PERMUTATIONS

1. The Permutations $S_n$

Suppose that $n \geq 2$ is an integer. $S_n = \text{Perm}\{1, 2, \ldots, n\}$ is the set of permutations (bijective mappings) of the set $\{1, 2, \ldots, n\}$. $S_n$ is a group under composition of mappings. $S_n$ is called the symmetric group on $n$ letters.

If $\{x_1, \ldots, x_n\}$ is any set with $n$ objects, then $S_n$ is isomorphic to $\text{Perm}\{x_1, \ldots, x_n\}$ by the isomorphism $\Lambda : S_n \to \text{Perm}\{x_1, \ldots, x_n\}$ which takes $\sigma \in S_n$ to $\Lambda(\sigma)$ defined by $\Lambda(\sigma)(x_i) = x_j$ if $\sigma(i) = j$.

A transposition is a permutation $\tau \in S_n$ which interchanges two elements of $\{1, 2, \ldots, n\}$ and leaves every other element of $\{1, 2, \ldots, n\}$ fixed. If $\tau$ is a transposition, we have that $\tau^{-1} = \tau$ and $\tau^2 = \text{id}$.

**Theorem 1.1.** Every permutation in $S_n$ is a product of transpositions.

**Proof.** We will prove this by induction on $n$, first verifying this for $S_2$. $S_2$ consists of the identity map $\text{id}$ and the transposition $\tau$ which interchanges 1 and 2. Since $\tau^2 = \text{id}$, every element of $S_2$ is a product of transpositions.

Now suppose that $n \geq 2$ and every element of $S_n$ is a product of transpositions. Suppose that $\sigma \in S_{n+1}$. If $\sigma = \text{id}$, then $\sigma = \lambda^2$ where $\lambda$ is the permutation which interchanges 1 and 2. Suppose that $\sigma \neq \text{id}$. Then there exist $i, j \in \{1, 2, \ldots, n+1\}$ with $i \neq j$ such that $\sigma(i) = \sigma(j)$. Let $\tau$ be the tranposition which interchanges $i$ and $j$. Then $\tau\sigma(i) = \tau(j) = i$.

Thus $\tau\sigma$ restricts to a permutation of the subset $U$ of $\{1, \ldots, n+1\}$ obtained by removing $i$ from the set $\{1, \ldots, n+1\}$. Since $U$ has $n$ elements, $\text{Perm}(U) \cong S_n$. Thus, by induction, $\tau\sigma$ is a product of transpositions of elements in the set $U$. Thus $\sigma = \tau(\tau\sigma)$ is a product of transpositions. \qed

We now define a mapping $\Psi : S_n \to \text{Gl}_n(\mathbb{R})$ by defining for $\sigma \in S_n$, $\Psi(\sigma)$ to be the matrix $A_\sigma$ obtained by interchanging the rows of the identity matrix $I_n$ as prescribed by the permutation. That is, the $i$-th row of $I_n$ is the $\sigma(i)$-th row of $A_\sigma$.

**Lemma 1.2.** Suppose that $\sigma \in S_n$ and $(x_1, \ldots, x_n)^t \in \mathbb{R}^n$. Then

\[
(1) \quad A_\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}.
\]

**Proof.** Let $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A_\sigma \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.
$A_\sigma$ takes the $i$-th row of $(x_1, \ldots, x_n)^t$ to the $\sigma(i)$-th row of $(y_1, \ldots, y_n)^t$. Thus $y_{\sigma(i)} = x_i$ for $1 \leq i \leq n$. Setting $j = \sigma(i)$, we have $\sigma^{-1}(j) = i$. Thus $y_j = x_{\sigma^{-1}(i)}$ for $1 \leq i \leq n$. □

An example is $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$. We have that $A_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, and

$$A_\sigma \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}.$$  

**Lemma 1.3.** Suppose that $\sigma, \tau \in S_n$ and $(x_1, \ldots, x_n)^t \in \mathbb{R}^n$. Then

(2) $A_{\sigma \tau} = A_\sigma A_\tau$.

**Proof.** Set

$$y_j = x_{\tau^{-1}(j)} \text{ for } 1 \leq j \leq n.$$  

Substituting $j = \sigma^{-1}(i)$, we obtain the formula

$$y_{\sigma^{-1}(i)} = x_{\tau^{-1}\sigma^{-1}(i)}.$$  

We have

$$A_{\sigma \tau} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{(\sigma \tau)^{-1}(1)} \\ \vdots \\ x_{(\sigma \tau)^{-1}(n)} \end{pmatrix} = \begin{pmatrix} x_{\tau^{-1}\sigma^{-1}(1)} \\ \vdots \\ x_{\tau^{-1}\sigma^{-1}(n)} \end{pmatrix} = \begin{pmatrix} y_{\sigma^{-1}(1)} \\ \vdots \\ y_{\sigma^{-1}(n)} \end{pmatrix} = A_\sigma \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A_\sigma \begin{pmatrix} x_{\tau^{-1}(1)} \\ \vdots \\ x_{\tau^{-1}(n)} \end{pmatrix} = A_\sigma A_\tau \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$  

Since this equality holds for all $(x_1, \ldots, x_n)^t \in \mathbb{R}^n$, we have that $A_{\sigma \tau} = A_\sigma A_\tau$. □

By Lemma 1.3, $\Psi : S_n \to \text{GL}_n(\mathbb{R})$ is a group homomorphism.

Now, for $\sigma \in S_n$, $A_\sigma = I_n$ if and only if $\sigma$ is the identity permutation id. Thus the kernel of $\Psi$ is $\{\text{id}\}$, and thus $\Psi$ is a 1-1 group homomorphism. Thus $S_n$ is isomorphic to the image of $S_n$ by $\Phi$, which is a subgroup of $\text{GL}_n(\mathbb{R})$.

**Theorem 1.4.** Suppose that $\sigma \in S_n$, and

$$\sigma = \alpha_1 \cdots \alpha_a,$$

$$\sigma = \beta_1 \cdots \beta_b$$

are two factorizations of $\sigma$ as a product of transpositions. then

$$a \equiv b \mod 2.$$  

**Proof.** We have

(3) $A_{\alpha_1} A_{\alpha_2} \cdots A_{\alpha_a} = A_{\alpha_1 \cdots \alpha_a} = A_\sigma = A_{\beta_1 \cdots \beta_b} = A_{\beta_1} A_{\beta_2} \cdots A_{\beta_b}$. 

Now for any transposition $\tau \in S_n$, $A_{\tau}$ is the elementary matrix obtained from $I_n$ by interchanging two rows of the identity matrix. Thus
\[
\det(A_{\tau}) = -1.
\]
Using the fact that the determinant preserves multiplication ($\det : \text{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ is a group homomorphism), we have from (3) that
\[
(-1)^a = \det(A_{\alpha_1}) \cdots \det(A_{\alpha_a}) = \det(A_{\sigma}) = \det(A_{\beta_1}) \cdots \det(A_{\beta_b}) = (-1)^b.
\]

**Definition 1.5.** Suppose that $\sigma \in S_n$ then we define $\text{sgn} (\sigma)$, the sign of $\sigma$, to be 1 if $\sigma$ can be expressed as a product of an even number of transpositions and the sign of $\sigma$ to be $-1$ if $\sigma$ can be expressed as a product of an odd number of transpositions.

This definition is well defined; every $\sigma$ can be expressed as some product of transpositions by Theorem 1.1. Given two different expressions of $\sigma$ as a product of transpositions, they have the same sign by Theorem 1.4.

**Lemma 1.6.** Suppose that $\sigma, \tau \in S_n$. Then
\[
\text{sgn}(\sigma \tau) = \text{sgn}(\sigma)\text{sgn}(\tau).
\]

**Proof.** Let
\[
\sigma = \alpha_1 \cdots \alpha_a
\]
and
\[
\tau = \beta_1 \cdots \beta_b
\]
where $a, b \in \mathbb{Z}_+$ be factorizations of $\sigma$ and $\tau$ as products of transpositions. Then
\[
\sigma \tau = \alpha_1 \cdots \alpha_a \beta_1 \cdots \beta_b
\]
expresses $\sigma \tau$ as a product of $a + b$ transpositions. We have
\[
\text{sgn}(\sigma \tau) = (-1)^{a+b} = (-1)^{a}(-1)^{b} = \text{sgn}(\sigma)\text{sgn}(\tau).
\]

Suppose that $\sigma \in S_n$. $\sigma$ is called an $r$-cycle if we can write $\{1, \ldots, n\} = A \cup B$, where $A = \{i_1, \ldots, i_r\}$ is a set of $r$ elements (and $B$ is a set of $n - r$ elements), and such that
\[
\sigma(i_1) = i_2, \sigma(i_2) = i_2, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1,
\]
and
\[
\sigma(j) = j \text{ if } j \in B.
\]
We use the notation $\sigma = (i_1, i_2, \ldots, i_r)$ to represent an $r$-cycle.

**Lemma 1.7.** Suppose that $\sigma$ is an $r$-cycle. Then the order of $\sigma$ is $o(\sigma) = r$.

**Proof.** Write $\sigma = (i_1, i_2, \ldots, i_r)$ for some (distinct) elements $i_1, \ldots, i_r \in \{1, \ldots, i_n\}$. Let $A = \{i_1, \ldots, i_r\}$. Suppose that $k \in \{1, \ldots, i_n\} \setminus A$. Then $\sigma(k) = k$, so that for any $s \geq 1$, (4)
\[
\sigma^s(k) = k \text{ if } k \in \{1, \ldots, i_n\} \setminus A.
\]
Suppose that $1 \leq i \leq r$. Then
\[
\sigma(i_j) = \begin{cases} 
  i_{j+1} & \text{if } 1 \leq j \leq r-1 \\
  i_1 & \text{if } j = r.
\end{cases}
\]
Thus

\[ \sigma^s(i_j) = \begin{cases} 
    i_{s+j} & \text{if } 1 \leq s \leq r - j \\
    i_{s-r+j} & \text{if } r - j < s \leq r
  \end{cases} \]

It follows that \( \sigma^r(i_j) = i_j \) if \( 1 \leq j \leq r \). Thus \( \sigma^r(k) = k \) if \( k \in A \). By (4), \( \sigma^r(k) = k \) if \( k \notin \{1, \ldots, n\} \setminus A \). Thus \( \sigma^r = \text{id} \).

If \( s \) is such that \( 1 \leq s < r \), then \( \sigma^s(i_1) = i_{s+1} \neq i_1 \) so \( \sigma^s \neq \text{id} \). Thus \( r \) is the smallest positive integer \( t \) such that \( \sigma^t = \text{id} \). By the definition of the order \( o(\sigma) \), we have that \( o(\sigma) = r \). \( \square \)

Two permutations \( \sigma \) and \( \tau \) are said to be disjoint if \( \sigma(i) = i \) whenever \( \tau(i) \neq i \) and \( \tau(i) = i \) whenever \( \sigma(i) \neq i \).

**Lemma 1.8.** Suppose that \( \sigma, \tau \in S_n \) are disjoint permutations. Then \( \sigma \tau = \tau \sigma \).

**Theorem 1.9.** Suppose that \( \sigma \in S_n \). Then \( \sigma \) can be expressed as a product of disjoint cycles. The expression is unique up to permuting the factors.

The proof of the theorem is by a simple algorithm to construct the factorization. As an example, we factor \( \sigma = (1, 2, 3, 4, 5, 6, 7) \) as \( \sigma = (1, 3, 6)(2, 4)(5, 7) \).

**Lemma 1.10.** Suppose that \( \sigma = (i_1 i_2 \cdots i_k) \in S_n \) is a \( k \)-cycle. Then

\[ \sigma = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2). \]

Theorem 1.9 and Lemma 1.10 give an algorithm to construct an explicit factorization of a permutation as a product of transpositions.

2. **The Alternating Group**

We have a mapping

\[ \Sigma : S_n \rightarrow U_2 = \{ \pm 1 \}, \]

defined by \( \Sigma(\sigma) = \text{sgn}(\sigma) \) for \( \sigma \in S_n \). By Lemma 1.6, \( \Sigma \) is a homomorphism. \( \Sigma \) is onto since \( \Sigma(\tau) = -1 \) if \( \tau \) is a transposition.

The kernel of \( \Sigma \) is

\[ A_n = \{ \sigma \in S_n \mid \text{sgn}(\sigma) = 1 \}. \]

\( A_n \) is a normal subgroup of \( S_n \) (since it is the kernel of \( \Sigma \)). \( A_n \) is called the alternating group on \( n \) letters. \( \Sigma \) induces an isomorphism of \( S_n/A_n \) with \( U_2 \), which is isomorphic to \( \mathbb{Z}_2 \).

**Theorem 2.1.** Suppose that \( n \geq 3 \) and \( \sigma \in A_n \). Then \( \sigma \) is a product of 3-cycles.

**Proof.** Since \( \sigma \) is a product of an even number of transpositions, it suffices to prove the theorem in the case when \( \sigma \) is a product of two 2-cycles. One of the following three cases then holds:

1. \( \sigma = (a, b)(a, b) \) for some \( a, b \in \{1, \ldots, a_n\} \) with \( a \neq b \).
2. \( \sigma = (a, b)(b, c) \) for some \( a, b, c \in \{1, \ldots, a_n\} \) with \( a, b, c \) distinct.
3. \( \sigma = (a, b)(c, d) \) for some \( a, b, c, d \in \{1, \ldots, a_n\} \) with \( a, b, c, d \) distinct.
Suppose that $\sigma$ is in case 1. Then $\sigma = \text{id} = (132)(123)$ is a product of 3-cycles. Suppose that $\sigma$ is in case 2. Then $\sigma = (abc)$. Suppose that $\sigma$ is in case 3. Then
\[
\sigma = (ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)
\]
is a product of 3-cycles. □