MA1057: INTRODUCTION TO ABSTRACT ALGEBRA
PERMUTATIONS

LECTURER: ARUNDHATHI KRISHNAN

1. Permutations

1.1. **Basic Definitions.** Let A and B be non-empty sets.

(i) A function $f : A \to B$ is said to be one-to-one, or injective, if $f(a) = f(a')$ implies that $a = a'$.
(ii) A function $f : A \to B$ is said to be onto, or surjective, if for every $b \in B$, there exists (a pre-image) $a \in A$ such that $f(a) = b$.
(iii) A function which is injective and surjective is called a bijection.

Definition 1.1.1. Let A be a (non-empty) set. A *permutation* of A is a bijective function from A to A.

Let us look at some elementary examples of permutations. In general, A can be *any* non-empty set, but our focus will be on the set $\{1, \ldots, n\}$, where n is a natural number.

Example 1.1.2. Let $A = \{1, 2, 3, 4\}$. Define $\alpha : A \to A$ as

$$\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \alpha(4) = 4.$$

This can be represented in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Let us see how to compose two functions on A in this representation. Let $\beta(1) = 2, \beta(2) = 1, \beta(3) = 4, \beta(4) = 3$. Then

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

The compositions $\beta \circ \alpha$ and $\alpha \circ \beta$ are given by

$$\beta \circ \alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}$$

and

$$\alpha \circ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}.$$

We note straightaway that $\alpha \circ \beta \neq \beta \circ \alpha$. That is, the product given by function composition is not *commutative*. We will denote the composition of two permutations $\alpha \circ \beta$ simply by $\alpha\beta$. We can also find the inverse of a permutation α, that is, the permutation which we denote by α^{-1} and satisfies

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = \text{ identity function on } \{1, 2, 3, 4\}.$$

For the particular example of α above, we get

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}.$$

Notation 1.1.3. For $n \in \mathbb{N}$, the set of permutations on $A = \{1, \ldots, n\}$ will be denoted by S_n. Elements of S_n can be represented in the following array form

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}.$$

Proposition 1.1.4. *For $n \in \mathbb{N}$, $|S_n| = n!$.*

Proof. Let α be any permutation in S_n. As α is a bijection on $\{1, \ldots, n\}$, there is a choice of n values for $\alpha(1)$, $n-1$ values for $\alpha(2)$, and so on, with a single value left as a choice for $\alpha(n)$. Hence there are $n! = n \cdots (1)$ permutations on the set with n points. $\square$

Example 1.1.5. Consider S_3, the set of permutations on $\{1, 2, 3\}$ whose cardinality is $3! = 6$. We list the elements out explicitly, using the same array form as above.

$$S_3 = \left\{ \varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \right.$$

$$\left. \beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \right\}.$$

Here ε denotes the identity permutation. Note that $\alpha^3 = \varepsilon = \beta^2$ and that $\beta\alpha = \alpha^2\beta$. We can also find inverses of all permutations by tracing backwards. For instance,

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \alpha^2.$$

Example 1.1.6. In S_5, consider

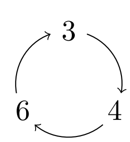
$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{bmatrix}, \ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{bmatrix}.$$

Find $\alpha\beta$, $\beta\alpha$, α^{-1}, β^{-1}, $(\alpha\beta)^{-1}$ and $\beta^{-1}\alpha^{-1}$. Also verify that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$, where ε is the identity function on $\{1, \ldots, 5\}$.

1.2. **Cycle Notation.** Let $\alpha \in S_6$ be given by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}.$$

We can write α as products of so-called *cycles* in the following way: $(1\,2)(3\,4\,6)(5)$. For instance, the cycle $(3\,4\,6)$ denotes that the action of the permutation α is as follows on $\{3, 4, 6\}$:



The permutation $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$ can be expressed as $(1,\, 5,\, 2,\, 3)(4,\, 6)$.

It is easily checked that $\alpha\beta = (1\,5)(2\,4\,3)(6)$ and $\beta\alpha = (1\,3\,6)(2\,5)(4)$. Often, a cycle with a single entry is omitted and it is understood that the point in question is fixed (for example, 6 in $\alpha\beta$ and 4 in $\beta\alpha$). The identity ε is often written as a single cycle, say (1).

Definition 1.2.1. For distinct numbers $a_1, \ldots, a_m \in \{1, \ldots, n\}$, a cycle of length m written as $(a_1 \cdots a_m)$ is the permutation which sends $a_1 \to a_2, a_2 \to a_3, \ldots, a_{m-1} \to a_m, a_m \to a_1$, and leaves all other elements of $\{1, \ldots, n\}$ unchanged.

Definition 1.2.2. The order of a permutation α is the smallest positive integer m such that $\alpha^m = (1)$, the identity permutation.

Example 1.2.3. In S_4, let

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1\,2\,3\,4).$$

Then

$$\gamma^2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = (1\,3)(2\,4),\ \gamma^3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = (1\,4\,3\,2),\ \text{and}\ \gamma^4 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = (1).$$

Hence the order of γ is 4.

Proposition 1.2.4. *Any permutation $\alpha \in S_n$ has finite order.*

Proof. The set $\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^n, \ldots\}$ is a subset of the set of all permutations S_n and hence must be finite. This means some of the powers of α must coincide, that is, $\alpha^k = \alpha^l$ for some $k < l \in \mathbb{N}$. Hence $\alpha^{l-k} = \alpha^0 = (1)$, so the order of α is less than or equal to $(l - k)$. □

Proposition 1.2.5. *A cycle of length m has order m.*

Proof. Consider a cycle of length m given by $\alpha = (a_1 \ldots a_m)$. It is clear that $(a_1 \ldots a_m)^m = (a_1) = (1)$, so the order of α is less than or equal to m. On the other hand, if $0 < k < m$, then $\alpha^k(a_1) = a_{k+1} \neq a_1$, so α^k is not the identity permutation. So the order of an m-cycle is m.

□

Definition 1.2.6. Two cycles $(a_1 \cdots a_m)$ and $(b_1 \cdots b_l)$ are said to be disjoint if they ave no elements in common, that is $a_i \neq b_j$ for all i, j.

Theorem 1.2.7. *Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.*

Proof. Let α be a permutation on $A = \{1, 2, \ldots, n\}$. Choose $a_1^1 \in A$ and let $a_2^1 = \alpha(a_1^1), a_3^1 = \alpha(a_2^1) = \alpha^2(a_1^1), \ldots$ until we arrive at $a_1^1 = \alpha^{m_1}(a_1^1)$ for some m_1. Such an m_1 must surely exist as the sequence $a_1^1, \alpha(a_1^1), \ldots$ takes values in the finite set A. To be precise, we must have $i < j \in \mathbb{N}_0$ such that $\alpha^i(a_1^1) = \alpha^j(a_1^1)$, so that $a_1^1 = \alpha^{j-i}(a_1^1)$. We express this relationship among $a_1^1, \ldots, a_{m_1}^1$ as the cycle $(a_1^1 \ldots a_{m_1}^1)$ and write $\alpha = (a_1^1 \ldots a_{m_1}^1) \cdots$. If all the entries of A are not exhausted, select $a_1^2 \in A$ such that a_1^2 does not belong to the cycle already considered. Repeat the same process as before to get a cycle $(a_1^2 \ldots a_{m_2}^2)$. We claim that this cycle and the previously constructed cycle have no elements in common. Indeed, if $\alpha^i(a_1^1) = \alpha^j(a_1^2)$ for some $i, j \in \mathbb{N}_0$, then $\alpha^{i-j}(a_1^1) = a_1^2$, which contradicts the criterion for choosing a_1^2. We continue building disjoint cycles in this manner until the (finitely many) elements of A run out, so that we get for some $k \in \mathbb{N}$ and $m_1, \ldots, m_k \in \mathbb{N}$,

$$\alpha = (a_1^1 \ldots a_{m_1}^1)(a_1^2 \ldots a_{m_2}^2) \cdots (a_1^k \ldots a_{m_k}^k).$$

□

We next show that disjoint cycles commute.

Theorem 1.2.8. *If the pair of cycles $\alpha = (a_1 \ldots a_m)$ and $\beta = (b_1 \ldots b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.*

Proof. Suppose α and β are permutations of $S = \{a_1 \ldots, a_m, b_1, \ldots, b_n, c_1 \ldots, c_s\}$ where the c_i-s are left fixed by α and β. We will show that $\alpha\beta(x) = \beta\alpha(x)$ for all $x \in S$.

First, suppose $x = c_i$ for some i. Then $\alpha\beta(c_i) = \alpha(c_i) = c_i = \beta(c_i) = \beta\alpha(c_i)$.

If $x = a_i$ for some i, then $\alpha\beta(a_i) = \alpha(a_i) = a_{i+1} = \beta(a_{i+1}) = \beta\alpha(a_i)$, with the understanding that $a_{m+1} = a_1$. Similarly, $\alpha\beta(b_i) = \alpha(b_{i+1}) = b_{i+1} = \beta(b_i) = \beta\alpha(b_i)$ with the understanding that $b_{n+1} = b_1$. □

Exercise 1.2.9. Let α and β be disjoint cycles. Show that for all $k \in \mathbb{N}$,

(i) $\alpha\beta^k = \beta^k\alpha$.
(ii) $(\alpha\beta)^k = \alpha^k\beta^k$.

Exercise 1.2.10. Let $\alpha_1, \ldots, \alpha_M$ be disjoint cycles. Show that for all $k \in \mathbb{N}$, $(\alpha_1 \cdots \alpha_M)^k = \alpha_1^k \cdots \alpha_M^k$.

We will show that the order of a permutation can be determined from the lengths of disjoint cycles whose product is the permutation. Let us first prove a lemma that we will need.

Lemma 1.2.11. *Suppose α is a permutation with order m and $N \in \mathbb{N}$ such that $\alpha^N = (1)$. Then $N = mk$ for some $k \in \mathbb{N}$.*

Proof. Clearly, $m \leq N$. Use the division algorithm to find $k, r \in \mathbb{N}$ such that $N = mk + r$, with $0 \leq r < m$. Then $\alpha^r = \alpha^{N-mk} = \alpha^N(\alpha^m)^{(-k)} = (1)$. As m is the smallest positive integer such that $\alpha^m = (1)$, we must have $r = 0$ and thus $N = mk$. □

Theorem 1.2.12. *The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

Proof. We proved in Proposition 1.2.5 that any cycle of length m has order m. We will call the elements $c_1, \ldots, c_s$ that appear in a permutation $\gamma = (c_1, \ldots, c_s)$ *symbols*. Suppose that α and β are disjoint cycles of length m and n, and let $k = \mathrm{lcm}(m, n)$. Then $\alpha^k = \varepsilon = \beta^k$. Now $(\alpha\beta)^k = \alpha^k\beta^k = \varepsilon$ as α and β are disjoint, by Exercise 1.2.9. Let t be the order of $\alpha\beta$. By Lemma 1.2.11, t divides k. Now, $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, so $\alpha^t = \beta^{-t}$. As α and β are disjoint cycles, there is no common symbol that appears in both. Hence, the same is true of α^t and β^{-t}, as raising a cycle to a power does not introduce any new symbols. Hence the equality of α^t and β^{-t} means that we must have $\alpha^t = \varepsilon = \beta^{-t}$, so that the orders of α and β, respectively m and n, both divide t, by another application of Lemma 1.2.11. Hence, the least common multiple k of m and n also divides t so that $k = t$. That is, $|\,\alpha\beta\,| = \mathrm{lcm}(m, n)$. The argument can now be extended to any finite product of disjoint cycles. □

Example 1.2.13. Find the orders of the following permutations:

(i) $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 1 & 4 & 2 & 5 & 3 \end{bmatrix}$
(ii) $\beta = (1\,2\,3)(4\,5\,6)(7\,8)$.
(iii) $\gamma = (1\,5\,2)(4\,5\,6\,7)(1\,2\,5)$
(iv) $\delta = (1\,2)(2\,3)(3\,4)(4\,5)(5\,6)$.

1.3. **Transpositions.**

Definition 1.3.1. A cycle of length 2 is called a *transposition*.

Theorem 1.3.2. *Every permutation in S_n for $n \geq 2$ can be written as a product of transpositions.*

Proof. The identity can be written as $\varepsilon = (1,2)(2,1)$. By Theorem 1.2.7, we know that every permutation can be written as a product of disjoint cycles as follows:

$$(a_1\ \dots\ a_m)(b_1\ \dots\ b_n)\cdots(c_1\ \dots\ c_s).$$

It is easily verified that this can be written as

$$(a_1\, a_m)(a_1\, a_{m-1})\cdots(a_1\, a_2)(b_1\, b_n)(b_1\, b_{n-1})\cdots(b_1\, b_2)\cdots(c_1\, c_s)(c_1\, c_{s-1})\cdots(c_1\, c_2).$$

□

It is worth noting that the decomposition above is *not unique*. For example, the cycle $(1,2,3,4,5)$ can be expressed as both $(1,5)(1,4)(1,3)(1,2)$ and $(5,4)(5,2)(2,1)(2,5)(2,3)(1,3)$. However, we observe that in both cases, the number of transpositions in the decomposition is even. Similarly, $\alpha = (1\,3) = (1\,2)(2\,3)(1\,2)$ can be written as a product of three transpositions, or a single transpositions, but in both cases, the number of transpositions is odd. We will show that if a permutation can be expressed as a product of an even number of transpositions, then *every* decomposition of it into a product of transpositions must contain an even number of transpositions. Similarly, if a permutation can be expressed as a product of an odd number of transpositions, then *every* decomposition of it into a product of transpositions must contain an odd number of transpositions. In order to prove this, we will construct a function

$$\mathrm{sign} : S_n \to \{-1, +1\},$$

with the following properties:

(i) $\mathrm{sign}(\tau) = -1$ for any transposition τ.
(ii) $\mathrm{sign}(\alpha\beta) = \mathrm{sign}(\alpha)\,\mathrm{sign}(\beta)$ for all $\alpha, \beta \in S_n$.

Hands on construction of the sign function: Write the permutation $\alpha \in S_n$ in its array representation. We will track down transpositions inside α by counting the number of crossings when we connect numbers from the first row with the same numbers on the second row.

Example 1.3.3. Suppose α is a permutation in S_5 with

$$\alpha = (3\,4) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{bmatrix}$$

We note that there is a single crossing, between 3-s and 4-s, denoting that the permutation can be decomposed into a single transposition.

Suppose $\beta \in S_5$ with

$$\beta = (1\,3\,4\,5\,2) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{bmatrix}$$

There are four crossings here denoting that the permutation can be decomposed into a product of four transpositions. Now, for instance, we have a crossing between 2-s and 4-s because the order in which 2 and 4 appear is reversed in the second line. That is

$$\beta(5) = 2 < 4 = \beta(3),$$

but

$$5 > 3, \text{ or equivalently, } \frac{\beta(3) - \beta(5)}{3 - 5} < 0.$$

Let us now define our sign function.

Definition 1.3.4. We define the sign of a permutation α as the following product:

$$\operatorname{sign}(\alpha) = \prod_{\substack{i<j,\\ i,j\in\{1,\dots,n\}}} \frac{\alpha(i)-\alpha(j)}{i-j}.$$

For β in Example 1.3.3, we get

$$\begin{aligned}
\operatorname{sign}(\beta) &= \prod_{\substack{i<j,\\ i,j\in\{1,\dots,n\}}} \frac{\beta(i)-\beta(j)}{i-j} \\
&= \frac{\beta(1)-\beta(2)}{1-2}\cdots\frac{\beta(1)-\beta(5)}{1-5}\cdot\frac{\beta(2)-\beta(3)}{2-3}\cdots\frac{\beta(2)-\beta(5)}{2-5}\cdot\frac{\beta(3)-\beta(4)}{3-4}\frac{\beta(3)-\beta(5)}{3-5}\cdot\frac{\beta(4)-\beta(5)}{4-5} \\
&= (-1)^4 = 1.
\end{aligned}$$

Proposition 1.3.5. *Let the sign function be as defined in 1.3.4. Then:*

(i) $\operatorname{sign}(\alpha)\in\{-1,+1\}$ *for all* $\alpha\in S_n$.
(ii) $\operatorname{sign}(\alpha\beta)=\operatorname{sign}(\alpha)\operatorname{sign}(\beta)$ *for all* $\alpha,\beta\in S_n$.
(iii) *If* $\tau=(k\,l)$ *is a transposition, then* $\operatorname{sign}(\tau)=-1$.
(iv) $\operatorname{sign}(\tau_1\tau_2\dots\tau_m)=(-1)^m$ *for any transpositions* $\tau_1,\dots,\tau_m$.

Proof. (i) We claim that in the product used to define the sign function, each of the terms $\alpha(i)-\alpha(j)$ with $i<j$ in the numerator of the fraction cancels with some term $k-l$, $(k<l)$ in the denominator, leaving behind only ±1. Now α being a permutation in S_n means that the set $\{\alpha(1),\dots,\alpha(n)\}$ is the same as the set $\{1,\dots,n\}$. Hence the elements of the sets $\{\alpha(i)-\alpha(j)\mid i<j\}$ and $\{i-j\mid i<j\}$ are the same except possibly for the signs $\pm$ (since $i-j<0$ for $i<j$ but we may have $\alpha(i)-\alpha(j)$ positive or negative). This means that for each $i<j$, $\alpha(i)-\alpha(j)=\pm(k-l)$ for some $k<l$, hence proving our claim.

(ii) For $\alpha,\beta\in S_n$,

$$\begin{aligned}
\operatorname{sign}(\alpha\beta) &= \prod_{\substack{i<j\\ i,j\in\{1,\dots,n\}}} \frac{\alpha(\beta(i))-\alpha(\beta(j))}{i-j} \\
&= \prod_{\substack{i<j\\ i,j\in\{1,\dots,n\}}} \frac{\alpha(\beta(i))-\alpha(\beta(j))}{\beta(i)-\beta(j)} \prod_{\substack{i<j\\ i,j\in\{1,\dots,n\}}} \frac{\beta(i)-\beta(j)}{i-j} \\
&= \operatorname{sign}(\alpha)\operatorname{sign}(\beta).
\end{aligned}$$

A note on why the first product is equal to $\operatorname{sign}(\alpha)$: As β is a bijection on $\{1,\dots,n\}$, each term $\frac{\alpha\beta(i)-\alpha\beta(j)}{\beta(i)-\beta(j)}$ can be written as

$$\frac{\alpha\beta(i)-\alpha\beta(j)}{\beta(i)-\beta(j)} = \frac{\alpha(k)-\alpha(l)}{k-l} = \frac{\alpha(l)-\alpha(k)}{l-k},\ k,l\in\{1,\dots,n\}$$

depending on whether $k<l$ or $l<k$.

(iii) Assume without loss of generality that $k<l$. Note that $\tau(i)=i$ for all $i\neq k,l$. Hence

$$\operatorname{sign}(\tau) = \prod_{\substack{i<j,\\ i,j\in\{1,\dots,n\}}} \frac{\tau(i)-\tau(j)}{i-j} = \frac{l-k}{k-l} = -1.$$

(iv) An easy consequence of (ii) and (iii).

□

Theorem 1.3.6. *If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (respectively, odd) number of 2-cycles.*

Proof. By (iv) of Proposition 1.3.5, if a permutation α can be expressed as a product of an even number of 2-cycles, then $\text{sign}(\alpha) = 1$ and if a permutation α can be expressed as a product of an odd number of 2-cycles, then $\text{sign}(\alpha) = -1$. As sign is a well-defined function, a permutation cannot take two different values simultaneously. □

The above theorem allows us to make the following definition unambiguously.

Definition 1.3.7. A permutation that can be expressed as a product of an even (odd) number of 2-cycles is called an even (respectively, odd) permutation.

Definition 1.3.8. The set of even permutations in S_n is denoted by A_n.

Theorem 1.3.9. *For $n \geq 2$, $|\, A_n \,| = \frac{n!}{2}$.*

Proof. The map
$$T : A_n \to \{\text{odd permutations}\}$$
given by $T(\alpha) := (1\,2)\alpha$ is a bijection (proof left as an exercise). Hence there are as many odd permutations as even, so that $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. □

Example 1.3.10. From Example 1.1.5, we have the set of permutations on $\{1, 2, 3\}$ in transposition form as follows:
$$S_3 = \{\varepsilon = (1), \alpha = (1\,3)(1\,2), \alpha^2 = (1\,2)(1\,3), \beta = (2\,3), \alpha\beta = (1\,2), \alpha^2\beta = (1\,3)\}.$$
Hence the set of even permutations is given by
$$A_3 = \{(1), (1\,3)(1\,2), (1\,2)(1\,3)\}.$$

Exercise 1.3.11. Find S_4, A_4 and $S_4 \setminus A_4$.

1.4. **Symmetric Groups.** We already observed that two permutations α and β in S_n can be composed to give another permutation $\alpha\beta$. We observe the following properties that are satisfied:

(i) Associativity: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in S_n$.
(ii) Existence of identity: There is an element $\varepsilon = (1) \in S_n$ such that $\alpha\varepsilon = \varepsilon\alpha = \alpha$ for all $\alpha \in S_n$.
(iii) Existence of inverse: For each $\alpha \in S_n$, there is an element $\beta \in G$ such that $\alpha\beta = \beta\alpha = \varepsilon$.

The algebraic object S_n with the binary operation of function composition is the prototype of a 'group'. What's more, every group is 'like' a subgroup of a symmetric group by a well-known theorem called Cayley's theorem.

References

[1] Course notes of Anca Mustata, Lecturer, University College Cork.
[2] Chapters 2 and 5. Gallian, Joseph. Contemporary Abstract Algebra. Nelson Education, 2012.