A is a nonempty set.

Let $S_n$ be the set of all permutations of the set $A$.

Special Case: $A = \{1, 2, \ldots, n\}$ we denote $S_n$ by $S_n$.

Example

$n = 3$

$S_3$ is the set of 6 $\binom{3}{2} = 6$ permutations of $\{1, 2, 3\}$.

\[
\begin{align*}
(1 \ 2 \ 3) & \quad (1 \ 3 \ 2) & \quad (2 \ 1 \ 3) & \quad (1 \ 2 \ 3) & \quad (1 \ 3 \ 2) & \quad (2 \ 3 \ 1) \\
(1 \ 2 \ 3) & \quad (2 \ 1 \ 3) & \quad (2 \ 3 \ 1) & \quad (1 \ 3 \ 2) & \quad (1 \ 2 \ 3) & \quad (3 \ 2 \ 1) \\
\end{align*}
\]

Second

\[
\begin{array}{ccccccc}
\ell_0 & \ell_1 & \ell_2 & \ell_3 & \ell_4 & \ell_5 & \ell_6 \\
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 \\
L_1 & L_0 & L_2 & L_3 & L_4 & L_5 & L_6 \\
L_2 & L_1 & L_0 & L_3 & L_4 & L_5 & L_6 \\
L_3 & L_2 & L_1 & L_0 & L_4 & L_5 & L_6 \\
L_4 & L_3 & L_2 & L_1 & L_0 & L_5 & L_6 \\
L_5 & L_4 & L_3 & L_2 & L_1 & L_0 & L_6 \\
L_6 & L_5 & L_4 & L_3 & L_2 & L_1 & L_0 \\
\end{array}
\]

\[
\begin{align*}
\ell_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} \\
\ell_1 \ell_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \ell_0 \\
\ell_1 \ell_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \ell_0 \\
\ell_2 \ell_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \ell_1 \\
\ell_2 \ell_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \ell_2 \\
\end{align*}
\]
Lemma. Let \( f : A \rightarrow A \) and \( g : A \rightarrow A \) which is both one-to-one and onto \( A \).

Then \( f \circ g : A \rightarrow A \) is one-to-one and onto \( A \).

Proof (one-to-one): Suppose that \( x, y \in A \) and that \( (f \circ g)(x) = (f \circ g)(y) \). We must show that \( x = y \).

So \( f(g(x)) = f(g(y)) \).

Since \( f : A \rightarrow A \) is one-to-one, it must be that \( g(x) = g(y) \). Since \( g \) is one-to-one, it must be that \( x = y \).

(onto) Let \( y \in A \) be given to us. We must show that there is an \( x \in A \) such that \( (f \circ g)(x) = y \). Since \( f : A \rightarrow A \) is onto \( A \), there is a \( b \in A \) such that \( f(b) = y \). Since \( g : A \rightarrow A \) is onto \( A \), there is a \( x \in A \) such that \( g(x) = b \).

Then \( (f \circ g)(x) = f(g(x)) = f(b) = y \), as required.

Corollary. Function composition is a binary operation on \( S_\mathbb{A} \).

We are trying to show that \( S_\mathbb{A} \) is a group under composition.

By the corollary, function composition is a binary operation on \( S_\mathbb{A} \). Composition of functions is always associative.
Let \( 1_A : A \to A \) where \( 1_A(x) = x \) for every \( x \in A \).

It's clear that for any \( \sigma \in S_A \) that
\[ 1_A \circ \sigma = \sigma = \sigma \circ 1_A \]

Finally if \( \sigma : A \to A \) is both one-to-one and onto \( A \) then \( \sigma \) has an inverse function \( \sigma^{-1} \) which is both one-to-one and onto.

Corollary: If \( A \) is any nonempty set then \( S_A \) is a group under function composition.

Lemma: Let \( G \) and \( G' \) be groups and let \( \theta : G \to G' \) where \( \theta(xy) = \theta(x) \theta(y) \) for all \( xy \in G \).

Then if \( H \) is a subgroup of \( G \) then \( \theta(H) = \{ \theta(h) \mid h \in H \} \) is a subgroup of \( G' \).

Proof: We must show that \( \theta(H) \) is a subgroup of \( G' \).

Consider \( e_G \) and \( e_G' \) be the identity elements of \( G \) and \( G' \) respectively.

Claim that \( \theta(e_G) = e_G' \). Let \( x \in G \).

Then \( \theta(x e_G) = \theta(x) \theta(e_G) \)

\( \theta(x) \) = \( x \)
So \( \theta(x) = \theta(x) \theta(e_a) \)

\[
[\theta(x)]^{-1} \theta(x) = [\theta(x)] \theta(x) \theta(e_a)
\]

\[
e_{G_1} = \theta(e_a)
\]

\[
e_{G_1} = \theta(e_a)
\]

Since \( H \) is a subgroup of \( G_1, e_{G_1} \in H \)

\[
\Rightarrow \theta(e_{G_1}) \in \theta(H) \Rightarrow e_{G_1} \in \theta(H).
\]

Let \( \theta(h_1) \) and \( \theta(h_2) \) be elements of \( \theta(H) \) where \( h_1, h_2 \in H \), we want to show \( \theta(h_1) \theta(h_2) \in \theta(H) \).

So \( \theta(h_1) \theta(h_2) = \theta(h_1 h_2) \) and \( h_1 h_2 \in H \)

because \( h_1, h_2 \in H \) and \( H \) is a subgroup of \( G_1 \). Let \( \theta(h) \in \theta(H) \) where \( h \in H \).

We must prove that \( [\theta(h)]^{-1} \in \theta(H) \), since \( h \in H \) and since \( H \) is a subgroup of \( G_1 \), it's true that \( h^{-1} \in H \). Claim that \( [\theta(h)]^{-1} = \theta(h^{-1}) \).

Now \( \theta(h) \theta(h^{-1}) = \theta(h h^{-1}) = \theta(e_{G_1}) = \theta(e_{G_1}) \theta(h) \)

Therefore \( [\theta(h)]^{-1} = \theta(h^{-1}) \in \theta(H) \), and we are done.