, a_m)\)
is called a cycle of length \(m\) or an \(m\)-cycle.

**Note:** When we express permutations using
cycle notation, we typically wish to express them as a product of disjoint cycles (meaning no two distinct cycles have a number in common).
Ex: Express $\alpha \beta \in S_8$ as a product of disjoint cycles if
$\alpha = (1\ 6\ 5\ 2\ 4)(3\ 7), \ \beta = (2\ 8\ 4)(1\ 5)(6\ 7)$

$\alpha \beta = (1\ 6\ 5\ 2\ 4)(3\ 7)(2\ 8\ 4)(1\ 5)(6\ 7)$

but these cycles are not disjoint.

$\alpha \beta = (1\ 2\ 8)(3\ 7\ 5\ 6)(4)$

$\alpha \beta = (1\ 2\ 8)(3\ 7\ 5\ 6)$

Thm 5.1: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Should be intuitively self-evident. See the book for detailed proof.

Thm 5.2: If $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ are disjoint cycles then $\alpha \beta = \beta \alpha$

Pf: Say $\alpha, \beta$ are permutations of a set $S$. To show the functions $\alpha \beta$ and $\beta \alpha$ are equal, we must check that $(\alpha \beta)(x) = (\beta \alpha)(x)$ for all $x \in S$. Consider any $x \in S$. 
Case 1: \( x = a_i \) for some \( 1 \leq i \leq m \). 

Then \( \alpha(x) = a_j \) where 
\[
    j = \begin{cases} 
        i+1 & \text{if } i < m \\
        1 & \text{if } i = m 
    \end{cases}
\]

Since \( \alpha \) and \( \beta \) are disjoint, we have 
\( \beta(x) = \beta(a_i) = a_i = x \) and \( \beta(a_j) = a_j \). 

So 
\[
    (\alpha \beta)(x) = \alpha(\beta(x)) = \alpha(x) = a_j = \beta(a_j) = \beta(\alpha(x)) = (\beta \alpha)(x)
\]

Case 2: \( x = b_i \) for some \( 1 \leq i \leq n \). 

As in Case 1, \( \beta(x) = b_j \) for some \( j \) and \( \alpha(x) = x \), \( \alpha(b_j) = b_j \) (since \( \alpha \) and \( \beta \) are disjoint). 

So 
\[
    (\alpha \beta)(x) = \alpha(\beta(x)) = \alpha(x) = b_j = \beta(x) = \beta(\alpha(x)) = (\beta \alpha)(x)
\]

Case 3: \( x \in S_0, \ldots, a_m, b_1, \ldots, b_n \). 

Then \( \alpha(x) = x \) and \( \beta(x) = x \). 

So 
\[
    (\alpha \beta)(x) = \alpha(\beta(x)) = x = \beta(\alpha(x)) = (\beta \alpha)(x)
\]

Thm 5.3: The order of a product of disjoint cycles is equal to the least common multiple of the lengths of the cycles.

Pf: We'll prove this for the product of 2 disjoint cycles. The proof of the general case is similar.
Say \( \alpha \) and \( \beta \) are disjoint cycles of lengths \( m \) and \( n \). Note that
\[
m = \text{order of } \alpha, \quad n = \text{order of } \beta.
\]
Setting \( k = \text{lcm}(m,n) \), we have \( \alpha^k = e = \beta^k \).
Since \( \alpha, \beta \) disjoint, they commute, so
\[
(\alpha \beta)^k = \alpha^k \beta^k = ee = e
\]
Therefore \( \text{(order of } \alpha \beta) \leq k \).
On the other hand, for every \( 0 < t < k \)
we have that \( \alpha^t \) and \( \beta^{-t} \) are disjoint
since \( \alpha, \beta \) are disjoint, so we must have
\[
\alpha^t \neq \beta^{-t} \quad \text{(since they are disjoint and at least one is not e since } 0 < t < k\text{)}.
\]
Thus \( \alpha^t \beta^t = e \) and so \( (\alpha \beta)^t = \alpha^t \beta^t = e \). \( \square \)

**Ex:** Order of \((169)(25)(78)\) is \(\text{lcm}(3,2,2) = 6\)
Order of \((5732)(146)(89)\) is \(\text{lcm}(4,3,2) = 12\)