Section I.6. Symmetric, Alternating, and Dihedral Groups

Note. In this section, we conclude our survey of the group theoretic topics which are covered in Introduction to Modern Algebra (MATH 4127/5127). We formally define several finite groups.

Definition I.6.1. Let \(i_1, i_2, \ldots, i_r\) (where \(r \leq n\)) be distinct elements of \(I_n = \{1, 2, \ldots, n\}\). Then \((i_1, i_2, \cdots, i_r)\) denotes the permutation that maps \(i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{r-1} \mapsto i_r, \) and \(i_r \mapsto i_1,\) and maps every other element of \(I_n\) onto itself. \((i_1, i_2, \cdots, i_r)\) is a cycle of length \(r;\) a 2-cycle is called a transposition.

Note. We multiply cycles by reading right to left, as we did in Section I.1:

\[(1, 2, 4, 3)(1, 2, 3) = (1, 4, 3, 2),\]

\[(1, 2, 3, 4)(4, 3, 2, 1) = (1)(2)(3)(4) = \iota.\]

Notice that in general, the inverse of \((i_1, i_2, \ldots, i_r)\) is \((i_r, i_{r-1}, \ldots, i_1)\).

Definition I.6.2. The permutations \(\sigma_1, \sigma_2, \ldots, \sigma_r\) of \(S_n\) are disjoint if for each \(1 \leq i \leq r\) and every \(k \in I_n,\) we have that \(\sigma_i(k) \neq k\) implies \(\sigma_j(k) = k\) for all \(j \neq i.\)
Note. When we use the notation of Definition I.6.1, we see that two or more cycles (of length greater than 1) are disjoint if and only if their cyclic notations do not share any elements. Any conversation of cycles and disjointness must be held in the context of some symmetric group $S_n$.

Note. The following result has played a role in some of my research in “automorphisms of Steiner triple systems.”

**Theorem I.6.3.** 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.

Note. Theorem I.6.3 allows us to classify a permutation according to its type. The *type* of permutation $\pi \in S_n$ is $[\pi] = [p_1, p_2, \ldots, p_n]$ if the disjoint cyclic decomposition of $\pi$ contains $p_i$ cycles of length $i$. For example, if $\pi$ is simply a cycle of length $n$, then $[\pi] = [0, 0, \ldots, 0, 1]$. If $\pi$ is the identity consisting of $n$ fixed points, then $[\pi] = [n, 0, 0 \ldots, 0]$. Notice that we have $n = \sum_{i=1}^{n} ip_i$. In studies of automorphisms of combinatorial designs, certain permutations are given special attention. A permutation of type $[0, 0, \ldots, 0, 1]$ is called *cyclic*. A permutation of type $[0, 0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0]$ or $[0, 0, \ldots, 0, 2, 0, \ldots, 0]$ is called *bicyclic*. A permutation of type $[f, (n-f)/2, 0, 0, \ldots, 0]$ is called an *involution* since its square is the identity.
Corollary I.6.4. The order of a permutation $\sigma \in S_n$ is the least common multiple of the orders of its disjoint cycles.

Corollary I.6.5. Every permutation in $S_n$ can be written as a product of (not necessarily disjoint) transpositions.

Note. There is not a unique way to represent a cycle as a product of transpositions:

$$(1, 2, 3) = (1, 3)(1, 2) = (1, 3)(1, 2)(1, 2)(1, 2)$$

However, there is a parameter preserved when writing a cycle as a product of transpositions.

Definition I.6.6. A permutation $\tau \in S_n$ is said to be even (respectively, odd) if $\tau$ can be written as a product of an even (respectively, odd) number of transpositions. The sign of a permutation $\tau$, denoted $\text{sgn}(\tau)$, is 1 or $-1$ according as to $\tau$ is even or odd, respectively.

Theorem I.6.7. A permutation in $S_n$ ($n \geq 2$) cannot be both even and odd.

Proof. Let $i_1, i_2, \ldots, i_n$ be the integers $1, 2, \ldots, n$ in some order and define

$$\Delta(i_1, i_2, \ldots, i_n) = \prod_{1 \leq j < k \leq n} (i_j - i_k).$$

Since we require $j < k$, we have $i_j - i_k \neq 0$ for all admissible $j$ and $k$. So
\[ \Delta(i_1, i_2, \ldots, i_n) \neq 0. \]

We first compute \( \Delta(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_n)) \) for \( \sigma \in S_n \) a transposition, say \( \sigma = (i_c, i_d) \) where \( c < d \). Applying \( \sigma \) to \( i_1, i_2, \ldots, i_n \) produces

\[ i_1, i_2, \ldots, i_{c-1}, i_d, i_{c+1}, \ldots, i_{d-1}, i_c, i_{d+1}, \ldots, i_n. \]

Computing \( \Delta \) for the original sequence \( i_1, i_2, \ldots, i_c, \ldots, i_d, \ldots, i_n \) gives

\[
\prod_{j<k, j,k \neq c,d} (i_j - i_k) \text{ (all the admissible differences involving neither } i_c \text{ nor } i_d) \\
\times \prod_{j < c} (i_j - i_c) \text{ (admissible differences with } i_c \text{ on the right)} \\
\times \prod_{j < c} (i_j - i_d) \text{ (some admissible differences with } i_d \text{ on the right)} \\
\times \prod_{c < j < d} (i_j - i_d) \text{ (remaining differences with } i_d \text{ on the right)} \\
\times \prod_{c < k < d} (i_c - i_k) \text{ (some admissible differences with } i_c \text{ on the left)} \\
\times \prod_{d < k} (i_c - i_k) \text{ (remaining differences with } i_c \text{ on the left)} \\
\times \prod_{d < k} (i_d - i_k) \text{ (admissible differences with } i_d \text{ on the left)} \\
\times (i_c - i_d) \text{ (since none of the above differences involve both } i_c \text{ and } i_d) \\
= (i_c - i_d)ABCDEFG \text{ where}
\]

\[
A = \prod_{j<k, j,k \neq c,d} (i_j - i_k); \quad B = \prod_{j < c} (i_j - i_c); \quad C = \prod_{j < c} (i_j - i_d); \\
D = \prod_{c < j < d} (i_j - i_d); \quad E = \prod_{c < k < d} (i_c - i_k); \quad F = \prod_{d < k} (i_c - i_k); \\
G = \prod_{d < k} (i_d - i_k).
\]

Denote

\[
\sigma(A) = \prod_{j<k, j,k \neq c,d} (\sigma(i_j) - \sigma(i_k))
\]
and similarly $\sigma(B), \sigma(C), \sigma(D), \sigma(E), \sigma(F)$, and $\sigma(G)$. Then we have

- $\sigma(A) = A$ since neither $i_c$ nor $i_d$ are involved.
- $\sigma(B) = C$ and $\sigma(C) = B$ since these involve interchanging $i_c$ in $B$ with $i_c$ in $C$.
- $\sigma(D) = (-1)^{d-c-1}E$ and $\sigma(E) = (-1)^{d-c-1}D$ since these involve interchanging $i_d$ in $D$ with $i_c$ in $E$ followed by $d - c - 1$ negative signs.
- $\sigma(F) = G$ and $\sigma(G) = F$ since these involve interchanging $i_c$ in $F$ with $i_d$ in $G$.

Finally, $\sigma(i_c - i_d)\sigma(i_c) - \sigma(i_d) = i_d - i_c = -(i_c - i_d)$. Consequently

$$\Delta(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_n)) = \Delta(i_1, i_2, \ldots, i_c-i_d, i_c-i_d, \ldots, i_d, i_d, \ldots, i_n)$$

$$= \prod_{j<k} (i_j - i_k) \text{ (all the admissible differences involving neither } i_c \text{ nor } i_d)$$
$$\times \prod_{j<c} (i_j - i_d) \text{ (admissible differences with } i_d \text{ on the right)}$$
$$\times \prod_{j<c} (i_j - i_c) \text{ (some admissible differences with } i_c \text{ on the right)}$$
$$\times \prod_{c<j<d} (-1)(i_c - i_j) \text{ (remaining differences with } i_c \text{ on the right)}$$
$$\times \prod_{c<k<d} (-1)(i_d - i_k) \text{ (some admissible differences with } i_d \text{ on the left)}$$
$$\times \prod_{d<k} (i_d - i_k) \text{ (remaining differences with } i_d \text{ on the left)}$$
$$\times \prod_{d<k} (i_c - i_k) \text{ (admissible differences with } i_c \text{ on the left)}$$
$$\times (i_c - i_d) \text{ (since none of the above differences involve both } i_c \text{ and } i_d)$$

$$= \sigma(A)\sigma(B)\sigma(C)\sigma(D)\sigma(E)\sigma(F)\sigma(G)\sigma(i_c - i_d)$$

$$= -(i_c - i_d)ACB(-1)^{d-c-1}E(-1)^{d-c-1}DGF$$
$$= -(i_c - i_d)ABCDEFG = -\Delta(i_1, i_2, \ldots, i_n).$$

So if one ordering of $1, 2, \ldots, n$ differs from another ordering by a transposition,
then the $\Delta$ values of these orderings differ by a negative sign.

**ASSUME** that for some $\tau \in S_n$, we have $\tau = \tau_1 \tau_2 \cdots \tau_r = \sigma_1 \sigma_2 \cdots \sigma_s$ with $\tau_i$ and $\sigma_j$ transpositions where $r$ is even and $s$ is odd. Then by the previous paragraph,

\[
\Delta(\tau(1), \tau(2), \ldots, \tau(n)) = \Delta((\tau_1 \tau_2 \cdots \tau_r)(1), (\tau_1 \tau_2 \cdots \tau_r)(2), \ldots, (\tau_1 \tau_2 \cdots \tau_r)(n))
\]

\[
= -\Delta((\tau_2 \tau_3 \cdots \tau_r)(1), (\tau_2 \tau_3 \cdots \tau_r)(2), \ldots, (\tau_2 \tau_3 \cdots \tau_r)(n))
\]

(dropping transposition $\tau_1$ which only affects two of the entries)

\[
= (-1)^{2r} \Delta((\tau_3 \tau_4 \cdots \tau_r)(1), (\tau_3 \tau_4 \cdots \tau_r)(2), \ldots, (\tau_3 \tau_4 \cdots \tau_r)(n))
\]

\[
= (-1)^s \Delta(1, 2, \ldots, n).
\]

Similarly

\[
\Delta(\tau(1), \tau(2), \ldots, \tau(n)) = \Delta((\sigma_1 \sigma_2 \cdots \sigma_s)(1), (\sigma_1 \sigma_2 \cdots \sigma_s)(2), \ldots, (\sigma_1 \sigma_2 \cdots \sigma_s)(n))
\]

\[
= (-1)^s \Delta(1, 2, \ldots, n).
\]

So we have shown that

\[
\Delta(\tau(1), \tau(2), \ldots, \tau(n)) = (-1)^r \Delta(1, 2, \ldots, n) = (-1)^s \Delta(1, 2, \ldots, n).
\]

Since $\Delta(1, 2, \ldots, n) \neq 0$ as shown above, then it must be that either both $r$ and $s$ are even or both $r$ and $s$ are odd, a CONTRADICTION. So the assumption that $r$ can be written as both an even number of transpositions and an odd number of transpositions is false.
Note. Notice that the proof of Theorem I.6.7 is really just an involved parity argument. Fraleigh gives two proofs of Theorem I.6.7, one based on linear algebra and the other based on counting cycles. Hungerford’s proof, you’ll notice, depends on very little background. It is the same proof given, for example, in Dummit and Foote’s Abstract Algebra, 3rd Edition (John Wiley and Sons, 2004).

**Theorem I.6.8.** For each $n \geq 2$, let $A_n$ be the set of all even permutations of $S_n$. Then $A_n$ is a normal subgroup of $S_n$ of index 2 and order $|S_n|/2 = n!/2$. Furthermore $A_n$ is the only subgroup of $S_n$ of index 2. The group $A_n$ is called the *alternating group* on $n$ letters.

**Definition I.6.9.** A group $G$ is said to be *simple* if $G$ has no proper normal subgroup.

Note. Any proper subgroup of an abelian group is normal. The only finite simple abelian groups are $\mathbb{Z}_p$ where $p$ is prime (this follows from exercise I.4.3 and the classification of finitely generated abelian groups [Theorem II.2.6]).

Note. The study of finite simple groups is fundamental to the study of finite groups. This is because, in a sense, all finite groups are composed of finite simple groups. This is spelled out more explicitly by the Jordan-Hölder Theorem (Theorem II.8.11 in Hungerford). For a relatively elementary discussion of finite simple groups and the 30 year program to classify them, as well as a statement of the classification theorem, see my notes from Introduction to Modern Algebra (MATH 4127/5127) on *Finite Simple Groups*. 
Note. In our next theorem, we show that $A_n$ is simple if and only if $n \neq 4$. Fraleigh covers this in an exercise (Exercise 15.39). A detailed solution to this is given in my online notes for Introduction to Modern Algebra (MATH 4127/5127) on The Alternating Groups $A_n$ are Simple for $n = 5$.

**Theorem I.6.10.** The alternating group $A_n$ is simple if and only if $n \neq 4$.

Note. We need two lemmas to prove Theorem I.6.10. The lemmas involve properties of 3-cycles in $S_n$.

**Lemma I.6.11.** Let $r$ and $s$ be distinct elements of $\{1, 2, \ldots, n\}$. Then $A_n$ (where $n \geq 3$) is generated by the 3-cycles $\{(r, s, k) \mid 1 \leq k \leq n, k \neq r, s\}$.

**Lemma I.6.12.** If $N$ is a normal subgroup of $A_n$ (where $n \geq 3$) and $N$ contains a 3-cycle, then $N = A_n$.

Note. We now have the equipment to prove Theorem I.6.10 ($A_n$ is simple if and only if $n \neq 4$). In fact, this is the same proof outlined in Fraleigh’s Exercise 15.39.

**Definition.** The subgroup of $S_n$ (for $n \geq 3$) generated by $a = (1, 2, 3, \ldots, n)$ and

$$
b = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} = \prod_{2 \leq i \leq \lfloor (n+2)/2 \rfloor} (i, n+2-i)
$$

is the **dihedral group of degree** $n$, denoted $D_n$. 
Note. Of course the dihedral group is called the dihedral group because it is generated by two elements. You know these groups from undergraduate algebra since $D_n$ represents the symmetries of a regular $n$-gon, as shown in Exercise I.6.13.

Note. In Section I.9 we’ll see a way to define a group in terms of generators and relations which they satisfy. The following result illustrates how this can be done for $D_n$.

**Theorem I.6.13.** For each $n \geq 3$ the dihedral group $D_n$ is a group of order $2n$ whose generators $a$ and $b$ satisfy:

(i) $a^n = (1); b^2 = (1); a^k \neq (1)$ if $0 < k < n$;

(ii) $ba = a^{-1}b$.

Any group $G$ which is generated by elements $a, b \in G$ satisfying (i) and (ii) for some $n \geq 3$ (with $e \in G$ in place of (1)) is isomorphic to $D_n$.

*Revised: 10/23/2019*