Permutation Group

In general, the permutations of a set X form a group S_X. If X is a finite set, we can assume X = {1,2,...,n}. In this case we write S_n instead of S_X . The following theorem says that S_n is a group. We call this group the **symmetric group** on n letters.

Theorem 5.1. The symmetric group on n letters, S_n, is a group with n! elements, where the binary operation is the composition of maps.

Proof. The identity of Sn is just the identity map that sends 1 to 1, 2 to 2, ..., n to n. If $f : S_n \to S_n$ is a permutation, then f^{-1} exists, since f is one-to-one and onto; hence, every permutation has an inverse. Composition of maps is associative, which makes the group operation associative. We leave the proof that $|S_n| = n!$ as an exercise.

A subgroup of S_n is called a **permutation group**.

A permutation $\sigma \in S_X$ is a **cycle of length k** if there exist elements $a_1,a_2,...,a_k \in X$ such that

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,.....,\sigma(a_k) = a_1$$

and $\sigma(x) = x$ for all other elements $x \in X$. We will write $(a_1,a_2,...,a_k)$ to denote the cycle σ. Cycles are the building blocks of all permutations.

Theorem 5.3. Every permutation in S_n can be written as the product of disjoint cycles.

Proof. We can assume that $X = \{1,2,...,n\}$. Let $\sigma \in S_n$, and define X_1 to be $\{\sigma(1), \sigma^2(1), \ldots\}$. The set X_1 is finite since X is finite. Now let i be the first integer in X that is not in X_1 and define X_2 by $\{\sigma(i), \sigma^2(i), \ldots\}$.

Again, X_2 is a finite set. Continuing in this manner, we can define finite disjoint sets X_3, X_4, ... Since X is a finite set, we are guaranteed that this process will end and there will be only a finite number of these sets, say r. If σ_i is the cycle defined by

$$\sigma_i(x)=\sigma(x), \text{ when } x \in Xi \text{ and } \sigma_i\ (\ x\ ) = x, \text{ else}$$

then $\sigma = \sigma_1\sigma_2\cdots\sigma_r$. Since the sets $X_1, X_2, ..., X_r$ are disjoint, the cycles $\sigma_1, \sigma_2, ..., \sigma_r$ must also be disjoint.

Sandip Chatterjee, Department of Mathematics

The simplest permutation is a cycle of length 2. Such cycles are called **transpositions**. Since

$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$

any cycle can be written as the product of transpositions, leading to the following proposition.

Proposition 5.4 Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Lemma 5.5. If the identity is written as the product of r transpositions, $id = \tau_1 \tau_2 \cdots \tau_r$, then r is an even number.

Proof. We will employ induction on r. A transposition cannot be the identity; hence, $r > 1$. If $r = 2$, then we are done. Suppose that $r > 2$. In this case the product of the last two transpositions, $\tau_{r-1}\tau_r$, must be one of the following cases:

$$(ab)(ab) = id$$
$$(bc)(ab) = (ac)(bc)$$
$$(cd)(ab) = (ab)(cd)$$
$$(ac)(ab) = (ab)(bc),$$

where a, b, c, and d are distinct.

The first equation simply says that a transposition is its own inverse. If this case occurs, delete $\tau_{r-1}\ \tau_r$ from the product to obtain $id = \tau_1\ \tau_2 \cdots \tau_{r-3}\ \tau_{r-2}$. By induction $r - 2$ is even; hence, r must be even.

In each of the other three cases, we can replace $\tau_{r-1}\tau_r$ with the right-hand side of the corresponding equation to obtain a new product of r transpositions for the identity. In this new product the last occurrence of a will be in the next-to-the-last transposition. We can continue this process with $\tau_{r-2}\tau_{r-1}$ to obtain either a product of r−2 transpositions or a new product of r transpositions where the last occurrence of a is in τ_{r-2}. If the identity is the product of r−2 transpositions, then again we are done, by our induction hypothesis; otherwise, we will repeat the procedure with $\tau_{r-3}\ \tau_{r-2}$.

At some point either we will have two adjacent, identical transpositions canceling each other out or a will be shuffled so that it will appear only in the first transposition. However, the latter case cannot occur, because the identity would not fix a in this instance. Therefore, the identity permutation must be the product of r−2 transpositions and, again by our induction hypothesis, we are done.

Theorem 5.6. If a permutation σ can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly, if σ can be expressed as the product of an odd number of transpositions, then any other product of transpositions equaling σ must also contain an odd number of transpositions.

Proof. Suppose that $\sigma = \sigma_1\sigma_2 \cdots\sigma_m = \tau_1 \tau_2\cdots\tau_n$,
where m is even. We must show that n is also an even number. The inverse of σ^{-1} is $\sigma_m \cdots\sigma_1$. Since

$$\mathrm{id} = \sigma\sigma_m \cdots\sigma_1 = \tau_1 \cdots\tau_n \sigma_m \cdots\sigma_1,$$

n must be even by Lemma 5.5. The proof for the case in which σ can be expressed as an odd number of transpositions is left as an exercise.

In light of Theorem 5.6, we define a permutation to be **even** if it can be expressed as an even number of transpositions and **odd** if it can be expressed as an odd number of transpositions.