Study Material

Subject: Mathematics

Semester: 2nd

Name of Teacher: Prabir Rudra

Topic: Permutation Groups (Group Theory) (CC-4)

Advice from faculty

The students of 2nd semester (Mathematics honours) are advised to read the enclosed study material on permutation groups. We will arrange a doubt clearing session on this topic via video conferencing by the end of this week. So the students are advised to read this material before attending the online session. We will inform you about the date and time of the doubt clearing session.

In case of any difficulty regarding the topic the students may contact the concerned teacher via various media (e-mail, WhatsApp, Google classroom, etc.) and get their queries settled.

e-mail: prudra.math@gmail.com

Date: 27.04.2020

Chapter 4

Permutation Groups

Almost without hyperbole, one can say that no branch of modern mathematics is now presented in the way as it was actually generated and group theory is no exception. Indeed, the genesis of group theory actually began with the permutation group, as it is called nowadays, towards analyzing and describing the relations between the roots of a polynomial equation. It was Cauchy (1815) who first made the systematic study of permutation group, irrespective of its reference to some polynomial equations. Actually it was the genius of Galois, who first (1829) understood them[1] to be a special case of a more general phenomenon and stressed upon the necessity of studying the underlying abstract structure and thus the theory of (finite) groups came into being.

4.1 Permutation group

Right from our school days we know that a *permutation* of n different elements is nothing but an arrangement of those elements in any order. For example, if we consider three elements x_1, x_2, x_3, then we can arrange them in any of the following six manners only.

$$x_1\,x_2\,x_3 \quad x_2\,x_1\,x_3 \quad x_3\,x_1\,x_2 \quad x_1\,x_3\,x_2 \quad x_2\,x_3\,x_1 \quad x_3\,x_2\,x_1$$

[1]It is a pity that his epoch making works came to light only in 1846, almost 14 years after his death. Galois failed twice at the entrance examination of the École Polytechnique. Twice he tried to communicate his works personally, once through Cauchy and then through Fourier, both of whom showed no interest; he then formally submitted it for publication to the Académie, which Poisson rejected as incomprehensible!

Each of these arrangements of x_1, x_2, x_3 is called a permutation. Note that each of these arrangements can be described as a bijective mapping from the set $S = \{x_1, x_2, x_3\}$ onto itself as shown below:

$$\begin{array}{l|l|l|l|l|l} x_1 \to x_1 & x_1 \to x_2 & x_1 \to x_3 & x_1 \to x_1 & x_1 \to x_2 & x_1 \to x_3 \\ x_2 \to x_2 & x_2 \to x_1 & x_2 \to x_1 & x_2 \to x_3 & x_2 \to x_3 & x_2 \to x_2 \\ x_3 \to x_3 & x_3 \to x_3 & x_3 \to x_2 & x_3 \to x_2 & x_3 \to x_1 & x_3 \to x_1 \end{array}$$

We now extend this idea over an arbitrary set of elements.

Definition 4.1.1. Let A be a nonempty set. A ***permutation*** of A is a bijective mapping of A onto itself.

Definition 4.1.2. A group $(G, *)$ is called a ***permutation group*** on a nonempty set A if the elements of G are some permutations of A and the operation $*$ is the composition of two mappings.

Example 4.1.3. Let X be a nonempty set and let S_X be the set of all bijective functions of X onto itself. Then $(S_X, \circ)$ is a group as we have shown in Example 3.1.9, where $\circ$ is the composition of functions. Hence $(S_X, \circ)$ is a permutation group.

Let us now consider permutation of a finite set. Suppose for any positive integer n, I_n denotes the finite set $\{1, 2, 3, \ldots, n\}$. For example, $I_3 = \{1, 2, 3\}$. Now any permutation on I_n is a bijective function on $\{1, 2, 3, \ldots, n\}$. The set of all permutations on I_n forms a group under the binary operation '*composition of two functions*'. This group is called the ***symmetric group*** on n elements and is denoted by S_n. It is easy to see that $|S_n| = n!$. Let $\alpha \in S_n$. Generally we demonstrate α in the following way:

$$\alpha : \begin{array}{l} 1 \longrightarrow \alpha(1) \\ 2 \longrightarrow \alpha(2) \\ 3 \longrightarrow \alpha(3) \\ \vdots \\ n \longrightarrow \alpha(n) \end{array}$$

where $\alpha(i)$ denotes the image of i under α, for all $i = 1, 2, \ldots, n$. But it is sometimes convenient to describe this permutation by means of the following notational device:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix}.$$

This notation is due to Cauchy and is called the ***two-row notation***. In the upper row, we list all the elemets of I_n and in the lower row under each element $i \in I_n$, we write the image of the element, i.e., $\alpha(i)$. For example, if $n = 3$ and α is a permutation on I_3 defined by $\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1$, then using the two-row notation we can write

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

The two-row notation of permutations is quite convenient while doing computations, such as determining the composition of permutations. Let

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \beta(1) & \beta(2) & \dots & \beta(n) \end{pmatrix}.$$

Now the composition $\alpha \circ \beta$ is also a permutation on I_n defined by $(\alpha \circ \beta)(i) = \alpha\big(\beta(i)\big)$ for all $i \in I_n$. Then,

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ \beta(1) & \beta(2) & \dots & \beta(n) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha\big(\beta(1)\big) & \alpha\big(\beta(2)\big) & \dots & \alpha\big(\beta(n)\big) \end{pmatrix}.$$

Let us consider the example with $n = 6$. Let α and β be two permutations on I_6 defined by

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

and

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

Let us compute $\alpha \circ \beta$ where $\alpha \circ \beta : I_6 \to I_6$ defined by $(\alpha \circ \beta)(i) = \alpha(\beta(i))$ for all $i \in I_6$. Thus,

$$(\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(6) = 5$$
$$(\alpha \circ \beta)(2) = \alpha(\beta(2)) = \alpha(5) = 2$$

and so on. From the above, it is clear that, when determining $(\alpha \circ \beta)(1)$(say), we start with β and finish with α, and read as follows : 1 goes to 6 (under β), 6 goes to 5 (under α) and so 1 goes to 5 (under $\alpha \circ \beta$). We can exhibit this in the following form:

$$\begin{aligned}
1 \xrightarrow{\beta} 6 \xrightarrow{\alpha} 5 \quad & 1 \xrightarrow{\alpha\circ\beta} 5 \\
2 \xrightarrow{\beta} 5 \xrightarrow{\alpha} 2 \quad & 2 \xrightarrow{\alpha\circ\beta} 2 \\
3 \xrightarrow{\beta} 3 \xrightarrow{\alpha} 4 \quad & 3 \xrightarrow{\alpha\circ\beta} 4 \\
4 \xrightarrow{\beta} 1 \xrightarrow{\alpha} 1 \quad & 4 \xrightarrow{\alpha\circ\beta} 1 \\
5 \xrightarrow{\beta} 2 \xrightarrow{\alpha} 3 \quad & 5 \xrightarrow{\alpha\circ\beta} 3 \\
6 \xrightarrow{\beta} 4 \xrightarrow{\alpha} 6 \quad & 6 \xrightarrow{\alpha\circ\beta} 6
\end{aligned}$$

Thus,

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

Example 4.1.4. In this example we consider the group S_3, the elements of this group being all the permutations on $I_3 = \{1, 2, 3\}$. As the number of bijective functions of I_3 onto itself is $3! = 6$, we have $|S_3| = 6$. We now enlist below the permutations on $I_3 = \{1, 2, 3\}$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We now show some computations regarding the composition or product of elements of S_3.

$$\gamma \circ \delta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \beta.$$

As a composition of mappings γ and δ, we may write:

$$\begin{aligned}
(\gamma \circ \delta)(1) &= \gamma\big(\delta(1)\big) = \gamma(2) = 3 \\
(\gamma \circ \delta)(2) &= \gamma\big(\delta(2)\big) = \gamma(1) = 1 \\
(\gamma \circ \delta)(3) &= \gamma\big(\delta(3)\big) = \gamma(3) = 2
\end{aligned}$$

The following calculation of $\delta \circ \gamma$ reveals an important fact.

$$\delta \circ \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha.$$

We find that $\gamma \circ \delta \neq \delta \circ \gamma$. Following is the incomplete Cayley table of this group. We leave it for the reader to fill it up.

$\circ$	e	α	β	γ	δ	σ
e	e	α	β	γ	δ	σ
α	α	β	e			
β	β	e	α			
γ	γ			e	β	
δ	δ			α	e	
σ	σ					e

The group S_3 is a noncommutative group of order 6.

In the following theorem, we prove this for any symmetric group $S_n, n \geq 3$.

Theorem 4.1.5. *If n is a positive integer such that $n \geq 3$, then the symmetric group S_n is a noncommutative group.*

Proof. Let $n \geq 3$. Let $\alpha, \beta \in S_n$ be defined by

$$\alpha(1) = 2, \alpha(2) = 1, \text{ and } \alpha(x) = x \text{ for all } x \neq 1, 2;$$
$$\beta(1) = 3, \beta(3) = 1, \text{ and } \beta(x) = x \text{ for all } x \neq 1, 3.$$

Then,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}$$

Now,

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix}$$

and

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

Thus $(\alpha \circ \beta)(1) = 3 \neq 2 = (\beta \circ \alpha)(1)$. Hence $\alpha \circ \beta \neq \beta \circ \alpha$ and so S_n is noncommutative, for $n \geq 3$. □

Let us now introduce a convention towards simplifying the two-row notation of a permutation. Consider the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}.$$

If $\alpha(i) = i$, then we drop the column $\begin{matrix} i \\ \alpha(i) \end{matrix}$. For example, let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$. Here $\alpha(1) = 1$ and $\alpha(3) = 3$. So we denote α by $\begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}$. Hence if we write $\alpha = \begin{pmatrix} 1 & 3 & 4 \\ 4 & 1 & 3 \end{pmatrix} \in S_5$, then we mean the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$.

Definition 4.1.6. A permutation σ on $I_n = \{1, 2, \ldots, n\}$ is called a ***k-cycle*** or cycle of length k if there exist distinct elements $i_1, i_2, \ldots, i_k$ in I_n such that

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \sigma(i_3) = i_4, \ldots, \sigma(i_{k-1}) = i_k,$$
$$\sigma(i_k) = i_1 \text{ and } \sigma(x) = x \text{ for all } x \in I_n \setminus \{i_1, i_2, \ldots, i_k\}.$$

A k-cycle with $k = 2$ is called a ***transposition.***

If a permutation σ on I_n is a k-cycle, we shall denote it by $(i_1\ i_2\ \ldots\ i_k)$. We shall refer to this new notation as *cycle notation.* For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{pmatrix}$$

is a permutation on $I_6 = \{1, 2, 3, 4, 5, 6\}$ such that:

$$\sigma(1) = 3,\ \sigma(3) = 2,\ \sigma(2) = 5,\ \sigma(5) = 1,\ \sigma(4) = 4,\ \sigma(6) = 6.$$

Hence, σ is a 4-cycle and we denote σ by $(1\,3\,2\,5)$. Observe that:

$$(1\,3\,2\,5) = (3\,2\,5\,1) = (2\,5\,1\,3) = (5\,1\,3\,2).$$

The term *cycle* regarding the cyclic notation may be understood in the light of the following diagram (Fig. 10). We show the diagram for the above permutation σ.

$$\text{or,} \qquad \sigma : 1 \to 3 \to 2 \to 5 \to 1$$

Consider now the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. For this permutation $\alpha(1) = 3, \alpha(3) = 1$ whereas $\alpha(2) = 4, \alpha(4) = 2$. Hence α is not a k-cycle.

Since k-cycles are nothing but special type of permutations, they can be composed, i.e., multiplied just like any two permutations. Consider the cycles $\sigma = (2\,4\,3)$ and $\delta = (1\,2\,6\,5)$. Then

$$\sigma : 2 \to 4 \to 3 \to 2 \text{ and } \sigma(x) = x \text{ when } x \neq 2, 4, 3 \text{ and,}$$

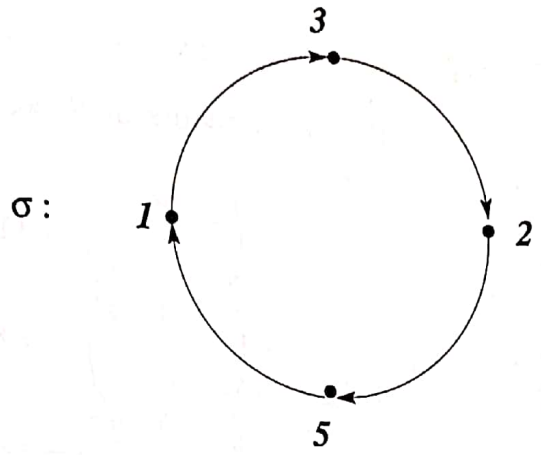

Fig. 10

$\delta : 1 \to 2 \to 6 \to 5 \to 1$ and $\delta(x) = x$ when $x \neq 1, 2, 5, 6$.

In other words, we can look upon σ and δ as mappings in the following manner:

$$\sigma : \begin{array}{l} 2 \to 4 \\ 4 \to 3 \\ 3 \to 2 \\ x \to x \\ \text{when } x \neq 2, 4, 3 \end{array} \qquad \delta : \begin{array}{l} 1 \to 2 \\ 2 \to 6 \\ 6 \to 5 \\ 5 \to 1 \\ x \to x \\ \text{when } x \neq 1, 2, 5, 6 \end{array}$$

Again viewed as permutations in a two-row notation, σ and δ are as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} \text{ and } \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

Now

$$\sigma\delta = \sigma \circ \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 3 & 1 & 5 \end{pmatrix}.$$

It is worth noticing that *while calculating $\sigma\delta$, we first consider the image of δ on the elements of I_6 and then on that image set, we further consider the image of σ.* Hence $\sigma \circ \delta : 1 \xrightarrow{\delta} 2 \xrightarrow{\sigma} 4$. Notice that under $\sigma\delta$,

$$1 \to 4 \to 3 \to 2 \to 6 \to 5 \to 1$$

Hence in this case $\sigma\delta$ is a 5-cycle.

But in general, product of two cycles may not be a cycle. To show this we consider the product of $\sigma = (5\,6)$ and $\delta = (3\,2\,4)$ from S_6. Then

$$\sigma\delta = \sigma \circ \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 6 & 5 \end{pmatrix}$$

is not a cycle.

Using the cycle notation we now write the elements of S_3 as follows:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3)$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2) \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3)$$

Hence,

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$$

consists of one 1-cycle, three 2-cycles and two 3-cycles.

Note that *the identity permutation e in the above example could have been represented as* (2) *or* (3) *also.*

Definition 4.1.7. Two cycles $(i_1\, i_2 \ldots i_t)$ and $(j_1\, j_2 \ldots j_k)$ of S_n are said to be ***disjoint*** if $\{i_1, i_2, \ldots, i_t\} \cap \{j_1, j_2, \ldots, j_k\} = \emptyset$.

Example 4.1.8. The cycles (2 4 3 5) and (1 6 8) are disjoint cycles, whereas the cycles (4 5 3 2) and (1 3 8) are not disjoint.

In the Example 4.1.8 above, we have considered two disjoint cycles $\alpha = (2\,4\,3\,5)$ and $\beta = (1\,6\,8)$. Now let us work out their compositions.

$$\alpha\beta = (2\,4\,3\,5)(1\,6\,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 5 & 3 & 2 & 8 & 7 & 1 \end{pmatrix};$$

$$\beta\alpha = (1\,6\,8)(2\,4\,3\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 5 & 3 & 2 & 8 & 7 & 1 \end{pmatrix}.$$

Hence $\alpha\beta = \beta\alpha$. Indeed, we have the following general result in the form of a theorem.

Theorem 4.1.9. *Let α and β be any two disjoint cycles in S_n. Then, $\alpha\beta = \beta\alpha$.*

Proof. Let $\alpha = (i_1\, i_2 \ldots i_t)$ and $\beta = (j_1\, j_2 \ldots j_k)$ be two disjoint cycles. We show that $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all $x \in I_n$. Now,

$$\alpha : \begin{array}{l} i_1 \to i_2 \\ i_2 \to i_3 \\ \vdots \\ i_{t-1} \to i_t \\ i_t \to i_1 \\ y \to y \\ \text{when } y \notin \{(i_1, i_2, \ldots, i_t\} \end{array} \qquad \beta : \begin{array}{l} j_1 \to j_2 \\ j_2 \to j_3 \\ \vdots \\ j_{k-1} \to j_k \\ j_k \to j_1 \\ y \to y \\ \text{when } y \notin \{j_1, j_2, \ldots, j_k\} \end{array}$$

Suppose x is neither $i_1, i_2, \ldots, i_t$ nor $j_1, j_2, \ldots, j_k$. Then $\alpha(x) = x$ and $\beta(x) = x$. Hence

$$(\alpha\beta)(x) = \alpha\Big(\beta(x)\Big) = \alpha(x) = x \text{ and } (\beta\alpha)(x) = \beta\Big(\alpha(x)\Big) = \beta(x) = x.$$

Suppose now x is one of $i_1, i_2, \ldots, i_t$. Hence $x \notin \{j_1, j_2, \ldots, j_k\}$. Then $\beta(x) = x$ and $\alpha(x)$ is one of $i_1, i_2, \ldots, i_t$. Hence $(\alpha\beta)(x) = \alpha\Big(\beta(x)\Big) = \alpha(x)$ and $(\beta\alpha)(x) = \beta\Big(\alpha(x)\Big) = \alpha(x)$ (since $\alpha(x) \notin \{j_1, j_2, \ldots, j_k\}$). Similarly, if x is one of $j_1, j_2, \ldots, j_k$, then $x \notin \{i_1, i_2, \ldots, i_t\}$ and as above we can show that $(\alpha\beta)(x) = \beta(x) = (\beta\alpha)(x)$. So we find that $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all $x \in I_n$. Consequently, $\alpha\beta = \beta\alpha$. □

Next we consider the following permutation from S_9.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 2 & 1 & 4 & 3 & 6 & 7 & 9 \end{pmatrix}$$

Under this permutation

$$\begin{aligned} \alpha(1) &= 5 \\ \alpha^2(1) = \alpha(\alpha(1)) &= \alpha(5) = 4 \\ \alpha^3(1) = \alpha(\alpha^2(1)) &= \alpha(4) = 1. \end{aligned}$$

So we find that 3 is the smallest positive integer such that $\alpha^3(1) = 1$. Now we define $\alpha_1 : I_9 = \{1, 2, 3 \ldots, 9\} \to I_9$ by

$$\begin{aligned} \alpha_1(1) &= \alpha(1) = 5 \\ \alpha_1(5) &= \alpha^2(1) = 4 \\ \alpha_1(4) &= \alpha^3(1) = 1 \end{aligned}$$

$$\text{and } \alpha_1(x) = x \text{ for all } x \in I_9 \setminus \{1, 4, 5\}.$$

Hence $\alpha_1 \in S_9$ and α_1 is a cycle given by $1 \to 5 \to 4 \to 1$. So we find that $\alpha_1 = (1\,5\,4)$ and $\alpha_1 \in S_9$.

Now $2 \notin \{\alpha(1), \alpha^2(1), \alpha^3(1)\} = \{1, 5, 4\}$. Starting with 2, we find that

$$\alpha(2) = 8$$
$$\alpha^2(2) = \alpha(\alpha(2)) = \alpha(8) = 7$$
$$\alpha^3(2) = \alpha(\alpha^2(2)) = \alpha(7) = 6$$
$$\alpha^4(2) = \alpha(\alpha^3(2)) = \alpha(6) = 3$$
$$\alpha^5(2) = \alpha(\alpha^4(2)) = \alpha(3) = 2.$$

Hence 5 is the smallest positive integer such that $\alpha^5(2) = 2$.

Now we define $\alpha_2 : I_9 = \{1, 2, 3 \ldots, 9\} \to I_9$ by

$$\alpha_2(2) = \alpha(2) = 8$$
$$\alpha_2(8) = \alpha^2(2) = 7$$
$$\alpha_2(7) = \alpha^3(2) = 6$$
$$\alpha_2(6) = \alpha^4(2) = 3$$
$$\alpha_2(3) = \alpha^5(2) = 2$$
$$\text{and } \alpha_2(x) = x \text{ for all } x \in I_9 \setminus \{2, 8, 7, 6, 3\}.$$

Clearly, $\alpha_2 \in S_9$ and under α_2

$$2 \to 8 \to 7 \to 6 \to 3 \to 2$$

and $x \to x$ for all $x \in I_9 \setminus \{2, 8, 7, 6, 3\}$. Hence α_2 defines a cycle $(2\,8\,7\,6\,3)$.

Note that $\alpha_1 = (1\,5\,4)$ and $\alpha_2 = (2\,8\,7\,6\,3)$ are disjoint and hence $\alpha_1\alpha_2 = \alpha_2\alpha_1$. Now $9 \notin \{1, 5, 4\} \cup \{2, 8, 7, 6, 3\}$. Starting with 9 we obtain $\alpha(9) = 9$. Hence 1 is the smallest positive integer such that $\alpha^1(9) = 9$. Now define $\alpha_3 : I_9 \to I_9$ by

$$\alpha_3(9) = \alpha(9) = 9$$
$$\text{and } \alpha_3(x) = x \text{ for all } x \in I_9 \setminus \{9\}.$$

Note that $\alpha_3 \in S_9$ and under α_3,

$$9 \to 9$$

and $x \to x$ for all $x \in I_9 \setminus \{9\}$. Consequently, α_3 is the identity permutation. Now it is easy to see that

$$\alpha = \alpha_1\alpha_2\alpha_3 = \alpha_1\alpha_2 = (1\,5\,4)(2\,8\,7\,6\,3)(9) = (1\,5\,4)(2\,8\,7\,6\,3).$$

Hence α is a product of disjoint cycles.

We can apply the above process for any permutation α on I_n for any integer $n \geq 2$ and show that α can be expressed as a product of disjoint cycles.

Theorem 4.1.10. *Any nonidentity permutation $\alpha \in S_n\,(n \geq 2)$ can be expressed as a product of disjoint cycles, where each cycle is of length ≥ 2.*

Proof. Let α be a permutation on S_n, $n \geq 2$. We begin by considering $1, \alpha(1), \alpha^2(1), \ldots$ until we find the smallest positive integer r such that $\alpha^r(1) = 1$. This gives us a r-cycle, say α_1, so that

$$\alpha_1 = (1\ \alpha(1)\ \alpha^2(1)\ \ldots \alpha^r(1)).$$

Let i be the smallest integer in I_n, that does not appear in α_1. Then we consider $\alpha(i), \alpha^2(i), \ldots$ so on, until we come across the smallest positive integer s such that $\alpha^s(i) = i$. Evidently this gives us an s-cycle, say α_2, so that:

$$\alpha_2 = (i\ \alpha(i)\ \alpha^2(i)\ \ldots \alpha^s(i)).$$

Before proceeding further, observe that α_1 and α_2, as we have constructed them, must be disjoint cycles, i.e.,

$$\left\{1, \alpha(1), \alpha^2(1), \ldots, \alpha^r(1)\right\} \cap \left\{i, \alpha(i), \alpha^2(i), \ldots, \alpha^s(i)\right\} = \emptyset.$$

Indeed, otherwise, if $\alpha^p(i) = \alpha^k(1)$ for some p, k $(1 \leq p \leq s$ and $1 \leq k \leq r)$, then we must have $\alpha^{p+1}(i) = \alpha(\alpha^p(i)) = \alpha(\alpha^k(1)) = \alpha^{k+1}(1)$ and so on, which in turn implies that $\alpha^{p+t}(i) = \alpha^{k+t}(1)$ for $t = 1, 2, \ldots$ Now there exists some t such that $p + t = s$. Hence for this t, $i = \alpha^{s+1}(i) = \alpha^{p+t+1}(i) = \alpha^{k+t+1}(1)$. This implies that i appears in α_1, a contradiction to the choice of i. Now if

$$\left\{1, \alpha(1), \alpha^2(1), \ldots, \alpha^r(1)\right\} \cup \left\{i, \alpha(i), \alpha^2(i), \ldots, \alpha^s(i)\right\} \neq I_n,$$

then we consider the smallest member of I_n not appearing in the left hand side union above and continue the same process as before to construct cycle α_3. Since I_n is finite, the aforesaid process must terminate after a finite number of steps, with some cycle, say, α_m. From the definition of the cycles $\alpha_1, \alpha_2, \ldots, \alpha_m$, it now follows that $\alpha = \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_m$. □

Next we consider a cycle $\alpha = (2\,4\,3\,5)$ on S_6. Under this permutation we have

$$\alpha : 2 \to 4 \to 3 \to 5 \to 2$$

and $x \to x$ whenever $x \in I_6 \setminus \{2, 4, 3, 5\}$. Now consider the 2-cycles $(2\,5), (2\,3), (2\,4)$. Let $\alpha_1 = (2\,5)$, $\alpha_2 = (2\,3)$ and $\alpha_3 = (2\,4)$. Consider the product

$$\alpha_1\alpha_2\alpha_3 = (2\,5)(2\,3)(2\,4).$$

Under this product,

$$
\begin{aligned}
2 &\xrightarrow{\alpha_3} 4 \xrightarrow{\alpha_2} 4 \xrightarrow{\alpha_1} 4\\
4 &\xrightarrow{\alpha_3} 2 \xrightarrow{\alpha_2} 3 \xrightarrow{\alpha_1} 3\\
3 &\xrightarrow{\alpha_3} 3 \xrightarrow{\alpha_2} 2 \xrightarrow{\alpha_1} 5\\
5 &\xrightarrow{\alpha_3} 5 \xrightarrow{\alpha_2} 5 \xrightarrow{\alpha_1} 2\\
x &\xrightarrow{\alpha_3} x \xrightarrow{\alpha_2} x \xrightarrow{\alpha_1} x
\end{aligned}
$$

when $x \neq 2, 3, 4, 5$.

Then,

$$\alpha_1\alpha_2\alpha_3 : 2 \to 4 \to 3 \to 5 \,, \to 2 \text{ and } x \to x \text{ for the rest.}$$

Consequently, $\alpha_1\alpha_2\alpha_3 = (2\,4\,3\,5)$.

In this way we can show that *any cycle* $(i_1, i_2, \ldots, i_k)$, $k \geq 3$ *can be expressed as* $(i_1\, i_k)(i_1\, i_{k-1}) \ldots (i_1\, i_2)$. Indeed we may have the following theorem.

Theorem 4.1.11. *Any cycle of length* ≥ 2 *is either a transposition (i.e., 2-cycle) or can be expressed as a product of transpositions.*

Combining the last two theorems we state the following:

Theorem 4.1.12. *Any nonidentity permutation of* S_n $(n \geq 2)$ *is either a transposition or can be expressed as a product of transpositions.*

Definition 4.1.13. A permutation $\alpha \in S_n$ is called an ***even permutation*** if α can be expressed as a product of an even number of 2-cycles and a permutation $\alpha \in S_n$ is called an ***odd permutation*** if α is either a 2-cycle or can be expressed as a product of an odd number of 2-cycles. The set of all even permutations in S_n forms a group. This group is called the ***alternating group*** and is denoted by A_n.

Note that according to the above definition the identity permutation is an even permutation. (why?) We now merely state the following theorem, which is a very important property of a permutation.

Theorem 4.1.14. *Any permutation in* S_n *is either an odd permutation or an even permutation, but never both.*

Example 4.1.15. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 7 & 4 & 2 & 1 \end{pmatrix} \in S_8.$$

Here $\alpha(1) = 8, \alpha^2(1) = \alpha(8) = 1$. Hence $1 \to 8 \to 1$ defines a 2-cycle, viz., $(1\,8)$.

Now $3 \notin \{1, 8\}$ and

$$\alpha(3) = 6, \alpha^2(3) = \alpha(6) = 4, \alpha^3(3) = \alpha(4) = 3$$

imply that $3 \to 6 \to 4 \to 3$ forms a 3-cycle $(3\,6\,4)$.

Now $5 \notin \{1, 8\} \cup \{3, 6, 4\}$ and

$$\alpha(5) = 7, \alpha^2(5) = \alpha(7) = 2, \alpha^3(5) = \alpha(2) = 5,$$

whence $5 \to 7 \to 2 \to 5$ defines a 3-cycle $(5\,7\,2)$. Hence $\alpha = (1\,8)(3\,6\,4)(5\,7\,2)$. Now $(3\,6\,4) = (3\,4)(3\,6)$ and $(5\,7\,2) = (5\,2)(5\,7)$. Hence $\alpha = (1\,8)(3\,4)(3\,6)(5\,2)(5\,7)$ is a product of *five* 2-cycles and so α is an odd permutation.

We have defined earlier, the notion of the *order of an element* in a group. In that light, let us examine the order of various elements of the permutation group S_n. *Since this group is finite, the order of any element of this group must also be finite.* Let $\alpha \in S_n$. To find the order of α, we need to compute $\alpha, \alpha^2, \alpha^3, \ldots$, until we find the first positive integer n, such that α^n becomes the identity permutation e. For example, let us consider the group

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Note that $(1\,2\,3) \circ (1\,2\,3) = (1\,3\,2) \neq e$ and $(1\,2\,3) \circ (1\,2\,3) \circ (1\,2\,3) = e$, whence order of $(1\,2\,3)$ is 3. In a similar manner, we may show that the order of $(1\,3\,2)$ is also 3.

Let us now consider $(1\,2) \in S_3$. Observe that, $(1\,2) \circ (1\,2) = e$ whence order of $(1\,2)$ is 2. Similarly, order of $(1\,3)$ as well as of $(2\,3)$ is 2. So we see that the order of 2-cycles in S_3 is 2, and the order of 3-cycles in S_3 is 3. Indeed, we have the following general result.

Theorem 4.1.16. *Let $n \geq 2$ and $\sigma \in S_n$ be a cycle. Then σ is a k-cycle if and only if order of σ is k.*

Proof. Let σ be a k-cycle in S_n, $n \geq 2$. Let $\sigma = (a_1\, a_2 \ldots a_k)$. Then $\sigma(a) = a$ for all $a \notin \{a_1, a_2, \ldots, a_k\}$. Now $\sigma^i(a_1) = a_{i+1}$ for all $1 \leq i < k$ and $\sigma^k(a_1) = a_1$. Consider a_i, $1 \leq i \leq n$. Now $\sigma^{k-i}(a_i) = a_k, \sigma^{k-i+1}(a_i) = a_1$. This implies that $\sigma^{k+l-i}(a_i) = a_l$ for all $1 \leq l < k$ and so $\sigma^k(a_i) = a_i$. Thus, $\sigma^k(a) = a$ for all a and so $\sigma^k = e$, whence $o(\sigma) \mid k$. Suppose $o(\sigma) = t$ and $t < k$. Then $a_1 = \sigma^t(a_1) = a_{t+1}$, a contradiction, since $a_{t+1} \neq a_1$. Hence $t = k$, i.e., $o(\sigma) = k$.

Conversely, suppose that $o(\sigma) = k$. Suppose σ is a t-cycle. Then as before we can show that $o(\sigma) = t$. This implies that $k = t$, i.e., σ is a k-cycle. □

Observe that, for a permutation $\alpha \in S_n$, which is not a cycle itself, a direct process to find the smallest positive integer n, for which $\alpha^n = e$, may be a very tedious task. However, we can decompose α into disjoint cycles, and then compute the order of each of them, which is nothing but the length of the respective cycles (by Theorem 4.1.16), and then use them to find the order of α. The next result will throw some light in this regard.

Theorem 4.1.17. *Let $\sigma \in S_r$, $r \geq 2$ and $\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k$ be a product of disjoint cycles. Suppose $o(\sigma_i) = n_i$, $i = 1, 2, \ldots, k$. Then $o(\sigma) = lcm(n_1, n_2, \ldots, n_k)$.*

Proof. Let $o(\sigma) = t$ and $m = lcm(n_1, n_2, \ldots, n_k)$. Now $m = n_i r_i$ for some $r_i \in \mathbb{N}$, for each $i = 1, 2, \ldots, k$. Since disjoint cycles commute, $\sigma^m = \sigma_1^m \circ \sigma_2^m \circ \ldots \circ \sigma_k^m = \sigma_1^{n_1 r_1} \circ \sigma_2^{n_2 r_2} \circ \ldots \circ \sigma_k^{n_k r_k} = e$ since $o(\sigma_i) = n_i$ for each i. Thus, $t \mid m$. In order to show that $m \mid t$, it suffices to show that $n_i \mid t$, i.e., $\sigma_i^t = e$, for each $i = 1, 2, \ldots, k$. Since disjoint cycles commute, $\sigma = \sigma_i \circ \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_{i+1} \circ \cdots \circ \sigma_k$. Let $a \in I_r$. If $\sigma_i(a) = a$, then $\sigma_i^t(a) = a$. Suppose σ_i moves a. Then as σ_i's are disjoint, $\sigma_j(a) = a$ for all $j \neq i$. Hence $\sigma_j^t(a) = a$ for all $j, j \neq i$. Thus, $a = \sigma^t(a) = (\sigma_i^t \circ \sigma_1^t \circ \sigma_2^t \circ \cdots \circ \sigma_{i-1}^t \circ \sigma_{i+1}^t \circ \cdots \circ \sigma_k^t)(a) = \sigma_i^t(a)$. Hence $\sigma_i^t = e$. As this is true for each $i = 1, 2, \ldots, k$, the theorem follows.

□

Before we end this section and plunge into exercises, let us discuss in brief a mind-boggling problem that comes under the purview of the so-called **recreational mathematics**. Known as the *Fifteen Puzzle*, this interesting game was conceived by Sam Loyd in 1878, and soon it became very popular. Even today one may find this game, which consists of fifteen square blocks, numbered from 1 to 15, contained within a square frame, with the sixteenth place empty (usually at the right-hand bottom corner). The blocks can be slided only horizontally and vertically via the empty slot. One may shuffle the blocks arbitrarily, and the game is to rearrange them back to the initial regular position.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Now suppose we get hold of one such toy which is set at the initial regular position. We deliberately erase the numbers 14 and 15 from the respective blocks and then imprint there 15 and 14 respectively.