1.6 Symmetric, Alternating, and Dihedral Groups

1.6.1 Symmetric groups $S_n$

Denote $I_n := \{1, 2, \ldots, n\}$. The symmetric group $S_n$ is the group of all bijections $I_n \to I_n$ with functional composition operation.

**Def.** Fix $n$. Given distinct elements $i_1, \ldots, i_r \in \{1, \ldots, n\}$, we use $(i_1i_2\cdots i_r)$ to denote the permutation that maps $i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_r \mapsto i_1$. $(i_1i_2\cdots i_r)$ is called an $r$-cycle, and $r$ is the order or the length of this cycle. A 2-cycle is called a transposition.

**Def.** The permutations $\sigma_1, \ldots, \sigma_r$ of $S_n$ are said to be disjoint provided that for each $k \in I_n$, there is at most one $r \in I_r$ such that $\sigma_i(k) \neq k$.

**Thm 1.22.** Every nonidentity permutation in $S_n$ is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.

**Ex.** In $S_6, (1\ 2\ 3\ 4\ 5\ 6)$ can be expressed as $(1\ 2\ 4)(3\ 5)$.

**Sketch of Proof of Theorem 1.22.** Let $\sigma \in S_n$ be the nonidentity permutation. Define a relationship in $I_n$, such that $i \sim j$ in $I_n$ if and only if $\sigma^k(i) = j$ for some $k \in \mathbb{Z}$. Then $\sim$ is an equivalent relationship. So $I_n$ is partitioned into $\sim$ equivalence classes. Each class has finitely many elements. Suppose $S := \{i_1, \ldots, i_r\}$ is a $\sim$ equivalent class. Then $i_1, \sigma(i_1), \sigma^2(i_1), \ldots$, are elements of $S$. There is a minimal $t \in \mathbb{Z}^+$ such that $\sigma^t(i_1) = \sigma^{t+s}(i_1)$ for some $s \in \{1, 2, \ldots, t\}$. Since $\sigma$ is a bijection, we have $\sigma^k(i_1) = \sigma^{k+s}(i_1)$ for any integer $k \geq 0$, and $S = \{i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{s-1}(i_1)\}$. Then $\sigma$ is the product of disjoint cycles $(i_1 \sigma(i_1) \sigma^2(i_1) \cdots \sigma^{s-1}(i_1))$ produced from these equivalent classes. We may omit the 1-cycles.

The uniqueness is easily seen from the uniqueness of the partition. \qed

**Cor 1.23.** The order of a permutation $\sigma \in S_n$ is the least common multiple of the orders of its disjoint cycles.

Two permutations $\sigma_1, \sigma_2 \in S_n$ are conjugate in $S_n$ if there exists a permutation $g \in S_n$ such that $g\sigma_1g^{-1} = \sigma_2$. Given two cycles of the same length in $S_n$, say $\sigma_1 = (a_1a_2\cdots a_r)$ and $\sigma_2 = (b_1b_2\cdots b_r)$, let $g \in S_n$ be the permutation that sends $a_i$ to $b_i$ for $i = 1, 2, \ldots, r$. Then $g\sigma_1g^{-1} = \sigma_2$. Conversely, every permutation that conjugates to $\sigma_1$ in $S_n$ is a cycle of the same length as $\sigma_1$.

**Cor 1.24.** Two permutations $\alpha, \beta \in S_n$ are conjugate in $S_n$ if and only if they have the same cycle structure.

A cycle can be expressed as a product of transpositions by the way that $(x_1) = (x_1x_2)(x_1x_2)$ and $(x_1x_2\cdots x_r) = (x_1x_r)(x_1x_{r-1}) \cdots (x_1x_3)(x_1x_2)$. Then we have the following result.

**Cor 1.25.** Every permutation in $S_n$ can be written as a product of (not necessarily disjoint) transpositions.
1.6.2 Alternating groups $A_n$

**Def.** A permutation is said to be even [resp. odd] if it can be written as a product of even [resp. odd] number of transpositions.

**Thm 1.26.** A permutation in $S_n$ ($n \geq 2$) cannot be both even and odd.

**Proof.** We use matrix theory to prove it. Denote $e_i := (0, 0, \cdots, 1_{i\text{-th term}}, \cdots, 0)$ in $\mathbb{R}^n$. Let $W_n$ be the set of $n \times n$ permutation matrices, i.e. matrices each of whose columns and rows consists of exactly one nonzero entry 1. Define $f : S_n \rightarrow W_n$ by $\sigma \mapsto P_\sigma$, where the $i$-th row of $P_\sigma$ is $e_{\sigma(i)}$. It is easy to check that $f$ is a group isomorphism. Moreover, $\det : W_n \rightarrow \{\pm 1\}$ is a group homomorphism. So $\det \circ f : S_n \rightarrow \{\pm 1\}$ is a group homomorphism. Obviously, $\det \circ f ((ab)) = -1$ for every transposition $(ab) \in S_n$. Hence for $\sigma \in S_n$, it is a product of even [resp. odd] number of transpositions if and only if $\det \circ f (\sigma) = 1$ [resp. $\det \circ f (\sigma) = -1$].

**Thm 1.27.** The set $A_n$ of all even permutations of $S_n$ forms a subgroup of $S_n$ of index 2.

So $A_n$ is a normal subgroup of $S_n$ with $|A_n| = n!/2$. $A_n$ is called the alternating group on $n$ letters.

**Lem 1.28.** Let $r, s$ be distinct elements of $\{1, 2, \cdots, n\}$. Then $A_n$ ($n \geq 3$) is generated by the 3-cycles $\{(rsk) | 1 \leq k \leq n, k \neq r, s\}$.

**Proof.** Every element of $A_n$ is a product of even numbers of transpositions. Since

$$(ab)(cd) = (acb)(acd), \quad (ab)(ac) = (acb),$$

$A_n$ is generated by all 3-cycles. A 3-cycle is of the form

$$\begin{align*}
(ras) &= (rsa)^2, \\
(rab) &= (rsb)(rsa)^2, \\
(sab) &= (rsb)^2(rsa), \\
\text{or} \quad (abc) &= (rsa)^2(rsc)(rsb)^2(rsa).
\end{align*}$$

This shows that $A_n$ is generated by $\{(rsk) | 1 \leq k \leq n, k \neq r, s\}$. □

**Lem 1.29.** If $N$ is a normal subgroup of $A_n$ ($n > 3$) and $N$ contains a 3-cycle, then $N = A_n$.

**Proof.** If $(abc) \in N$, then for any $d \neq a, b, c$,

$$(abd) = (ab)(cd)(abc)^2(cd)(ab) = [(ab)(cd)(abc)^2](ab)(cd)^{-1} \in N.$$ 

So $N$ contains all 3-cycles. Thus $N = A_n$. □
1.6. SYMMETRIC, ALTERNATING, AND DIHEDRAL GROUPS

Def. A group $G$ is simple if $G$ has no proper normal subgroups.

Ex. A cyclic group is simple if and only if it is isomorphic to $\mathbb{Z}_p$ for some prime $p$.

Thm 1.30. The alternating group $A_n$ is simple when $n \neq 4$.

See textbook (Section 1.6) for a complete proof. The key idea is to show that every non-proper normal subgroup of $A_n$ contains a 3-cycle.

1.6.3 Dihedral group $D_n$

The subgroup of $S_n$ generated by $a = (123 \cdots n)$ and $b = (2n)(3(n - 1)) \cdots (i(n + 2 - i)) \cdots$ is called the dihedral group of degree $n$, denoted $D_n$. It is isomorphic to the group of all symmetries of a regular $n$-gon.

Thm 1.31. The dihedral group $D_n$ ($n \geq 3$) is a group of order $2n$ whose generators $a$ and $b$ satisfy:

1. $a^n = b^2 = e; a^k \neq e$ if $0 < k < n$;
2. $ba = a^{-1}b$. 