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

$$\beta = \begin{bmatrix} 1 & 2 & 3 & \ldots & n \\ \beta(1) & \beta(2) & \beta(3) & \ldots & \beta(n) \end{bmatrix}$$
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 \( n \) cycles.

Ex: \( \alpha = \begin{bmatrix} 1 & 4 & 2 & 3 & 5 & 7 \end{bmatrix} \) as above
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
\[ \gamma = (1642)(57) \]
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
\[ \sigma = (15)(2)(3)(47)(6) \]
or
\[ \sigma = (15)(47) \]
with the bottom notation being most preferred.

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

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 distinct cycles (meaning no two distinct cycles have a number in common).
Ex: Express $\alpha \beta$ as a product of disjoint cycles if
$\alpha = (1\ 6\ 5\ 2\ 4)(3\ 7), \ \beta = (2\ 8\ 4)(1\ 5)(6\ 7)$

$\alpha \beta = (1\ 6\ 5\ 2\ 4)(3\ 7)(2\ 8\ 4)(1\ 5)(6\ 7) \leftarrow$ but these cycles are not disjoint

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

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

**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 $\alpha = (a_1, a_2, \cdots, a_m)$ and $\beta = (b_1, b_2, \cdots, b_n)$ 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

\[
\begin{align*}
j &= \begin{cases} 
i + 1 & \text{if } i < m \\ 1 & \text{if } i = m \end{cases}
\end{align*}
\]

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

So,

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

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 \( \beta \) disjoint).

So

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

Case 3: \( x \in \{ a_1, \ldots, a_m, b_1, \ldots, b_n \} \)

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

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

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

**Pr:** 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 \( \alpha^k = \varepsilon = \beta^k \).

Since \( \alpha, \beta \) disjoint, they commute, so

\[ (\alpha \beta)^k = \alpha^k \beta^k = \varepsilon \varepsilon = \varepsilon \]

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

\[ \alpha^t \neq \beta^{-t} \text{ (since they are disjoint and at least one is not } \varepsilon \text{ since } 0 < t < k) \]

thus \( \alpha^t \beta^{-t} \neq \varepsilon \) and so \( (\alpha \beta)^t = \alpha^t \beta^{-t} \neq \varepsilon \). \[ \square \]

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

**Ex:** List all possible orders for elements of \( S_6 \).

The identity has order 1. All other elements can be written as a product of disjoint cycles each having length at least 2, and the sum of their lengths at most 6 (since the cycles must partition the set \( \{1,2,3,4,5,6\} \)). We list all possibilities:
• the identity  
• a 6-cycle  
• a 5-cycle  
• a 4-cycle  
• a 4-cycle & a 2-cycle  
• a 3-cycle  
• a 3-cycle & a 2-cycle  
• a 3-cycle & a 3-cycle  
• a 2-cycle  
• a 2-cycle & a 2-cycle  
• a 2 cycle & a 2-cycle & a 2 cycle  

So $\text{order of } a = 6 \in S_6 = \{1, 2, 3, 4, 5, 6\}$

(See Example 5 in the book for something more interesting)

**Ex:** How many elements in $S_6$ have order 6?

By previous example, the elements in $S_6$ of order 6 are 6-cycles and products of a 3-cycle and a distant 2-cycle.

There are 6! ways to order the numbers 1 through 6, and each such ordering describes a 6-cycle. However, each 6-cycle $(a_1 a_2 \cdots a_6)$ can be written in 6 ways:

$(a_1 a_2 \cdots a_6) = (a_2 a_3 \cdots a_6 a_1) = \cdots = (a_5 a_6 a_1 \cdots a_4)$

So $\# \text{ of 6-cycles} = \frac{6!}{6} = 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$
Similarly,

# of ways of choosing an ordered sequence of 3 elements from 1 through 6

\[ \frac{6 \cdot 5 \cdot 4}{3} \cdot \frac{3 \cdot 2}{2} = 120 \]

\begin{itemize}
  \item every 3-cycle can be written in 3 ways
  \item every 2-cycle can be written in 2 ways
\end{itemize}

Therefore, \( S_6 \) has 120 + 120 = \( 240 \) elements having order 6.

Then 5.4: Every \( a \in S_n \) (with \( n \geq 1 \)) can be written as a product of 2-cycles.

**Proof:** \( a \) can be written as a product of disjoint cycles (Thm 5.2). So it suffices to check every cycle can be written as a product of 2-cycles. Indeed, one can directly verify that

\[ (a_1 a_2 \ldots a_m) = (a_1 a_m)(a_2 a_{m-1}) \cdots (a_{m-1} a_2). \]

**Ex:** \((51324) = (54)(52)(53)(51)\)

Any given permutation can be written as a product of 2-cycles in many ways. However:

**Lemma:** If \( \xi = \beta_1 \beta_2 \ldots \beta_r \) where each \( \beta_i \) is a 2-cycle, then \( r \) is even.
Thm 5.5: Every permutation of a finite set can be written as a product of an even number of 2-cycles or a product of an odd number of 2-cycles, but not both.

Proof: Towards a contradiction, suppose there is a permutation $\sigma$ and 2-cycles $\beta_1, \ldots, \beta_r, \chi_1, \ldots, \chi_s$ with $\beta_1 \beta_2 \cdots \beta_r = \chi_1 \chi_2 \cdots \chi_s$, $r$ even, and $s$ odd. Then

$$e = \beta_r^{-1} \beta_{r-1}^{-1} \cdots \beta_1^{-1} \chi_1 \chi_2 \cdots \chi_s$$

and $r+s$ is odd, contradicting the above lemma $\square$

Def: A permutation is
- even if it can be written as a product of an even number of 2-cycles
- odd if it can be written as a product of an odd number of 2-cycles

Thm 5.6: The set of even permutations in $S_n$ form a subgroup of $S_n$.

Proof: We'll use one-step subgroup test. $e$ is even by lemma, so set of even permutations is nonempty.
Next suppose \( \alpha, \beta \) are even permutations. This means there are 2-cycles \( \tau_1, \ldots, \tau_r \), \( S_1, \ldots, S_s \) with \( r \) is even and
\[
\alpha = \tau_1 \cdots \tau_r, \quad \beta = S_1 \cdots S_s.
\]
Then
\[
\alpha \beta^{-1} = \tau_1 \tau_2 \cdots \tau_r (S_1 S_2 \cdots S_s)^{-1} = \tau_1 \tau_2 \cdots \tau_r S_1 S_2 \cdots S_s \quad \text{(each inverse is a 2-cycle)}
\]
Since \( r+s \) is even, \( \alpha \beta^{-1} \) is an even permutation \( \Box \)

**Defn.** The group of even permutations of \( \{1, 2, \ldots, n\} \) is denoted \( A_n \) and called the alternating group of degree \( n \).

**Thm 5.7** \( A_n \) has order \( \frac{n!}{2} \).

**Pr.** Define \( f : S_n \to S_n \) by \( f(\sigma) = (12) \sigma \). Then \( f \) is a bijection, and it takes even permutations to odd permutations and odd permutations to even permutations. So
\[
\# \text{ even permutations} = \# \text{ odd permutations}
\]
and therefore \( |A_n| = \frac{1}{2} |S_n| = \frac{1}{2} (n!) \) \( \Box \)