Chapter 6
The Symmetric Group "An Example of Finite Nonabelian Group"

This chapter discusses the group $\mathfrak{S}_n$ (Corollary 5.1.11), the symmetric group on n elements, which is one of the most important examples of finite groups and is widely used in applications to geometry and physics (Carter, 2009). The importance of symmetry groups in abstract algebra is due to the fact that for any finite group G, there is a symmetric group $\mathfrak{S}_n$ that contains a copy of G. For each $n \in \mathbb{N}$, the group $\mathfrak{S}_n$ consists of all the bijective maps of $\{1, 2, \ldots, n\}$ to itself, called permutations of $\{1, 2, \ldots, n\}$. These permutations are usually denoted by symbols such as ϕ and ψ. The identity permutation that corresponds to the identity map of $\{1, 2, \ldots, n\}$ is denoted by e. In this chapter, Sect. 6.1 provides a representation of the elements of $\mathfrak{S}_n$ as matrices and specifies the order of $\mathfrak{S}_n$ in terms of the integer n. Additionally, the notion of pairwise disjoint permutations is discussed, and their commutativity is verified. In Sect. 6.2, cycles, a special case of permutations, are defined and studied. The main result of this section is Proposition 6.2.9, which states that any permutation can be written as a finite product of disjoint cycles. The proof of this proposition requires a study of orbits of a permutation which discussed in Sect. 6.3 and followed by the proof of Proposition 6.2.9. The last two sections of this chapter discuss methods for determining the order of permutations and classifying permutations as odd and even.

6.1 Matrix Representation of Permutations

Let $n \in \mathbb{N}$. Each permutation ϕ of $\{1, 2, \ldots, n\}$ can be represented using a $2 \times n$ matrix. The first row of the matrix lists elements of the domain of the permutation. The images are represented in the second row with the image $\phi(i)$ placed directly under i, for each $1 \leq i \leq n$. i.e., the matrix representation of a permutation ϕ is

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

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_6

For example, if $n = 4$, the permutation $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ is the map determined by

$$\phi(1) = 3, \phi(2) = 1, \phi(3) = 4, \text{ and } \phi(4) = 2.$$

The matrix representation of the identity permutation e is

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Remark 6.1.1 The elements in the first row in the matrix representation of ϕ can be written in any order; however, the images of the elements must be carefully arranged in the second row, ensuring that the image of any element i must be exactly below i. For example, all of the following matrices represent the same permutation:

$$\begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 2 & 4 & 1 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

When a matrix representation is used, the composition of two permutations (two bijective maps) ϕ and ψ is determined by the equation $\psi \circ \phi(k) = \psi(\phi(k))$. For example,

$$\text{if } \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \text{ then } \psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

The computations can be sketched as follows:
$1 \xrightarrow{\phi} 3 \xrightarrow{\psi} 1$ gives $1 \xrightarrow{\psi\circ\phi} 1$,
$2 \xrightarrow{\phi} 1 \xrightarrow{\psi} 4$ gives $2 \xrightarrow{\psi\circ\phi} 4$,
$3 \xrightarrow{\phi} 4 \xrightarrow{\psi} 2$ gives $3 \xrightarrow{\psi\circ\phi} 2$, and
$4 \xrightarrow{\phi} 2 \xrightarrow{\psi} 3$ gives $4 \xrightarrow{\psi\circ\phi} 3$ (Fig. 6.1).

The matrix representation of ϕ^{-1} can be obtained by exchanging the two rows in the matrix ϕ. One can check that the composition of ϕ and ϕ^{-1} yields the identity map on $\{1, 2, \ldots, n\}$. For example,

$$\text{if } \phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \text{ then } \phi^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

and the composition of ϕ and ϕ^{-1} yields the identity permutation e.

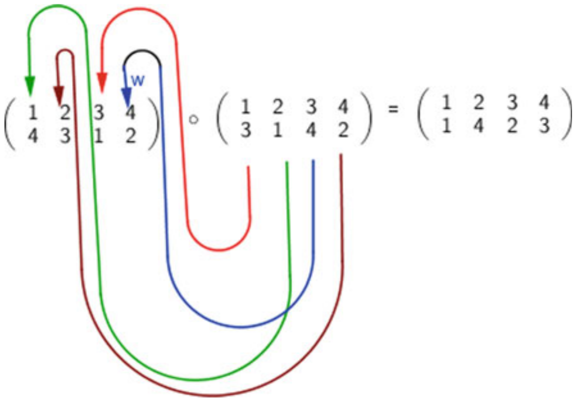

Fig. 6.1 A composition of two permutations

Example 6.1.2 Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$ be two permutations on $\{1, 2, \ldots, 5\}$. One can easily check that

1. $\phi(3) = 2, \phi(5) = 4, \psi(2) = 5$, and $\psi(4) = 4$.
2. $\phi^2 = \phi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$.
3. $\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$ and $\psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$.
4. $\phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ and $\psi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$.
5. $\phi^{-1} \circ \psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$.

The nonequality $\phi \circ \psi \neq \psi \circ \phi$ shows that $\mathfrak{S}_5$ is not abelian.

Proposition 6.1.3 *The group $\mathfrak{S}_n$ is not abelian for each $n \geq 3$.*

Proof Assume that $n \geq 3$. Consider the permutations

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \\ 2 & 1 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \end{pmatrix}, \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \\ 3 & 2 & 1 & 4 & 5 & \ldots\ldots & n-1 & n \end{pmatrix}.$$

Both permutations are elements in $\mathfrak{S}_n$. Since $\phi \circ \psi(1) = 3 \neq 2 = \psi \circ \phi(1)$, thus $\mathfrak{S}_n$ is not abelian. ■

Example 6.1.4 The following statements describe the elements of $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, and $\mathfrak{S}_4$.

1. There exists only one bijection of the set $\{1\}$. Thus, $\mathfrak{S}_1$ contains only the identity map

$$\phi = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e.$$

2. For $\phi \in \mathfrak{S}_2$, a bijective map of $\{1, 2\}$, there are two choices for the image of number 1 under ϕ, namely 1 or 2. After choosing the image of 1, only one choice is left for the image of 2. Therefore, either $\phi(1) = 1$ and $\phi(2) = 2$, yielding the identity map on $\{1, 2\}$, or $\phi(1) = 2$ and $\phi(2) = 1$. These values are all the possibilities for ϕ. Hence,

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1\,2 \\ 1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix} \right\}.$$

   Note that $|\mathfrak{S}_2| = 2 \times 1 = 2!$.
3. In the case of $\mathfrak{S}_3$, the choices are branched. For a bijective map ϕ on $\{1, 2, 3\}$, there are three choices for $\phi(1)$. On choosing the image for number 1, two choices are left for $\phi(2)$, and having chosen one of these, only one choice remains for $\phi(3)$. By the multiplication rule (De Temple & Webb, 2014), there are $3 \times 2 \times 1 = 3!$ ways to form ϕ. Figure 6.2. illustrates the choices for determining an element of $\mathfrak{S}_3$.

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \right\}$$

4. For the group $\mathfrak{S}_4$, one can use a tree similar to that shown in (3) to find all possible permutations. Table 6.1 lists all possible choices for $\phi(i)$, $1 \le i \le 4$.

   Each column, from the second on, represents an element of $\mathfrak{S}_4$. For example, the second column represents the identity permutation, and the third column represents the permutation $\begin{pmatrix} 1\;2\;\;3\;4 \\ 1\;2\;\;4\;3 \end{pmatrix}$. Clearly, there exist $24 = 4!$ permutations in $\mathfrak{S}_4$.

The same method used to solve this example can be used to prove the following theorem.

Theorem 6.1.5 *Let $n \in \mathbb{N}$. There exist $n!$ permutations in $\mathfrak{S}_n$.*

Proof The number of elements in $\mathfrak{S}_n$ is equal to the number of all possibilities of ϕ. To construct ϕ, the process is initiated by choosing an element for $\phi(1)$ from $\{1, 2, \ldots, n\}$. There are n choices for $\phi(1)$. Once $\phi(1)$ is chosen, $n-1$ choices remain for $\phi(2)$, namely $\{1, 2, \ldots, n\}\backslash\{\phi(1)\}$. After $\phi(1)$ and $\phi(2)$ have been selected, $n-2$ choices remain for $\phi(3)$, and so on. Continuing such selections, eventually, only one choice remains for $\phi(n)$. By the multiplication rule, the number of ways to form ϕ is

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!.$$

Therefore, there are $n!$ possibilities for ϕ. ■

Fig. 6.2 Elements of $\mathfrak{S}_3$

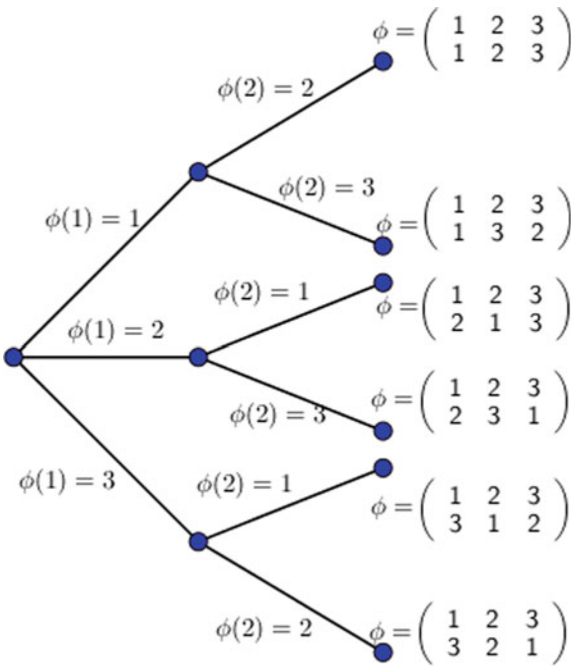
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\phi(2) = 2$
$\phi(2) = 3$
$\phi(1) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$\phi(2) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
$\phi(1) = 2$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
$\phi(2) = 3$
$\phi(1) = 3$
$\phi(2) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$\phi(2) = 2$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Table 6.1 Elements of $\mathfrak{S}_4$

$\phi(1)$	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4
$\phi(2)$	2	2	3	3	4	4	1	1	3	3	4	4	1	1	2	2	4	4	1	1	2	2	3	3
$\phi(3)$	3	4	2	4	2	3	3	4	1	4	1	3	2	4	1	4	1	2	2	3	1	3	1	2
$\phi(4)$	4	3	4	2	3	2	4	3	4	1	3	1	4	2	4	1	2	1	3	2	3	1	2	1

Definition 6.1.6 Let $n \in \mathbb{N}$, ϕ be a permutation on $\{1, 2, \dots, n\}$, and k be an element of $\{1, 2, \dots, n\}$. We say ϕ fixes k if $\phi(k) = k$; otherwise, we say ϕ moves k. The subset of all elements in $\{1, 2, \dots, n\}$ that are moved by ϕ is denoted by Move(ϕ). The subset of all permutations in $\mathfrak{S}_n$ that fix k is denoted by $(\mathfrak{S}_n)_k$. i.e.,

$$\text{Move}(\phi) = \{k : \phi(k) \neq k\} \text{ and } (\mathfrak{S}_n)_k = \{\phi \in \mathfrak{S}_n : \phi(k) = k\}.$$

For example, in $\mathfrak{S}_3$,

$$\text{Move}\left(\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}\right) = \{2, 3\},\ \text{Move}\left(\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}\right) = \emptyset,$$

$$(\mathfrak{S}_3)_2 = \left\{\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}\right\},\ (\mathfrak{S}_3)_1 = \left\{\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}\right\}.$$

Remark 6.1.7 The element $k \in \text{Move}(\phi)$ if and only if $\phi(k) \in \text{Move}(\phi)$. This result follows directly by the injectivity of ϕ.

Definition 6.1.8 Let $n \in \mathbb{N}$ and ϕ, ψ be two distinct permutations on $\{1, 2, \ldots, n\}$. The permutations ϕ and ψ are said to be disjoint if $\text{Move}(\phi) \cap \text{Move}(\psi) = \emptyset$. Let $\phi_1, \ldots, \phi_m$ be distinct permutations on $\{1, 2, \ldots, n\}$. The permutations $\phi_1, \ldots, \phi_m$ are called pairwise disjoint if ϕ_i, ϕ_j are disjoint for all $i \neq j$, where $1 \leq i, j \leq m$.

Having two disjoint permutations on $\{1, 2, \ldots, n\}$ means that if one of them moves an element k then the other one fixes k. For any integer n, the identity permutation on $\{1, 2, \ldots, n\}$ does not move any element. Therefore, $\text{Move}(e) = \emptyset$, and it is disjoint from other permutations.

Example 6.1.9 The permutations

$$\phi_1 = \begin{pmatrix} 1\,2\,3 & 4\,5 \\ 1\,5\,3 & 2\,4 \end{pmatrix}, \ \phi_2 = \begin{pmatrix} 1\,2\,3 & 4\,5 \\ 3\,2\,1 & 4\,5 \end{pmatrix}$$

are disjoint permutations in $\mathfrak{S}_5$. Similarly,

$$\phi_1 = \begin{pmatrix} 1\,2\,3 & 4\,5\,6 \\ 3\,2\,1 & 4\,5\,6 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1\,2\,3 & 4\,5\,6 \\ 1\,5\,3 & 4\,2\,6 \end{pmatrix} \text{ and}$$
$$\phi_3 = \begin{pmatrix} 1\,2\,3 & 4\,5\,6 \\ 1\,2\,3 & 6\,5\,4 \end{pmatrix}$$

are pairwise disjoint permutations in $\mathfrak{S}_6$. The permutations

$$\phi_1 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$$

are in $\mathfrak{S}_3$ and are not disjoint as $\text{Move}(\phi_1) \cap \text{Move}(\phi_2) = \{1, 2\} \neq \emptyset$.

Proposition 6.1.10 *Let $n \in \mathbb{N}$, and let ϕ, ψ be permutations on $\{1, 2, \ldots, n\}$. If ϕ, ψ are disjoint, then $\phi \circ \psi = \psi \circ \phi$ (any two disjoint permutations commute).*

Proof Assume that ϕ, ψ are disjoint. Let k be an element in $\{1, 2, \ldots, n\}$. Since $\text{Move}(\phi) \cap \text{Move}(\psi) = \emptyset$, only one of the following three cases holds:

1. $k \in \text{Mov}(\phi) \wedge k \notin \text{Mo}v(\psi)$.
2. $k \in \text{Mov}(\psi) \wedge k \notin \text{Mov}(\phi)$.
3. $k \notin \text{Mov}(\phi) \cup \text{Mov}(\psi)$.

If the first case holds, then Remark 6.1.7 implies that $\phi(k) \in \text{Mov}(\phi)$. Thus, $\phi(k) \notin \text{Mov}(\psi)$ and

$$\phi \circ \psi(k) = \phi(\psi(k)) = \phi(k) = \psi(\phi(k)) = \psi \circ \phi(k).$$

Similarly, the second case follows by exchanging the role of ϕ and ψ. For the last case, $\phi(k) = k = \psi(k)$, which implies that

$$\phi \circ \psi(k) = \phi(\psi(k)) = \phi(k) = k = \psi(k) = \psi(\phi(k)).$$

■

According to Lemma 5.4.5 (2),

Corollary 6.1.11 *Let $n \in \mathbb{N}$. If ϕ and ψ are two disjoint permutations on $\{1, 2, \ldots, n\}$, then*

$$(\phi\psi)^k = \phi^k \psi^k \text{ for all } k \in \mathbb{N}.$$

Using Exercises 5.25 and 6.2.7, one can easily show the following corollary.

Corollary 6.1.12 *Let $m \in \mathbb{N}$ and $\phi_1, \phi_2, \ldots, \phi_m$ be a set of pairwise disjoint permutations. If $(\phi_1\phi_2 \ldots \phi_m)^k = e$ for some $k \in \mathbb{N}$, then $\phi_i^k = e$ for each $1 \leq i \leq m$.*

The following example shows that the converse of Proposition 6.1.10 is not true.

Example 6.1.13 On $\{1, 2, 3, 4\}$, consider the permutations

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

As $\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \psi \circ \phi$, the two permutations commute, but they are not disjoint since $\text{Move}(\phi) \cap \text{Move}(\psi) = \{1, 2\} \neq \emptyset$. In general, for any permutation ϕ not equal to the identity, ϕ commutes with itself, but $\text{Move}(\phi) \cap \text{Move}(\phi) = \text{Move}(\phi) \neq \emptyset$, and thus, ϕ and ϕ are not disjoint.

6.2 Cycles on $\{1, 2, \ldots, n\}$

Although the matrix representation gives a complete description of a permutation, there are other representations that are often useful. One such representation based on the notion of cycles.

Definition 6.2.1 Let $n, k \in \mathbb{N}$ and $i_1, i_2, \ldots, i_k$ be distinct elements in $\{1, 2, \ldots, n\}$. A cycle (or a cyclic permutation) $\psi = (i_1 i_2 \ldots i_k)$ on $\{1, 2, \ldots, n\}$ means the function defined on $\{1, 2, \ldots, n\}$ by

$$\psi(j) = \begin{cases} i_{s+1} & j = i_s \wedge 1 \leq s < k \\ i_1 & j = i_k \\ j & j \notin \{i_1, \dots, i_k\} \end{cases}$$

for any $j \in \{1, 2, \dots, n\}$. The number k is called the length of the cycle. A cycle of length k is called a k-cycle, and a 2-cycle is called a transposition. The trivial cycle is a cycle of length 1. Let a be an element in $\{1, 2, \dots, n\}$. We say that a appears in the cycle $(i_1 i_2 \dots i_k)$, denoted by $a \in (i_1 i_2 \dots i_k)$, if $a = i_s$ for some $1 \leq s \leq k$.

Intuitively, a cycle $(i_1 i_2 \dots i_k)$ is the function on $\{1, 2, \dots, n\}$ that takes i_s to the following element in the line, takes the last element to the first element, and fixes all elements that do not appear in the cycle, i.e., $(i_1 i_2 \dots i_k)(i_s) = \begin{cases} i_{s+1} & 1 \leq s < k \\ i_1 & s = k \end{cases}$. For example, the cycle $(3\ 2\ 6\ 4)$ on $\{1, 2, 3, 4, 5, 6\}$ is the function that takes $3 \to 2, 2 \to 6, 6 \to 4, 4 \to 3$ and fixes all other elements in $\{1, 2, 3, 4, 5, 6\}$. The length of $(3\ 2\ 6\ 4)$ is 4. The cycle $(1\ 4)$ is the function on $\{1, 2, 3, 4, 5, 6\}$ that takes $1 \to 4$, $4 \to 1$ and fixes all other elements in $\{1, 2, 3, 4, 5, 6\}$. The length of $(1\ 4)$ is 2. The cycle $(1\ 4)$ represents a transposition. The map $\mathcal{R}_{s,t}$ in Example 1.5.17 is the transposition $(s\ t)$ on $\{1, 2, \dots, n\}$. Using Definition 6.2.1, one can easily verify that for any k such that $1 \leq k \leq n$,

$$(i_2 \dots i_k i_1) = (i_1 i_2 \dots i_k) = (i_k i_1 i_2 \dots i_{k-1})$$

as all of these cycles represent the following function

$$i_1 \to i_2, i_2 \to i_3, \dots, i_{k-1} \to i_k, i_k \to i_1 \wedge j \to j \quad \forall\, j \notin \{i_1, \dots, i_k\}.$$

For example, on $\{1, 2, \dots, 8\}$, the cycles

$$(3\ 1\ 5\ 2), (2\ 3\ 1\ 5), (5\ 2\ 3\ 1), \text{ and } (1\ 5\ 2\ 3)$$

represent the same cycle of length 4. The transposition $(3\ 5)$ exchanges 5 and 3. The cycles $(3\ 1\ 5\ 2)$ and $(3\ 5)$ are visualized as in Fig. 6.3.

Definition 6.2.2 (*Product of cycles*) Let $n, k, r \in \mathbb{N}$, and let $(i_1 i_2 \dots i_k)$ and $(j_1 j_2 \dots j_r)$ be two cycles on $\{1, 2, \dots, n\}$. The product of $(i_1 i_2 \dots i_k)$ and

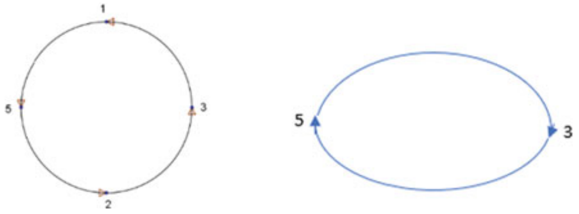

Fig. 6.3 Cycles $(3\ 1\ 5\ 2)$ and $(3\ 5)$

$(j_1 j_2 \ldots j_r)$ is defined as their composition $(i_1 i_2 \ldots i_k) \circ (j_1 j_2 \ldots j_r)$, obtained by applying $(j_1 j_2 \ldots j_r)$ then $(i_1 i_2 \ldots i_k)$. i.e.,

$$(i_1 i_2 \ldots i_k) \circ (j_1 j_2 \ldots j_r)(j) = (i_1 i_2 \ldots i_k)((j_1 j_2 \ldots j_r)(j)).$$

The product of $(i_1 i_2 \ldots i_k)$ and $(j_1 j_2 \ldots j_r)$ is denoted by $(i_1 i_2 \ldots i_k)\ (j_1 j_2 \ldots j_r)$.

Remark 6.2.3 Let $n \in \mathbb{N}$.

1. For each $i \in \{1, 2, \ldots, n\}$, the trivial cycle (i) on $\{1, 2, \ldots, n\}$ maps i to itself and fixes all other elements. Hence,

$$(1) = (2) = \cdots = (i) = \cdots = (n)$$

   all of which represent the identity function on $\{1, 2, \ldots, n\}$.
2. For $i, j \in \{1, 2, \ldots, n\}$ such that $i \neq j$, $(ij)^2 = (ij)(ij) = e$.
3. No representation exists for the identity function as a transposition.

Example 6.2.4

1. On $\{1, 2, 3, 4, 5\}$, consider the two cycles $(2\ 4\ 1)$ and $(3\ 5\ 4)$. The product of the two cycles can computed as $(2\ 4\ 1)(3\ 5\ 4) = (3\ 5\ 1\ 2\ 4)$ or $(3\ 5\ 4)(2\ 4\ 1) = (2\ 3\ 5\ 4\ 1)$. Cleary that the product of cycles need not be commutative.
2. Consider the set $\{1, 2, 3, 4, \ldots, 8\}$. If $\rho = (1\ 4\ 3\ 8)(2\ 6\ 3)(4\ 2)$ (a product of three cycles), then

$$\rho(1) = 4, \rho(2) = 3, \rho(3) = 2, \rho(4) = 6,$$
$$\rho(5) = 5, \rho(6) = 8, \rho(7) = 7, \rho(8) = 1.$$

   The product ρ can be written as a product of the two cycles $(1\ 4\ 6\ 8)(2\ 3)$. However, ρ has no representation as one cycle.
3. On $\{1, 2, 3, 4, \ldots, 10\}$, consider $\sigma = (2\ 5)(2\ 7)(2\ 4)(2\ 1)$. This permutation can be written as one cycle $\sigma = (2\ 1\ 4\ 7\ 5)$.
4. On $\{1, 2, 3, 4, \ldots, 9\}$, $(2\ 3\ 6\ 7\ 9)(3) = (2\ 3\ 6\ 7\ 9)(8) = (2\ 3\ 6\ 7\ 9)(7) = (2\ 3\ 6\ 7\ 9)$.
5. On $\{1, 2, 3, 4, \ldots, 8\}$, $(2\ 5\ 6\ 1\ 7)(4\ 5\ 3\ 2\ 6\ 1) = (4\ 6\ 7\ 2\ 1)(5\ 3)$

$$(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 2) = (2\ 5\ 7\ 4\ 6)$$
$$(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 1) = (1\ 5)(2\ 7\ 4\ 6).$$

6. The product of two cycles is not necessarily a cycle. For example, on $\{1, 2, 3, 4, \ldots, 11\}$, consider $(2\ 5\ 6\ 1\ 7)(4\ 5\ 3\ 2\ 6\ 1)$ and $(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 1)$. Both products are product of cycles but cannot be written as one cycle.

The following lemma is needed later and can be easily proved using Definition 6.2.1 and induction on r.

Lemma 6.2.5 *Let $n \in \mathbb{N}$, and let $(i_1 i_2 \dots i_k)$ be a cycle on $\{1, 2, \dots, n\}$. For any positive integer r and any $1 \leq s \leq k$,*

$$((i_1 i_2 \cdots i_k))^r (i_s) = i_{f(s,r)}$$

where $f(s, r) = \begin{cases} r + s \bmod k \text{ if } r + s \neq qk \text{ for all } q \in \mathbb{N} \\ k \qquad\qquad\quad \text{if } r + s = qk \text{ for some } q \in \mathbb{N} \end{cases}.$

As the product (composition) of the two cycles $(i_1 i_2 \dots i_k)$ and $(i_k i_{k-1} \dots i_1)$ is the identity, both cycles are bijective maps on $\{1, 2, \dots, n\}$. This result is stated in the following proposition.

Proposition 6.2.6 *Let $n, k \in \mathbb{N}$, and let $i_1, i_2, \dots, i_k$ be distinct elements in $\{1, 2, \dots, n\}$. The cycle $(i_1 i_2 \dots i_k)$ is a permutation on $\{1, 2, \dots, n\}$, whose inverse is the cycle $(i_k i_{k-1} \dots i_1)$.*

As an example for applying Proposition 6.2.6, consider the group $\mathfrak{S}_7$ and the permutation $\phi = (2\ 3\ 1\ 4\ 7\ 5)$. The inverse permutation is $\phi^{-1} = (5\ 7\ 4\ 1\ 3\ 2)$. The reader should notice that although the inverse of a cycle is a cycle, the set of all cycles in $\mathfrak{S}_n$ is not closed under the product of cycles (composition in $\mathfrak{S}_n$), as shown in items (2) and (6) in Example 6.2.4. Hence, the subset of all cycles in $\mathfrak{S}_n$ does not form a group under the composition (the product of cycles).

If $(i_1 i_2 \dots i_k)$ is a cycle on $\{1, 2, \dots, n\}$, then by renaming the elements in $\{1, 2, \dots, n\} \backslash \{i_1, i_2, \dots, i_k\}$ to be $i_{k+1}, i_{k+2}, \dots, i_n$, the following corollary can be easily proved:

Corollary 6.2.7 *Let $n, k \in \mathbb{N}$ such that $k \leq n$. Any cycle $(i_1 i_2 \dots i_k)$ on $\{1, 2, \dots, n\}$ has a matrix representation as*

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k & i_{k+1} & i_{k+2} & \dots & i_n \\ i_2 & i_3 & \dots & i_k & i_1 & i_{k+1} & i_{k+2} & \dots & i_n \end{pmatrix}.$$

Example 6.2.8

1. The cycle $(2\ 3\ 1\ 5)$ on $\{1, 2, 3, 4, 5\}$ can be represented as $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,1\,4\,2 \end{pmatrix}$.
2. Let

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

The permutation ϕ is the matrix representation for the cycle $(1\ 4\ 7\ 6\ 3)$.

3. Let

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

The permutation ϕ is a matrix representation for the transposition (1 3).

4. Let

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

The permutation ψ cannot be written as a cycle on $\{1, 2, 3, \ldots, 9\}$. However, it can be written as a product of cycles as: $(1\ 4\ 7\ 6\ 3)(2\ 5\ 9)$.

5. Let

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

The permutation ψ cannot be written as a cycle on $\{1, 2, 3, \ldots, 6\}$. However, it can be written as a product of cycles as: $(1\ 6\ 4)(2\ 3\ 5)$.

6. Consider the group $\mathfrak{S}_7$. If $\phi = (2\ 3\ 1)(4\ 7\ 5)$, then

$$\phi^{-1} = ((2\ 3\ 1)(4\ 7\ 5))^{-1} = (4\ 7\ 5)^{-1}(2\ 3\ 1)^{-1} = (5\ 7\ 4)(1\ 3\ 2).$$

As seen in the above example that certain permutations cannot be written as cycles but can be written as a product of two or more cycles. In general, we have the following proposition.

Proposition 6.2.9 *Let $n \in \mathbb{N}$. Any permutation on $\{1, 2, \ldots, n\}$ can be written as a finite product of disjoint cycles.*

The importance of the decomposition in Proposition 6.2.9 is due to the fact that disjoint cycles commute (Proposition 6.1.10). Therefore, one can write any permutation as a product of commuting cycles. We postpone the proof of the proposition to the subsequent sections. We end this section by recalling the notion of disjoint cycles and presenting several observations. As any cycle is a permutation (Proposition 6.2.6), thus all definitions and universal results for permutations apply to cycles. For example, Definition 6.1.8 still holds for cycles. Proposition 6.1.10 implies that any disjoint cycles on $\{1, 2, \ldots, n\}$ commute, and if ϕ and ψ are two disjoint cycles on $\{1, 2, \ldots, n\}$, then by Corollary 6.1.11,

$$(\phi\psi)^k = \phi^k\psi^k \text{ for all } k \in \mathbb{N}.$$

Lemma 6.2.10 *Let $n \in \mathbb{N}$. If $(i_1 i_2 \ldots i_k)$ is a cycle on $\{1, 2, \ldots, n\}$, then*

$$\text{Move}((i_1 i_2, \ldots, i_k)) = \{i_1, i_2, \ldots, i_k\}.$$

Proof Assume that $\phi = (i_1 i_2 \ldots i_k)$. As $i_1 \xrightarrow{\phi} i_2, i_2 \xrightarrow{\phi} i_3, \ldots, i_{k-1} \xrightarrow{\phi} i_k, i_k \xrightarrow{\phi} i_1$ and all i_s s are distinct, then $\phi(i_s) \neq i_s$ for each $1 \leq s \leq k$. Hence, $\{i_1, i_2, \ldots, i_k\} \subseteq \text{Move}(\phi)$. For the other inclusion, if $j \notin \text{Move}(\phi)$, then by definition of a cycle, $\phi(j) = j$, which implies that $j \notin \{i_1, i_2, \ldots, i_k\}$. ■

The above lemma and Definition 6.1.8 imply the following results:

Corollary 6.2.11 *Let $n, k, r \in \mathbb{N}$. The cycles $(i_1 i_2 \dots i_k)$ and $(j_1 j_2 \dots j_r)$ on $\{1, 2, \dots, n\}$ are disjoint if and only if $i_s \neq j_t$ for all s, t such that $1 \leq s \leq k$, $1 \leq t \leq r$.*

This corollary can be used to decide if two cycles are disjoint. For example, one can directly say that the cycles $(1\ 5)$ and $(2\ 7\ 4\ 6)$ on $\{1, 2, 3, 4, 5, 6, 7\}$ are disjoint while $(2\ 7\ 4\ 3)$ and $(4\ 6\ 3)$ are not.

6.3 Orbits of a Permutation

In this section, we use the elements of $\mathfrak{S}_n$ to define equivalence relations on the set $\{1, 2, \dots, n\}$ where $n \in \mathbb{N}$. Each $\phi \in \mathfrak{S}_n$ defines an equivalence relation on $\{1, 2, \dots, n\}$, dividing the set $\{1, 2, \dots, n\}$ into disjoint sets (equivalence classes) called orbits of ϕ. More information regarding equivalence relations can be found in Sect. 1.4.

Definition 6.3.1 Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. On $\{1, 2, \dots, n\}$ define the relation $\cong_\phi$ by

$$i \cong_\phi j \Leftrightarrow \exists\, m \in \mathbb{Z} \ni j = \phi^m(i), \quad \text{where } i, j \in \{1, 2, \dots, n\}.$$

Lemma 6.3.2 *Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. The relation $\cong_\phi$ in* Definition 6.3.1 *is an equivalence relation.*

Proof For each $i \in \{1, 2, \dots, n\}$, $i = \phi^0(i)$, thus $i \cong_\phi i$ and $\cong_\phi$ is reflexive. Assume that $i \cong_\phi j$. i.e., there exists $m \in \mathbb{Z} \ni j = \phi^m(i)$. Applying the function ϕ^{-m} on both sides yields $i = \phi^{-m}(j)$. Therefore, $\exists\, l = -m \in \mathbb{Z}$ such that $i = \phi^l(j)$, i.e., $j \cong_\phi i$, and $\cong_\phi$ is symmetric. Finally, let $i \cong_\phi j$ and $j \cong_\phi k$. According to the definition of $\cong_\phi$, there exist $m, l \in \mathbb{Z}$ such that $j = \phi^m(i)$ and $k = \phi^l(j)$. Set $s = l + m \in \mathbb{Z}$, then

$$\phi^s(i) = \phi^{l+m}(i) = \phi^l\big(\phi^m(i)\big) = \phi^l(j) = k.$$

i.e., $i \cong_\phi k$ and $\cong_\phi$ is transitive. By Definition 1.4.1, the relation $\cong_\phi$ is an equivalence relation. ■

The equivalence classes generated by the relation $\cong_\phi$ form a partition of the set $\{1, 2, \dots, n\}$ (Theorem 1.4.10). These equivalence classes are called the orbits of ϕ.

Definition 6.3.3 Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. For each $0 \leq i \leq n$, the equivalence class of $\cong_\phi$ that contains i, denoted by $\mathcal{O}r_\phi(i)$, is called the orbit of i under ϕ. The sets $\mathcal{O}r_\phi(i)$, $i \in \{1, 2, \dots, n\}$ are called the orbits of ϕ.

Any two orbits of $\phi \in \mathfrak{S}_n$ (by their construction) are either identical or disjoint, and the union of the orbits of ϕ is the set $\{1, 2, \ldots, n\}$. One also has that for each $i \in \{1, 2, \ldots, n\}$,

$$\begin{aligned}\mathcal{O}r_\phi(i) &= \big\{j \in \{1, 2, \ldots, n\} : i \cong_\phi j\big\} = \big\{j \in \{1, 2, \ldots, n\} : \exists\, m \in \mathbb{Z} \ni j = \phi^m(i)\big\}\\ &= \big\{\phi^m(i) : m \in \mathbb{Z}\big\}.\end{aligned}$$

Proposition 6.3.4 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \ldots, n\}$. The orbit of i under ϕ is a nonempty finite set given by*

$$\mathcal{O}r_\phi(i) = \big\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\big\}$$

where *k is the smallest nonnegative integer satisfying $\phi^k(i) = i$.*

Proof Let $i \in \{1, 2, \ldots, n\}$. As $i = \phi^0(i) \in \{\phi^m(i) : m \in \mathbb{Z}\} = \mathcal{O}r_\phi(i) \subseteq \{1, 2, \ldots, n\}$, then $\mathcal{O}r_\phi(i)$ is a nonempty finite set. Hence, there exist $m_1, m_2 \in \mathbb{Z}$ such that

$$m_1 < m_2 \text{ and } \phi^{m_1}(i) = \phi^{m_2}(i).$$

Applying the function ϕ^{-m_1} on both sides yields $\phi^{m_2-m_1}(i) = i$; i.e., there exists a nonnegative integer $s = m_2 - m_1$ such that $\phi^s(i) = i$. Let k be the smallest nonnegative integer satisfying $\phi^k(i) = i$ and $B = \big\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\big\}$, we show that $B = \mathcal{O}r_\phi(i)$. Since

$$B = \big\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\big\} \subseteq \big\{\phi^m(i) : m \in \mathbb{Z}\big\} = \mathcal{O}r_\phi(i),$$

then $B \subseteq \mathcal{O}r_\phi(i)$. For the other inclusion, let $\phi^m(i)$ be any element of $\mathcal{O}r_\phi(i)$ where $m \in \mathbb{Z}$. Applying the Euclidean Algorithm 2.4.1 on m, k, gives that there exist two integers $q, r \in \mathbb{Z}$ such that

$$m = qk + r, \quad 0 \le r < k.$$

That is,

$$\phi^m(i) = \phi^{r+qk}(i) = \phi^r\left(\phi^{qk}(i)\right) = \phi^r\left(\left(\phi^k\right)^q(i)\right)$$

$$= \begin{cases} \phi^r\left(\underbrace{\phi^k \circ \phi^k \circ \cdots \circ \phi^k(i)}_{q \text{ times}}\right) = \phi^r(i) & q \ge 0 \\ \phi^r\left(\underbrace{\phi^{-k} \circ \phi^{-k} \circ \cdots \circ \phi^{-k}(i)}_{-q \text{ times}}\right) = \phi^r(i)\; q < 0 \end{cases}$$

i.e., $\phi^m(i) = \phi^r(i) \in B$, which implies that $\mathcal{O}r_\phi(i) \subseteq B$. ■

The last proposition provides a practical method for determining the orbits of a permutation ϕ in $\mathfrak{S}_n$, as follows:

- Begin by choosing an integer $i \in \{1, 2, \dots, n\}$, and compute $\phi(i), \phi^2(i), \dots$ until i is reached.
- The set $\left\{\phi(i), \phi^2(i), \dots, i\right\}$ forms $\mathcal{O}r_\phi(i)$, the first orbit.
- Choose an integer from the set $\{1, 2, \dots, n\} \backslash \mathcal{O}r_\phi(i)$ and compute its orbit in the same way as the first orbit.
- Repeat the same process until the obtained orbits contains all the elements in $\{1, 2, \dots, n\}$.

Example 6.3.5 Let

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$$

be a permutation on $\{1, 2, \dots, 11\}$. The orbits of ϕ can be obtained as follows:

- By choosing a number in $\{1, 2, \dots, 11\}$, say $i = 2$, one can compute
$$\phi(2) = 6, \phi^2(2) = \phi(6) = 5, \phi^3(2) = \phi(5) = 2$$
to obtain $\mathcal{O}r_\phi(2) = \{2, 5, 6\}$.
- Select a number in the set $\{1, 2, \dots, 11\} \backslash \{2, 5, 6\}$, say $i = 1$. Compute
$$\phi(1) = 9, \phi(9) = 3, \phi(3) = 8, \phi(8) = 1$$
to obtain $\mathcal{O}r_\phi(1) = \{1, 3, 8, 9\}$.
- Choose a number in $\{1, 2, \dots, 11\} \backslash \{2, 5, 6, 1, 3, 8, 9\}$, say $i = 4$. Compute $\phi(4) = 10, \phi(10) = 4$ to obtain $\mathcal{O}r_\phi(4) = \{4, 10\}$.
- Choose a number in $\{1, 2, \dots, 11\} \backslash \{2, 5, 6, 1, 3, 8, 9, 4, 10\}$, say $i = 7$. Compute $\phi(7) = 7$ to obtain $\mathcal{O}r_\phi(7) = \{7\}$.
- Only one element remains in the set $\{1, 2, \dots, 11\} \backslash \{2, 5, 6, 1, 3, 8, 9, 4, 10, 7\}$, which is 11. Compute $\phi(11) = 11$, which yields$\mathcal{O}r_\phi(11) = \{11\}$.
- Terminate the process as there are no elements remain in $\{1, 2, \dots, 11\}$.

Thus, all the distinct orbits of ϕ are $\{2, 6, 5\}, \{1, 9, 3, 8\}, \{4, 10\}, \{7\}, \{11\}$. Note that since the orbits of a permutation are equivalence classes (either identical or disjoint), then $\mathcal{O}r_\phi(5) = \mathcal{O}r_\phi(6) = \{2, 5, 6\}$, $\mathcal{O}r_\phi(9) = \mathcal{O}r_\phi(3) = \mathcal{O}r_\phi(8) = \{1, 3, 8, 9\}$, and $\mathcal{O}r_\phi(10) = \{4, 10\}$.

The following definition restates Definition 1.5.3 using the notation of this chapter. We remind the reader that any permutation $\phi \in \mathfrak{S}_n$ is a bijective function from $\{1, 2, \dots, n\}$ to itself.

Definition 6.3.6 Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $A \subseteq \{1, 2, \dots, n\}$. The restriction of ϕ on the subset A, denoted by $\phi_{|A}$ is the function on A that satisfies $\phi_{|A}(x) = \phi(x)\ \forall\, x \in A$.

The next proposition shows that the restriction of a permutation on one of its orbits is a cycle that is formed by the elements of such an orbit.

Proposition 6.3.7 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \dots, n\}$. The restriction of ϕ on $\mathcal{O}r_\phi(i)$ is the cycle $\big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)$ on $\{1, 2, \dots, n\}$. i.e.,*

$$\phi_{|\mathcal{O}r_\phi(i)} = \big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)$$

where kis the smallest nonnegative integer satisfying $\phi^k(i) = i$.

Proof Assume that $i \in \{1, 2, \dots, n\}$. We show that

$$\phi_{|\mathcal{O}r_\phi(i)}(j) = \big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)(j) \quad \forall\, j \in \mathcal{O}r_\phi(i).$$

Let $j \in \mathcal{O}r_\phi(i)$. Since $\mathcal{O}r_\phi(i) = \big\{i, \phi(i), \phi^2(i), \dots, \phi^{k-1}(i)\big\}$, there exists an integer s such that $0 \le s \le k-1$ and $j = \phi^s(i)$. Using Definition 6.2.1, we obtain

$$\begin{aligned}
\big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)(j) &= \big(i\ \phi(i)\phi^2(i) \dots \phi^{k-1}(i)\big)\big(\phi^s(i)\big) \\
&= \begin{cases} \phi^{s+1}(i) & 0 \le s < k-1 \\ i & s = k-1 \end{cases} \\
&= \begin{cases} \phi^{s+1}(i) & 0 \le s < k-1 \\ \phi^k(i) & s = k-1 \end{cases} \\
&= \phi^{s+1}(i) = \phi\big(\phi^s(i)\big) = \phi(j) = \phi_{|\mathcal{O}r_\phi(i)}(j).
\end{aligned}$$

■

Intuitively, the pervious proposition indicates that if ϕ is a permutation on $\{1, 2, \dots, n\}$, then for each $i \in \{1, 2, \dots, n\}$, the restriction $\phi_{|\mathcal{O}r_\phi(i)}$ is the cycle obtained by inserting i as the first element in the cycle and continuously applying ϕ on the element to obtain the next one. This process is repeated until all the elements in the orbit have been considered.

Example 6.3.8

1. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$.

   The orbits of ϕ are

   $$\{1, 3, 8, 9\}, \{2, 5, 6\}, \{4, 10\}, \{7\}, \{11\} \text{ (Example 6.3.5).}$$

   Therefore, according to the results of the last proposition,

$$\phi_{|\{1,3,8,9\}} = (1\ 9\ 3\ 8), \phi_{|\{7\}} = (7), \phi_{|\{2,5,6\}} = (2\ 6\ 5), \phi_{|\{4,10\}} = (4\ 10),\ \ \phi_{|\{11\}} = (11).$$

2. The orbits of $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ as a permutation in $\mathfrak{S}_4$ are

$$\mathcal{O}r_\phi(1) = \{1, 2, 3\} = \mathcal{O}r_\phi(2) = \mathcal{O}r_\phi(3),\ \ \mathcal{O}r_\phi(4) = \{4\}.$$

The permutation ϕ has only one orbit that contains more than one element. Therefore, ϕ is a cycle.

Corollary 6.3.9 *Let $n \in \mathbb{N}$, and $\phi \in \mathfrak{S}_n$. For each $i \in \{1, \ldots, n\}$* not fixed by ϕ,

$$\text{Move}\Big(\phi_{|\mathcal{O}r_\phi(i)}\Big) = \mathcal{O}r_\phi(i).$$

Proof Let $i \in \{1, 2, \ldots, n\}$. The results of Lemma 6.2.10, Propositions 6.3.4, and 6.3.7 can be used to obtain

$$\begin{aligned}\text{Move}\Big(\phi_{|\mathcal{O}r_\phi(i)}\Big) &= \text{Move}\big((i\ \phi(i)\phi^2(i)\ldots\phi^{k-1}(i))\big) \\ &= \big\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\big\} = \mathcal{O}r_\phi(i).\end{aligned}$$

■

As the orbits of ϕ (by construction) are disjoint, the following direct result can be obtained.

Corollary 6.3.10 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \ldots, n\}$. The cycles obtained by the restriction of ϕ on its orbits are disjoint cycles.*

Next, we prove Proposition 6.2.9 by showing that any permutation ϕ is a product of the cycles obtained by the restrictions of ϕ on its orbits.

Proof of Proposition 6.2.9

Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $A_1, \ldots, A_m$ be the distinct orbits of ϕ. For each $1 \leq j \leq m$, let ψ_j be the cycle obtained by the restriction of ϕ on A_j. We show that

$$\phi(i) = \psi_m \circ \psi_{m-1} \circ \cdots \circ \psi_2 \circ \psi_1(i)\ \text{ for each }\ i \in \{1, 2, \ldots, n\}.$$

Assume $i \in \{1, 2, \ldots, n\}$. As the orbits of ϕ form a partition for $\{1, 2, \ldots, n\}$, there exists l, $1 \leq l \leq m$ such that $i \in A_l$ and $i \notin A_j$ for all $j \neq l$. Therefore, $i \in \text{Move}(\psi_l)$ and $i \notin \text{Move}\big(\psi_j\big)$ for all $j \neq l$ (Corollary 6.3.9). Therefore,

- $\psi_j(i) = i$ for each $1 \leq j < l$
- $\psi_l(i) = \phi(i)$ (Proposition 6.3.7)
- $\psi_j(\phi(i)) = \phi(i)$ for each $l < j \leq m$

where the last line follows by Remark 6.1.7. That is,

$$\psi_{l-1} \circ \cdots \circ \psi_1(i) = i,\ \psi_l(i) = \phi(i), \quad \psi_m \circ \cdots \circ \psi_{l+1}(\phi(i)) = \phi(i)$$

which implies

$$\psi_m \circ \cdots \circ \psi_1(i) = \psi_m \circ \cdots \circ \psi_{l+1}(\psi_l(\psi_{l-1} \circ \cdots \circ \psi_1(i))) = \phi(i).$$

According to Corollary 6.3.10, the cycles ψ_j are disjoint. ■

Example 6.3.11

1. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$ be a permutation in $\mathfrak{S}_{11}$. The distinct orbits of ϕ are $\{1, 9, 3, 8\}$, $\{2, 6, 5\}$, $\{4, 10\}$, $\{7\}$, $\{11\}$, and the corresponding cycles are

$$(1\ 9\ 3\ 8), (2\ 6\ 5), (4\ 10), (7), (11).$$

Hence, ϕ can be written as the following product of disjoint cycles

$$\phi = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10)(7)(11) = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10).$$

2. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 2 & 7 & 4 \end{pmatrix}$ be a permutation in $\mathfrak{S}_7$. Similar to (1), the permutation ϕ can be written as a product of disjoint cycles as follows:

$$\phi = (1\ 3)(2\ 5)(4\ 6\ 7).$$

The reader may notice that

- For a permutation $\phi \in \mathfrak{S}_n$, the number of disjoint cycles (with a length greater than one) form ϕ is less than $n/2$. This occurs because of the simple fact that if the set $\{1, 2, \ldots, n\}$ was divided into disjoint subsets where each subset contains at least two elements, then the number of such subsets must be less than or equal to half of the original set.
- The set of distinct orbits (equivalence classes) of the permutation ϕ is unique (Corollary 1.4.14). Therefore, if all the cycles (length one included) are considered in writing the permutation as a product of disjoint cycles, this product will be unique up to cycle rearrangements.

Proposition 6.3.12 *Let $n \in \mathbb{N}$. If all cycles of length one are considered, then any permutation on $\{1, 2, \ldots, n\}$ can be uniquely (up to rearrangement) written as a finite product of disjoint cycles.*

Example 6.3.13 Using the results of Example 6.1.4, one can easily verify that the group $\mathfrak{S}_1$ consists of only 1-cycle (identity permutation). For $n = 2$, the symmetric group $\mathfrak{S}_2 = \{(1), (12)\}$ consists of two cycles: 1-cycle and 2-cycle (a transposition). The group $\mathfrak{S}_3$ consists of six cycles: one 1-cycle, two 2-cycles, and three 3-cycles. The group $\mathfrak{S}_4$ contains cycles and permutations that cannot be written as one cycle. The elements of $\mathfrak{S}_4$ consist of one 1-cycle, six 2-cycles, eight 3-cycles, six 4-cycles, and three permutations written as a product of two cycles. Similarly, one can continue to analyze the structure of $\mathfrak{S}_n$ using the multiplication rule, as in Example 6.1.4.

6.4 Order of a Permutation

For any $n \in \mathbb{N}$, the orders of the permutations in $\mathfrak{S}_n$ can be investigated. We start with an example of which computing ϕ^k for different permutation ϕ in $\mathfrak{S}_n$ for some chosen k and n.

Example 6.4.1

1. In $(\mathfrak{S}_5, \circ)$, if $\phi = (1\ 2\ 3\ 4)$, then

$$\begin{aligned}\phi^2 &= (1\ 2\ 3\ 4)^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (13)(24)\\ \phi^3 &= (1\ 2\ 3\ 4)^3 = (1\ 2\ 3\ 4)(13)(24) = (1\ 4\ 3\ 2)\\ \phi^4 &= \phi^2\phi^2 = (13)(24)(13)(24) = (13)(13)(24)(24) = (1)(2) = e.\end{aligned}$$

2. In $(\mathfrak{S}_3, \circ)$, if $\phi = (1\ 2)$, then

$$\begin{aligned}\phi^2 &= (1\ 2)^2 = (1) = e.\\ \phi^3 &= (1\ 2)^3 = (1\ 2)(1\ 2)^2 = (1\ 2)e = (1\ 2).\end{aligned}$$

   In general, $\phi^{2k+1} = (1\ 2)$, and $\phi^{2k} = e$ for any integer k.

3. In $(\mathfrak{S}_7, \circ)$, if $\phi = (1\ 2\ 3)(2\ 7\ 1\ 6)$, then $\phi = (1\ 6\ 3)(2\ 7)$ and

$$\begin{aligned}\phi^2 &= ((1\ 6\ 3)(2\ 7))^2 = (1\ 6\ 3)(2\ 7)(1\ 6\ 3)(2\ 7)\\ &= (1\ 6\ 3)(1\ 6\ 3)(2\ 7)(2\ 7) = ((1\ 6\ 3))^2 = (1\ 3\ 6)\\ \phi^3 &= \phi^2\phi = (1\ 3\ 6)(1\ 6\ 3)(2\ 7) = (2\ 7)\\ \phi^4 &= \phi^3\phi = (2\ 7)(1\ 6\ 3)(2\ 7) = (2\ 7)(2\ 7)(1\ 6\ 3) = (1\ 6\ 3)\\ \phi^5 &= \phi^4\phi = (1\ 6\ 3)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(2\ 7)\\ \phi^6 &= \phi^5\phi = (1\ 3\ 6)(2\ 7)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(1\ 6\ 3)(2\ 7)(2\ 7) = e.\end{aligned}$$

4. In $(\mathfrak{S}_6, \circ)$, if $\phi = (2\ 5\ 4)(6\ 3\ 1)(4\ 3)$, then

$$\begin{aligned}
\phi &= (1\ 6\ 3\ 2\ 5\ 4)\\
\phi^2 &= (1\ 3\ 5)(2\ 4\ 6)\\
\phi^3 &= \phi^2\phi = (1\ 2)(3\ 4\ )(5\ 6)\\
\phi^4 &= \phi^2\phi^2 = (1\ 5\ 3)(2\ 6\ 4)\\
\phi^5 &= \phi^4\phi = (1\ 4\ 5\ 2\ 3\ 6)\\
\phi^6 &= \phi^5\phi = (1\ 4\ 5\ 2\ 3\ 6)(1\ 6\ 3\ 2\ 5\ 4) = e.
\end{aligned}$$

The reader may note that computing ϕ^k becomes increasingly complicated as k and n become bigger, and some of the above computations were cumbersome. The computations of the exponent can be simplified using Propositions 6.2.9, and 6.2.6 and the results presented in this section. The following lemma computes the order of a cycle. Recall the order of an element in a group defined in Sect. 5.5.

Lemma 6.4.2 *Let $n \in \mathbb{N}$. The order of a cycle in $\mathfrak{S}_n$ is equal to its length, i.e.,*

$$\operatorname{ord}((i_1 i_2 \dots i_k)) = k$$

where $i_1, i_2, \dots, i_k$ are elements in $\{1, 2, \dots, n\}$. In particular, the order of a transposition is 2.

Proof We show that k is the smallest positive integer such that $(i_1 i_2 \dots i_k)^k = e$. Let $1 \le s \le k$. By Lemma 6.2.5,

$$(i_1 i_2 \dots i_k)^k (i_s) = i_{f(s,k)}$$

where

$$\begin{aligned}
f(s,k) &= \begin{cases} k+s \mod k & \text{if } \ k+s \neq qk \text{ for all } q \in \mathbb{N}\\ k & \text{if } \ k+s = qk \text{ for some } q \in \mathbb{N}\end{cases}\\
&= \begin{cases} s \mod k & \text{if } \ k+s \neq qk \text{ for all } q \in \mathbb{N}\\ k & \text{if } \ k+s = qk \text{ for some } q \in \mathbb{N}\end{cases}
\end{aligned}$$

Since $1 \le s \le k$, then $k+1 \le s+k \le 2k$, which implies that the only possibility for $s+k$ to be a multiple of k is $2k$, i.e.,

$$\begin{aligned}
f(s,k) &= \begin{cases} s \mod k & k+s \neq 2k\\ k & k+s = 2k\end{cases}\\
&= \begin{cases} s \mod k & s \neq k\\ k & s = k\end{cases}\\
&= s.
\end{aligned}$$

i.e., $(i_1 i_2 \dots i_k)^k (i_s) = i_s$ for each $1 \le s \le k$, and $(i_1 i_2 \dots i_k)^k = e$. Let r be a positive integer such that $r < k$. We compute $(i_1 i_2 \dots i_k)^r (i_1)$ as follows:

$$(i_1 i_2 \dots i_k)^r(i_1) = i_{f(1,r)}$$

where

$$f(1,r) = \begin{cases} r+1 \bmod k & \text{if } r+1 \neq qk \text{ for all } q \in \mathbb{N} \\ k & \text{if } r+1 = qk \text{ for some } q \in \mathbb{N}. \end{cases}$$

Since $r < k$, we have $r+1 < k+1 \leq 2k$, which implies that the only possibility for $r+1$ to be a multiple of k is k. i.e.,

$$f(1,r) = \begin{cases} r+1 \bmod k & \text{if } r+1 \neq k \\ k & \text{if } r+1 = k. \end{cases}$$

In both cases $f(1,r) = r+1 \neq 1$. i.e., $(i_1 i_2 \dots i_k)^r(i_1) \neq i_1$. Therefore $((i_1 i_2 \dots i_k))^r \neq e$. ■

Since every permutation in $\mathfrak{S}_n$ is a finite product of disjoint commuting cycles, one can calculate the order of a permutation using the orders (lengths) of its factor cycles using the following lemma.

Proposition 6.4.3 *Let $n \in \mathbb{N}$. The order of a permutation is the least common multiple of the orders of its factor disjoint cycles. i.e., if $\psi_1, \psi_2, \dots, \psi_s$ are a set of pairwise disjoint cycles such that length ψ_i equals k_i, where $1 \leq i \leq s$, then*

$$\operatorname{ord}(\psi_1\psi_2\cdots\psi_s) = \operatorname{lcm}(k_1, k_2, \dots, k_s).$$

Proof Let $l = \operatorname{lcm}(k_1, k_2, \dots, k_s)$. For each $1 \leq i \leq s$, there exists an integer m_i such that $l = k_i m_i$. As $\psi_1, \psi_2, \dots, \psi_s$ are pairwise disjoint cycles, they commute, which implies that

$$\begin{aligned}(\psi_1\psi_2\cdots\psi_s)^l &= (\psi_1)^l(\psi_2)^l\cdots(\psi_s)^l = (\psi_1)^{k_1m_1}(\psi_2)^{k_2m_2}\cdots(\psi_s)^{k_sm_s} \\ &= e\cdot e\cdots e = e.\end{aligned}$$

By Lemma 5.5.6, $\operatorname{ord}(\psi_1\psi_2\cdots\psi_s)$ divides l. On another hand, since

$$(\psi_1\psi_2\dots\psi_s)^{\operatorname{ord}(\psi_1\psi_2\dots\psi_s)} = e$$

and the cycles $\psi_1, \psi_2, \dots, \psi_s$ are disjoint, by Corollary 6.1.12, $\psi_i^{\operatorname{ord}(\psi_1\psi_2\dots\psi_s)} = e$ for each $1 \leq i \leq s$, which implies that k_i divides $\operatorname{ord}(\psi_1\psi_2\dots\psi_s)$ for each $1 \leq i \leq s$. Therefore, the least common multiple $l = \operatorname{lcm}(k_1, k_2, \dots, k_s)$ divides $\operatorname{ord}(\psi_1\psi_2\dots\psi_s)$. Proposition 2.2.5 (3) implies the result. ■

Considering the above results, we compute some of the permutations in Example 6.4.1, leaving the others as an exercise:

- In $(\mathfrak{S}_5, \circ)$, if $\phi = (1\ 2\ 3\ 4)$, then $\operatorname{ord}(\phi) = 4$, and

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

- In $(\mathfrak{S}_7, \circ)$, let $\phi = (1\ 2\ 3)(2\ 7\ 1\ 6)$. The permutation ϕ is not a cycle but can be written as a product of disjoint cycles $\phi = (1\ 6\ 3)(2\ 7)$. Thus, $\mathrm{ord}(\phi) = \mathrm{lcm}(3, 2) = 6$, and

$$\begin{aligned}
\phi^2 &= ((1\ 6\ 3)(2\ 7))^2 = ((1\ 6\ 3))^2 = (1\ 3\ 6)\\
\phi^3 &= \phi^2\phi = (1\ 3\ 6)(1\ 6\ 3)(2\ 7) = e(2\ 7) = (2\ 7)\\
\phi^4 &= ((1\ 3\ 6))^2 = (1\ 6\ 3)\\
\phi^5 &= \phi^4\phi = (1\ 6\ 3)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(2\ 7)\\
\phi^6 &= e.
\end{aligned}$$

- In $(\mathfrak{S}_6, \circ)$, let $\phi = (2\ 5\ 4)(6\ 3\ 1)(4\ 3)$. This permutation is a product of cycles that are not disjoint. By rewriting ϕ as a product of disjoint cycles, we obtain $\phi = (1\ 6\ 3\ 2\ 5\ 4)$, a 1-cycle of length 6. Therefore, $\mathrm{ord}(\phi) = 6$.

Example 6.4.4 Consider the permutation $\phi = (2\ 4)(1\ 3\ 6)$ in $\mathfrak{S}_7$. To find ϕ^{100}, one first computes the order of ϕ. As ϕ is a product of disjoint cycles, $\mathrm{ord}(\phi) = \mathrm{lcm}(2, 3) = 6$. i.e., $\phi^6 = e$. Applying the division algorithm on 6 and 100 yields $100 = 16 \times 6 + 4$. Thus,

$$\begin{aligned}
\phi^{100} &= \phi^{4+16\times 6} = \phi^4\left(\phi^6\right)^{16}\\
&= \phi^4(e)^{16} = \phi^4.
\end{aligned}$$

The cycles $(2\ 4)$ and $(1\ 3\ 6)$ are disjoint, and thus, they commute. Consequently,

$$\phi^4 = ((2\ 4)(1\ 3\ 6))^4 = (2\ 4)^4(1\ 3\ 6)^4.$$

Since $(2\ 4)^4 = \left((2\ 4)^2\right)^2 = e^2 = e$ and $(1\ 3\ 6)^4 = (1\ 3\ 6)^3(1\ 3\ 6)^1 = e(1\ 3\ 6) = (1\ 3\ 6)$, then $\phi^4 = (1\ 3\ 6)$.

The next example shows that both conditions $a * b = b * a$ and $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$ in Proposition 5.5.11 cannot be eliminated.

Example 6.4.5 The cycles $(1\ 2)$, $(1\ 3)$, and $(3\ 4)$ are elements in the group $\mathfrak{S}_4$. Each of these cycles is a cycle of order 2, and

$$\begin{aligned}
\mathrm{ord}((1\ 2)(1\ 3)) &= \mathrm{Ord}((1\ 3\ 2)) = 3 \neq 4 = \mathrm{ord}((1\ 2)) \cdot \mathrm{ord}((1\ 3))\\
\mathrm{ord}((1\ 2)(1\ 3\ 4)) &= \mathrm{Ord}((1\ 3\ 4\ 2)) = 4 \neq 6 = \mathrm{ord}((1\ 2)) \cdot \mathrm{ord}((1\ 3\ 4))\\
\mathrm{ord}((1\ 2)(3\ 4)) &= 2 \neq 4 = \mathrm{ord}((1\ 2)) \cdot \mathrm{ord}((3\ 4)).
\end{aligned}$$

The next example shows that the assumption for a group G to be abelian in Proposition 5.5.13 is essential. Recall that for any $m \in \mathbb{Z}$, $mG = \{a^m : a \in G\}$ and $G[m] = \{a \in G : a^m = e\}$.

Example 6.4.6 Consider the symmetric group $\mathfrak{S}_4$. As shown in Example 6.3.13, the group $\mathfrak{S}_4$ consists of one 1-cycle, six 2-cycles, eight 3-cycles, six 4-cycles, and three products of 2-cycles. Each of these permutations, except the 3-cycles, has an order that divides 4. Therefore,

1. The set $4\mathfrak{S}_4$ contains only the identity and the 3-cycles. Since $(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$ is not an element in $4\mathfrak{S}_4$, the set $4\mathfrak{S}_4$ is not closed under the product of cycles, so it is not a group.
2. The set $\mathfrak{S}_4[4]$ contains all the permutations, except the 3-cycles. Since $(1\ 2)(2\ 4) = (1\ 2\ 4)$ is not an element of $\mathfrak{S}_4[4]$, the set $\mathfrak{S}_4[4]$ is not closed under the product of cycles, so it is not a group.

6.5 Odd and Even Permutations

In this section, each permutation in $\mathfrak{S}_n$ for $n \in \mathbb{N}$ is classified as an even or odd permutation. For $n > 1$, this determination is based on expressing a permutation ϕ as a finite product of transpositions. Expressing ϕ as a product of transpositions can be performed by expressing the permutation as a product of cycles, then writing each cycle as a product of transpositions. In the case where $n = 1$, the group $\mathfrak{S}_1$ has only one cycle of length 1. Hence, no transposition in $\mathfrak{S}_1$. Recall that a cycle $(i_1 i_2 \ldots i_k)$ in $\mathfrak{S}_n$, where $2 \le k \le n$, is

$$(i_1 i_2 \ldots i_k)(i_s) = \begin{cases} i_{s+1} & 1 \le s < k \\ i_1 & s = k \end{cases} \quad \text{for } 1 \le s \le k.$$

Proposition 6.5.1 *Let $n \in \mathbb{N}$ such that $n > 1$. Any cycle in $\mathfrak{S}_n$ can be written as a product of transpositions. Namely, $e = (i_1 i_2)(i_1 i_2)$ for any $i_1 \neq i_2$ and*

$$(i_1 i_2 \ldots i_k) = (i_1 i_k)(i_1 i_{k-1}) \ldots (i_1 i_3)(i_1 i_2) \quad \text{for any } 2 \le k \le n.$$

Proof The statement for the identity element is clear. Let $n \ge 2$ and assume that $(i_1 i_2 \ldots i_k)$ is a cycle in $\mathfrak{S}_n$. It suffices to show that $(i_1 i_2 \ldots i_k)(i_s) = (i_1 i_k)(i_1 i_{k-1}) \ldots (i_1 i_3)(i_1 i_2)(i_s)$ for any $1 \le s \le k$.

- If $s = 1$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \ldots (i_1 i_3)(i_1 i_2)$ on i_1 is given by the steps

$$i_1 \xrightarrow{(i_1 i_2)} i_2 \xrightarrow{(i_1 i_3)} i_2 \cdots i_2 \xrightarrow{(i_1 i_{k-1})} i_2 \xrightarrow{(i_1 i_k)} i_2$$

and yields i_2, which is $(i_1 i_2 \ldots i_k)(i_1)$.

- If $1 < s < k$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)$ on i_s is given by the steps

$$i_s \xrightarrow{(i_1 i_2)} i_s \xrightarrow{(i_1 i_3)} i_s \cdots \xrightarrow{(i_1 i_{s-1})} i_s \xrightarrow{(i_1 i_s)} i_1 \xrightarrow{(i_1 i_{s+1})} i_{s+1} \xrightarrow{(i_1 i_{s+2})} i_{s+1} \cdots i_{s+1} \xrightarrow{(i_1 i_k)} i_{s+1}$$

Thus, $i_{s+1} = (i_1 i_2 \dots i_k)(i_s)$.

- If $s = k$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)$ to i_k is given by the steps

$$i_k \xrightarrow{(i_1 i_2)} i_k \xrightarrow{(i_1 i_3)} i_k \cdots i_k \xrightarrow{(i_1 i_{k-1})} i_k \xrightarrow{(i_1 i_k)} i_1$$

and yields $i_1 = (i_1 i_2 \dots i_k)(i_k)$.

Hence, the equality is satisfied for all $1 \leq s \leq k$. ■

Remark 6.5.2

1. According to the previous proposition, any cycle of length k, where $k > 1$, can be written as a product of $k - 1$ transpositions.
2. For any $n \in \mathbb{N}$, and for any $i, j \in \{1, 2, \dots, n\}$ such that $i \neq j$, the transposition (ij) can be written as $(ij) = (aj)(ai)(aj)$, where $a \in \{1, 2, \dots, n\} \backslash \{i, j\}$.

Corollary 6.5.3 *Let $n \in \mathbb{N}$ such that $n > 1$.*

1. *Any permutation in $\mathfrak{S}_n$ can be written as a product of a finite number of transpositions.*
2. *Any permutation in $\mathfrak{S}_n$ can be written as a product of a finite number of transpositions of the form (ak_i) for fixed $a \in \{1, 2, \dots, n\}$ with $k_i \in \{1, 2, \dots, n\} \backslash \{a\}$.*

Example 6.5.4 Consider the group $(\mathfrak{S}_9, \circ)$

$$\begin{aligned} e &= (5\ 8)(5\ 8),\ e = (1\ 2\ 3)(3\ 2\ 1) = (1\ 3)(1\ 2)(3\ 1)(3\ 2), \\ &= (1\ 3)(1\ 2)(1\ 3)(1\ 3)(1\ 2)(1\ 3). \\ \phi &= (3\ 6\ 4\ 2)(5\ 8\ 7) = (3\ 2)(3\ 4)(3\ 6)(5\ 7)(5\ 8) \\ &= (3\ 2)(3\ 4)(3\ 6)(3\ 7)(3\ 5)(3\ 7)(3\ 8)(3\ 5)(3\ 8). \\ \psi &= (4\ 3\ 5\ 1) = (4\ 1)(4\ 5)(4\ 3). \end{aligned}$$

Using Corollary 6.5.3, one can classify the permutations into odd and even permutations, as follows

Definition 6.5.5 Let $n \in \mathbb{N}$ such that $n > 1$, and $\phi \in \mathfrak{S}_n$. We say that ϕ is an odd permutation if it can be written as a product of an odd number of transpositions. We say that ϕ is an even permutation if ϕ can be written as a product of an even number of transpositions.

Example 6.5.6

1. The identity permutation is an even permutation.
2. Let

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}.$$

   As $\phi = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10) = (1\ 8)(1\ 3)(1\ 9)(2\ 5)(2\ 6)(4\ 10)$, then ϕ is even.
3. Let

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

   The permutation $\phi = (1\ 3\ 5\ 2\ 4\ 6)$ is a cycle of length 6, and thus, it is an odd permutation.

Writing a permutation as a product of transpositions is not unique. For example, if $\phi = \tau_m \dots \tau_2\tau_1$, where $\tau_1, \tau_2, \dots, \tau_m$ are transpositions, then

$$\tau_m \dots \tau_2\tau_1(1\ 3)(1\ 2)(3\ 1)(3\ 2) \text{ and } \tau_m \dots \tau_2\tau_1(5\ 8)(5\ 8)$$

are equal to ϕ. However, if ϕ is represented as a product of an odd (resp. even) number of transpositions, then the number of transpositions in any other such representation of ϕ must be odd (resp. even). In the remainder of this section, we prove that any permutation ϕ cannot be simultaneously even and odd. We show the result for the identity permutation, and then for the general case. The following technical lemmas are needed.

Lemma 6.5.7 *Let $n \in \mathbb{N}$ such that $n > 1$. If σ and (ij) are different transpositions in $\mathfrak{S}_n$, then there exists a transposition τ in $\mathfrak{S}_n$ and $l \in \{1, 2, \dots, n\}$ such that $i \notin \tau$ and $\sigma(ij) = (il)\tau$.*

Proof If σ and (ij) are disjoint cycles, they commute, and the result follows by putting $\tau = \sigma$ and $l = j$. If σ and (ij) are not disjoint, then $\sigma = (is)$ or $\sigma = (sj)$ for some $s \in \{1, 2, \dots, n\}\backslash\{i, j\}$.

- If $\sigma = (is)$, then

$$\sigma(ij) = (is)(ij) = (ijs) = (jsi) = (ji)(js) = (ij)(js).$$

  and the result follows by putting $\tau = (js)$ and $l = j$.
- If $\sigma = (sj)$, then

$$\sigma(ij) = (sj)(ij) = (jis) = (sji) = (si)(sj) = (is)(js)$$

  and the result follows by putting $\tau = (js)$ and $l = s$. ∎

Lemma 6.5.8 *Let $n \in \mathbb{N}$, $n > 1$, and $\phi \in \mathfrak{S}_n$. Let $\phi = \tau_k\tau_{k-1}\cdots\tau_1, k \geq 2$ be a representation of ϕ as a product of transpositions. Let $s \in \tau_1$ for some $s \in \{1, 2, \ldots, n\}$. If ϕ cannot be expressed as a product of $k-2$ transpositions, then for each i such that $1 \leq i \leq k$, there is a representation of ϕ as a product of transpositions*

$$\alpha_k\alpha_{k-1}\cdots\alpha_i\cdots\alpha_1$$

such that α_i is the first transposition that moves s.

Proof The proof is done by induction on i. Assume that ϕ cannot be written as a product of $k-2$ transpositions.

- If $i = 1$, let $\alpha_t = \tau_t$ for all $1 \leq t \leq k$, then $\alpha_k\alpha_{k-1}\cdots\alpha_1$ is a representation of ϕ as a product of transpositions such that α_1 is the first transposition that moves s; i.e., the statement is true at $i = 1$.
- Assume that the statement is true for i. That is, there exists $\sigma_k\sigma_{k-1}\cdots\sigma_1$, a representation of ϕ as a product of transpositions such that σ_i is the first transposition that moves s.
- To prove the statement for $i+1$, we need to find a representation of ϕ as a product of transpositions $\alpha_k\alpha_{k-1}\cdots\alpha_1$, such that the first transposition that moves s is α_{i+1}.

  By the induction hypothesis $\phi = \sigma_k\sigma_{k-1}\cdots\sigma_1$ such that σ_i is the first transposition that moves s. If $\sigma_{i+1} = \sigma_i$, then $\sigma_{i+1}\sigma_i = e$, and ϕ can be written as a product of $k-2$ transpositions, which contradicts the assumption. Thus, $\sigma_{i+1} \neq \sigma_i$. By Lemma 6.5.7, there exists a transposition τ and $l \in \{1, 2, \ldots, n\}$, such that $s \notin \tau$ and $\sigma_{i+1}\sigma_i = (sl)\tau$. By defining the following set of transpositions

$$\alpha_j = \begin{cases} (sl) & j = i+1 \\ \tau & j = i \\ \sigma_j & j \notin \{i, i+1\} \end{cases}$$

  the product

$$\begin{aligned} \alpha_k\alpha_{k-1}\cdots\alpha_{i+2}\alpha_{i+1}\alpha_i\alpha_{i-1}\cdots\alpha_1 &= \sigma_k\sigma_{k-1}\cdots\sigma_{i+2}(sl)\tau\sigma_{i-1}\cdots\sigma_1 \\ &= \sigma_k\sigma_{k-1}\cdots\sigma_{i+2}\sigma_{i+1}\sigma_i\sigma_{i-1}\cdots\sigma_1 = \phi \end{aligned}$$

  is an expression for ϕ as a product of transpositions such that α_{i+1} is the first transposition that moves s. Thus, by induction, the statement is true for all i where $1 \leq i \leq k$. ■

Lemma 6.5.9 *Let $n \in \mathbb{N}$, $n > 1$, and $e \in \mathfrak{S}_n$. If e is written as a product of k transpositions, then it can be written as a product of $k-2$ transpositions.*

Proof Assume that $e = \tau_k\tau_{k-1}\cdots\tau_1$ for some $k \geq 2$ and $s \in \tau_1$ where $s \in \{1, 2, \ldots, n\}$. If e cannot be written as a product of $k-2$ transpositions, then by Lemma 6.5.8, there exists an expression for e as a product of transpositions $\alpha_k\alpha_{k-1}\cdots\alpha_1$, where α_k is the first transposition that moves s. Hence, $\alpha_k(s) \neq s$. However, $s = e(s) = \alpha_k\alpha_{k-1}\cdots\alpha_1(s) = \alpha_k(s)$, which is a contradiction. ■

The identity permutation is an even permutation as $e = (ij)(ij)$ for any $i \neq j$. The following result shows that e cannot be odd.

Corollary 6.5.10 *Let $n \in \mathbb{N}$. The identity permutation $e \in \mathfrak{S}_n$ is not an odd permutation.*

Proof Assume that e can be written as a product of k transpositions where k is odd, i.e., $k = 2q + 1$ for some integer q. Repeatedly applying Lemma 6.5.9, e can be written as a product of $k - 2$ transpositions then as $k - 4$ transpositions, and finally after q repetitions, e can be written as a product of $k - 2q$ transpositions. Since $k - 2q = 1$, then e is a transposition, which contradicts that e is the identity map. ■

Corollary 6.5.11 *Let $n \in \mathbb{N}$, $n > 1$, and $\phi \in \mathfrak{S}_n$. The permutation ϕ is either even or odd and cannot be both.*

Proof Let $\phi = \tau_k\cdots\tau_1$ and $\phi = \alpha_s\cdots\alpha_1$ be two expressions for ϕ as product of transpositions. Using the second expression, we obtain $\phi^{-1} = \alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_s^{-1}$ which implies that

$$e = \phi^{-1}\phi = \alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_s^{-1}\cdot\tau_k\cdots\tau_1 = \alpha_1\cdots\alpha_s\cdot\tau_k\cdots\tau_1$$

Thus, e is a product of $k + s$ transpositions. As e cannot be an odd permutation, then $k + s$ must be an even integer. Therefore, k and s must be either both even, or both odd. ■

Using the last corollary and Remark 6.5.2 (1), one obtains the following result.

Corollary 6.5.12 *Let $n, k \in \mathbb{N}$, $n > 1$, $k \leq n$, and ϕ is a cycle of length k. The cycle ϕ is an odd permutation if and only if k is even, and vice versa.*

For each $n \in \mathbb{N}$, the set of even permutations in $\mathfrak{S}_n$ is denoted by $\mathcal{A}_n$, while $\mathcal{B}_n$ denotes the set of all odd permutation of $\mathfrak{S}_n$. Since e is an even permutation, $\mathcal{A}_n$ is never empty. The last corollary shows that the two sets do not intersect.

$$\mathcal{A}_n = \{\phi \in \mathfrak{S}_n : \phi \text{ is even}\}, \mathcal{B}_n = \{\phi \in \mathfrak{S}_n : \phi \text{ is odd}\}.$$

If $n = 1$, then $\mathfrak{S}_1 = \mathcal{A}_1 = \{e\}$ and $\mathcal{B}_1 = \emptyset$.
If $n = 2$, then $\mathfrak{S}_2 = \{e, (1\ 2)\}$, $\mathcal{A}_2 = \{e\}$, and $\mathcal{B}_2 = \{(1\ 2)\}$.

Example 6.5.13 To list all the elements in $\mathcal{A}_3$ and $\mathcal{B}_3$, list all the elements of $\mathfrak{S}_3$

$$\mathfrak{S}_3 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 3), (1\ 2), (2\ 3)\}.$$

As all the permutations $\mathfrak{S}_3$ are cycles, by using Corollary 6.5.12, we obtain

$$\mathcal{A}_3 = \{(1\ 2)(1\ 2), (1\ 3)(1\ 2), (1\ 2)(1\ 3)\}, \mathcal{B}_3 = \{(1\ 3), (1\ 2), (2\ 3)\}.$$

Another way to determine if a permutation is odd or even is by defining a function on $\mathfrak{S}_n$, called the sign function.

Definition 6.5.14 Let $n \in \mathbb{N}$, and ϕ in $\mathfrak{S}_n$. The sign of ϕ, denoted by $\operatorname{sgn}(\phi)$, is defined as $(-1)^k$, where k is the number of transpositions in any expression for ϕ as a product of transpositions.

Corollary 6.5.15 *Let* $n \in \mathbb{N}$. *The map* $\operatorname{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ *satisfies*

$$\operatorname{sgn}(\phi) = \begin{cases} 1 & \text{if } \phi \text{ is even} \\ -1 & \text{if } \phi \text{ is odd} \end{cases}$$

for any $\phi \in \mathfrak{S}_n$.

The following proposition provides a computationally convenient way to determine the sign of a permutation without the need of writing it as a product of transpositions.

Proposition 6.5.16 *Let* $n \in \mathbb{N}$, *and* ϕ *in* $\mathfrak{S}_n$. *The sign of* ϕ *is computed using the following equation*

$$\operatorname{sgn}(\phi) = \prod_{1 \le i < j \le n} \frac{\phi(j) - \phi(i)}{j - i}.$$

Example 6.5.17: Let $\phi = (1\ 2) \in \mathfrak{S}_3$. As the permutation ϕ is odd, then $\operatorname{sgn}(\phi)$ is -1. Using the formula in Proposition 6.5.16,

$$\begin{aligned}\operatorname{sgn}(\phi) &= \frac{\phi(3) - \phi(2)}{3 - 2} \frac{\phi(3) - \phi(1)}{3 - 1} \frac{\phi(2) - \phi(1)}{2 - 1} \\ &= \frac{3 - 1}{1} \cdot \frac{3 - 2}{2} \cdot \frac{1 - 2}{1} = (2)\left(\frac{1}{2}\right)(-1) = -1,\end{aligned}$$

as expected.

Our next goal is to show that $\mathcal{A}_n$ is always a group, and $\mathcal{B}_n$ is not a group for any n. We begin with the following proposition.

Proposition 6.5.18 Let $n \in \mathbb{N}$, and $\phi, \psi \in \mathfrak{S}_n$.

1. If ϕ, ψ have the same parity, then $\phi \circ \psi$ is even.
2. If ϕ, ψ have opposite parity, then $\phi \circ \psi$ is odd.
3. The product of two even (odd) permutations is an even permutation.

4. The product of a finite number of even permutations is an even permutation.
5. ϕ^{-1} is even (odd) if and only if ϕ is even (odd).
6. The cycle $(i_1 \dots i_k)$ is even (odd) if and only if k is odd (even).

Proof Let $\phi = \tau_k \cdots \tau_1$ and $\psi = \beta_s \cdots \beta_1$ be expressions of ϕ, ψ as products of transpositions. The composition $\phi \circ \psi = \tau_k \cdots \tau_1 \cdot \beta_s \cdots \beta_1$ is a product of $k + s$ transpositions.

1. If k and s have the same parity (either both even or both odd), then $k + s$ is even, and $\phi \circ \psi$ is even.
2. If k and s have the opposite parity (one is even and the other is odd), then $k + s$ is odd, so $\phi \circ \psi$ is odd.
3. The statement (3) follows form (1).
4. The statement of (4) follows from (3) by induction on the number of permutations.
5. The result of (5) follows as $\phi^{-1} = \tau_1^{-1} \cdots \tau_k^{-1} = \tau_1 \cdots \tau_k$ can be expressed using the same number of transpositions forming ϕ.
6. The result in (6) follows by Remark 6.5.2 which states that any cycle of length k where $k > 1$, can be written as a product of $k - 1$ transpositions. ■

Note that since the product of two odd permutations is even, $\mathcal{B}_n$ is never closed and thus is never a group under the composition of maps.

Corollary 6.5.19 *Let* $n \in \mathbb{N}$, $n > 1$. *The set* $\mathcal{A}_n$ *of all even permutations on* $\{1, 2, \dots, n\}$ *forms a group under composition.*

Proof As $e \in \mathcal{A}_n$, the set $\mathcal{A}_n$ is a nonempty subset of $\mathfrak{S}_n$. As the composition of two even permutations is even, $\mathcal{A}_n$ is closed under composition, which implies that $\circ$ forms a binary operation on $\mathcal{A}_n$ (Proposition 4.1.6). The associativity property is inherited from $\mathfrak{S}_n$, and e serves as an identity element in $\mathcal{A}_n$. As the inverse of an even permutation is even (Proposition 6.5.18 (5)), $\mathcal{A}_n$ is closed undertaking the inverse, and thus, it is a group. ■

Definition 6.5.20 Let $n \in \mathbb{N}$, $n > 1$. The group $\mathcal{A}_n$ is called the alternating group of degree n.

Figure 6.4 summarized the main results about permutation that are shown in this chapter.

Summary 6.5.20

Let $n \in \mathbb{N}$.

1. The permutations, cycles, and transpositions are all elements in the group $\mathfrak{S}_n$.
2. Any transposition is a cycle, any cycle is a permutation, but the converse is not true.
3. Disjoint permutations commute.
4. Any permutation can be expressed as a finite product of pairwise disjoint cycles.
5. Any permutation can be expressed as a finite product of transpositions.

Fig. 6.4 Summary

Exercises

Solved Exercises

6.1 Consider the following permutations.

$$\alpha = (2\ 5\ 6)(3\ 4) \in \mathfrak{S}_7$$

$$\beta = (2\ 5\ 3)(8\ 9\ 1\ 1)(7\ 1\ 4) \in \mathfrak{S}_{11}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 1 & 6 & 4 & 7 \end{pmatrix} \in \mathfrak{S}_7$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 2 & 3 & 10 & 6 & 4 & 7 & 9 & 8 & 1 \end{pmatrix} \in \mathfrak{S}_{10}.$$

(a) Write the matrix representation of the permutations α and β.
(b) Write the permutations γ and δ as a product of disjoint cycles.
(c) Find the order of all the above permutations.
(d) For each of the permutations determine whether it is odd or even.
(e) Find Move(α), Move(γ).
(f) Find γ^{39} and δ^{121}.
(g) Are the permutations α and γ disjoint? Explain.

Solution:

(a) Using the result in Corollary 6.2.7, we have

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

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 5 & 2 & 7 & 3 & 6 & 1 & 9 & 11 & 10 & 8 \end{pmatrix}.$$

(b) Applying the method in the proof of Proposition 6.2.9 yields

$$\gamma = (1\ 5\ 6\ 4) \text{ and } \delta = (1\ 5\ 6\ 4\ 10)(8\ 9).$$

(c) By Proposition 6.4.3,

$$\operatorname{ord}(\alpha) = \operatorname{lcm}(3, 2) = 6, \text{ and } \operatorname{ord}(\beta) = \operatorname{lcm}(3, 3, 3) = 3.$$

As $\gamma = (1\ 5\ 6\ 4)$ is a cycle of length 4, then $\operatorname{ord}(\gamma) = 4$. Finally, $\operatorname{ord}(\delta) = \operatorname{lcm}(5, 2) = 10$.

(d) Using the results in Proposition 6.5.18, one can obtain

- $\alpha = (2\ 5\ 6)(3\ 4)$ is a product of an even cycle and an odd cycle, and thus an odd permutation.
- $\beta = (2\ 5\ 3)(8\ 9\ 11)(7\ 1\ 4)$ is a product of three even cycles, and thus, it is an even permutation.
- $\gamma = (1\ 5\ 6\ 4)$ is a 4-cycle, and thus, it is an odd permutation.
- $\delta = (1\ 5\ 6\ 4\ 10)(8\ 9)$ is a product of even and odd permutations, and thus, it is an odd permutation.

(e) Using Definition 6.1.6, we obtain

$$\text{Move}(\alpha) = \{2, 3, 4, 5, 6\} \text{ and } \text{Move}(\gamma) = \{1, 4, 5, 6\}.$$

(f) Several methods can be used to compute γ^{39}, we present two methods both of which use the fact that $\text{ord}(\gamma) = 4$. The first method applies the quotient-remainder theorem on 39 and 4 to obtain

$$\gamma^{39} = \gamma^{9\times4+3} = \left(\gamma^4\right)^9\gamma^3 = \gamma^3 = (4\ 6\ 5\ 1).$$

An alternative method that uses fewer computations starts by noting that $\gamma\ \gamma^{39} = \gamma^{40} = (\gamma^4)^{10} = e$, thus $\gamma^{39} = \gamma^{-1} = (1\ 5\ 6\ 4)^{-1} = (4\ 6\ 5\ 1)$.

The two methods are applied to compute δ^{121} using the fact that $\text{ord}(\delta) = 10$, as follows:

$$\delta^{121} = \delta^{12\times10+1} = (\delta^{10})^{12}\delta = e\delta = \delta.$$

and

$$\delta^{-1}\delta^{121} = \delta^{120} = (\delta^{10})^{12} = e, \text{ which implies that } \delta^{120} = \delta.$$

(g) No. The permutations α and γ are not disjoint since $\text{Move}(\alpha) \cap \text{Move}(\gamma) \neq \emptyset$.

6.2. Let $\alpha = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 4\ 3 \end{pmatrix}$, and $\beta = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 1\ 3\ 4 \end{pmatrix}$. Do α and β commute? Find $(\alpha\beta)^4$.

Solution:

Expressing α and β as a product of cycles yields

$$\alpha = (3\ 4) \text{ and } \beta = (1\ 2).$$

Since α and β are disjoint, by Proposition 6.1.10, $\alpha\beta = \beta\alpha$. Using the result of Corollary 6.1.11, we obtain

$$(\alpha\beta)^4 = \alpha^4\beta^4 = \left((34)^2\right)^2\left((12)^2\right)^2 = e.$$

6.3. Let $\alpha = (2\ 5\ 6)(3\ 2\ 4\ 1) \in \mathfrak{S}_7$. Find $\alpha^{-1}(2)$ and $\alpha(5)$.

Solution:

Since α takes 5 to 6 then $\alpha(5) = 6$. To compute $\alpha^{-1}(2)$, we must compute α^{-1} using one of the following methods:

- $\alpha = (256)(3241) = (135624)$, which implies that $\alpha^{-1} = (426531)$.
- $\alpha^{-1} = (3241)^{-1}(256)^{-1} = (1423)(652)$.

In both cases, $\alpha^{-1}(2) = 6$.

6.4. Let A be any nonempty set. Consider the symmetric group of A (Corollary 5.1.11). For each element f in $\mathfrak{S}_A$, define the relation $\cong_f$ on A as follows:

$$i \cong_f j \Leftrightarrow \exists\, m \in \mathbb{Z} \ni j = f^m(i).$$

The relation $\cong_f$ is an equivalence relation on the set A (Check!). The equivalence classes of such relation are called the orbits of f and given for each $i \in A$ as

$$\mathcal{O}r_f(i) = \left\{f^k(i) : k \in \mathbb{Z}\right\}.$$

Consider the additive group $(\mathbb{Z}, +)$. Let $f : \mathbb{Z} \to \mathbb{Z}$ be the map defined by $f(n) = n + 2$. As f is a bijective map on $\mathbb{Z}$, then f belongs to $\mathfrak{S}_{\mathbb{Z}}$, the symmetric group on $\mathbb{Z}$. Find all the distinct orbits of f.

Solution:

Let $i \in \mathbb{Z}$ be an arbitrary element.

$$\mathcal{O}r_f(i) = \left\{f^k(i) : k \in \mathbb{Z}\right\}.$$

One can show by induction on k that $f^k(i) = i + 2k$. Therefore, for any $i \in \mathbb{Z}$

$$\mathcal{O}r_f(i) = \{i + 2k : k \in \mathbb{Z}\} = i + 2\mathbb{Z}.$$

By applying the quotient-remainder theorem (Theorem 2.1.2) on i and 2, one obtain that there exist $q, r \in \mathbb{Z}$ such that $i = 2q + r$, where $0 \le r < 2$, i.e.,

$$\mathcal{O}r_f(i) = i + 2\mathbb{Z} = r + 2q + 2\mathbb{Z} = r + 2\mathbb{Z}, \text{ where } r = 0, 1.$$

Hence, only two orbits of f exist, namely $2\mathbb{Z}$ (at $r = 0$) and $1 + 2\mathbb{Z}$ at $(r = 1)$.

6.5. Consider the symmetric group $\mathfrak{S}_9$. Find two elements α, β in $\mathfrak{S}_9$ such that

$$\operatorname{ord}(\alpha) = \operatorname{ord}(\beta) = 5 \text{ and } \operatorname{ord}(\alpha\beta) = 9.$$

Solution:

Let $\alpha = (1\ 2\ 3\ 4\ 5), \beta = (1\ 6\ 7\ 8\ 9) \in \mathfrak{S}_9$. As the order of any cycle is equal to its length, then $\operatorname{ord}(\alpha) = 5 = \operatorname{ord}(\beta)$. The product

$$\alpha\beta = (1\ 2\ 3\ 4\ 5)(1\ 6\ 7\ 8\ 9) = (1\ 6\ 7\ 8\ 9\ 2\ 3\ 4\ 5).$$

Therefore, $\operatorname{ord}(\alpha\beta) = 9$.

6.6. Prove that $\alpha = (4\ 5\ 7\ 2\ 1\ 8) \in \mathfrak{S}_8$ is not a product of 3-cycles.

Solution:

Assume that α is a product of only 3-cycles. As any 3-cycle is an even permutation, thus by Proposition 6.5.18 (4), α is an even permutation, which contradicts the fact that

$$\alpha = (4\ 8)(4\ 1)(4\ 2)(4\ 7)(4\ 5)$$

is a product of five transpositions. Therefore, α cannot be a product of only 3-cycles.

6.7. Let $n \in \mathbb{N}$ such that $n > 1$. Prove that in $\mathfrak{S}_n$, the number of even permutations equals the number of odd permutations. Namely,

$$|\mathcal{A}_n| = |\mathcal{B}_n| = \frac{n!}{2}.$$

Solution:

Since $n > 1$, then $(1\ 2) \in \mathfrak{S}_n$. Define

$$\begin{aligned} f : \mathcal{A}_n &\to \mathcal{B}_n \\ \phi &\mapsto (12)\phi. \end{aligned}$$

The permutation $(1\ 2)$ is an odd permutation. Therefore, by Proposition 6.5.18 (2), the permutation $(1\ 2)\phi$ is odd for each $\phi \in \mathcal{A}_n$. Hence, f defines a function from $\mathcal{A}_n$ to $\mathcal{B}_n$. The map f is injective since

$$\begin{aligned} f(\phi_1) = f(\phi_2) &\Rightarrow (1\ 2)\phi_1 = (1\ 2)\phi_2 \\ &\Rightarrow (1\ 2)(1\ 2)\phi_1 = (1\ 2)(1\ 2)\phi_2 \\ &\Rightarrow \phi_1 = \phi_2. \end{aligned}$$

Since for any $\psi \in \mathcal{B}_n$, the permutation $(1\ 2)\psi \in \mathcal{A}_n$ and satisfies $f((1\ 2)\psi) = \psi$, then f is also surjective. Thus, f is a bijective map, and $|\mathcal{A}_n| = |\mathcal{B}_n|$. Since $\{\mathcal{A}_n, \mathcal{B}_n\}$ form a partition of the set $\mathfrak{S}_n$, then $n! = |\mathfrak{S}_n| = |\mathcal{A}_n| + |\mathcal{B}_n| = 2|\mathcal{A}_n|$, which implies the result.

6.8. Let $n \in \mathbb{N}$. Show that $\mathcal{A}_n = \mathfrak{S}_n$ if and only if $n = 1$.

Solution:

If $n = 1$, then $\mathfrak{S}_1 = \{e\}$. Since $\mathcal{A}_1$ is a group, it cannot be empty, and $\mathcal{A}_1$ is a nonempty subset of $\{e\}$. Thus, $\mathfrak{S}_1 = \mathcal{A}_1$. For the other direction, assume that $n > 1$, then $\alpha = (1\ 2)$ belongs to $\mathfrak{S}_n$. As the permutation α is odd permutation then α does not belong to $\mathcal{A}_n$. Therefore, $\mathfrak{S}_n \neq \mathcal{A}_n$.

6.9. Let $n \in \mathbb{N}$ and α be a cycle in $\mathfrak{S}_n$. Show that

$$\text{ord}(\alpha) \text{ is odd if and only if } \alpha \text{ is an even permutation.}$$

Solution:

Assume that $\alpha = (i_1 i_2 \dots i_k)$ is a cycle in $\mathfrak{S}_n$. According to Lemma 6.4.2, we obtain $\text{ord}(\alpha) = k$. Proposition 6.5.18 (6) now implies the result.

6.10. Let $n \in \mathbb{N}$, where $n \geq 3$. Show that no nontrivial cycle belongs to the center of $\mathfrak{S}_n$. i.e., $C(\mathfrak{S}_n) = \{e\}$ for all $n \geq 3$.

Solution:

Let $\alpha = (i_1 i_2 \dots i_k)$ be any cycle in $\mathfrak{S}_n$ such that $k \geq 2$.

- If $k = 2$, then $\alpha = (i_1 i_2)$. By choosing $i_3 \in \{1, 2, \dots, n\} \backslash \{i_1, i_2\}$ $(n \geq k)$, and direct computations yield,

$$\alpha(i_1 i_3) = (i_1 i_3 i_2) \neq (i_1 i_2 i_3) = (i_1 i_3)\alpha,$$

and α is not in the center.

- If $k > 2$, then $(i_1 i_2 \dots i_k)(i_1 i_k)(i_k) = i_2 \neq i_k = (i_1 i_k)(i_1 i_2 \dots i_k)(i_k)$. i.e.,

$$\alpha(i_1 i_k)(i_k) \neq (i_1 i_k)\alpha(i_k)$$

and α is not in the center.

Unsolved Exercises

6.11. Let $\phi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,1\,5\,2 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,4\,5 \end{pmatrix}$ be permutations in $\mathfrak{S}_6$.

Express both ϕ and ψ as a product of disjoint cycles. Find $\phi \circ \psi$ and $\psi \circ \phi$.

6.12. In $\mathfrak{S}_4$, find α^{6431}, where $\alpha = (1\ 2\ 3\ 4)$.

6.13. Consider the group $\mathfrak{S}_6$ and the permutations

$$\phi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,5\,2\,1\,6\,4 \end{pmatrix}, \psi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,5\,3\,1\,6 \end{pmatrix}, \varphi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,5\,6\,5\,4 \end{pmatrix}$$

Find the order of these permutations. Find the permutation $\psi \circ \phi \circ \varphi$ and its inverse.

6.14. Find the order of the given permutations:

$$\alpha = (2\ 4\ 1\ 7)(3\ 5\ 6) \text{ as an element in } \mathfrak{S}_7$$
$$\beta = (1\ 4\ 2)(8\ 6)(3\ 5\ 6\ 7) \text{ as an element in } \mathfrak{S}_8$$

6.15. Consider the group $\mathfrak{S}_7$. Write the following permutations as a product of transpositions.

- $(1\ 2\ 3)(4\ 3\ 6\ 5)$.
- $(1\ 2\ 3\ 4\ 5)$.
- $(5\ 7)(3\ 2\ 4)(1\ 6)$.
- $(1\ 2\ 3)(4\ 5\ 6)$.
- $(3\ 4\ 2\ 6)(3\ 4\ 2\ 6)$.

6.16. Consider the group $\mathfrak{S}_8$. Let $\phi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 5\,4\,6\,2\,3\,8\,1\,7 \end{pmatrix}$, and $\psi = (1\ 5\ 3\ 4)$

i. Find the permutations

$$\phi^3\psi^{-2}\phi,\ \ \psi^2\phi\psi,\ \ \phi^2\psi^2,\ \ \phi\psi\phi,\ \ \psi\phi,\ \ \phi\psi,\ \ \psi^{-1}, \phi^{-1}.$$

ii. Find the parity of ϕ, ψ, and all permutations in (i).
iii. Find $\operatorname{ord}(\phi)$, $\operatorname{ord}(\psi)$, $\operatorname{ord}(\phi^2)$, and $\operatorname{ord}(\psi^4)$.
iv. Find the orbits of ϕ and ψ and the orbits of all permutations in (i).
v. Compute ϕ^7, ψ^6, ϕ^{22}.

6.17. Consider the permutations $\phi = (1\ 3\ 5)(1\ 2)$ and $\psi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 5\,2\,1\,7\,3\,6\,4 \end{pmatrix}$ as elements in $\mathfrak{S}_7$. Determine if these permutations are even or odd.

6.18. Let $\alpha = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,4\,3\,1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix}$ be elements in $\mathfrak{S}_4$.

a. Express α, β as products of transpositions.
b. Determine if α, β are even or odd permutations.
c. Find $\alpha \circ \beta$ and $\beta \circ \alpha$ and determine their parity.
d. Find the orders of $\alpha \circ \beta$, $\beta \circ \alpha$, β, α.
e. Does $\alpha(2) \in \operatorname{Move}(\alpha)$? Find $\operatorname{Move}(\alpha) \cap \operatorname{Move}(\beta)$.
f. Find all the distinct orbits of α and β.

6.19. Repeat all the questions in Exercise 6.18 given that $\beta = (2\ 4\ 3\ 5)$ and $\alpha = (1\ 2\ 3\ 6)$ as elements in $\mathfrak{S}_6$.

6.20. Consider the permutations $\phi = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,2\,4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$ as elements in $\mathfrak{S}_4$. Find $(\psi\phi)^5$ and its order as an element of $\mathfrak{S}_4$.

6.21. Give an example of $n \in \mathbb{N}$, and elements α and β in $\mathfrak{S}_n$ such that $\operatorname{ord}(\alpha) = \operatorname{ord}(\beta)$and $\operatorname{ord}(\alpha\beta) = 4$.

6.22. Give an example of $n \in \mathbb{N}$, and elements α and β in $\mathfrak{S}_n$ such that $\operatorname{ord}(\alpha) = 3$, $\operatorname{ord}(\beta) = 4$. and $\operatorname{ord}(\alpha\beta) \neq \operatorname{lcm}(3, 4)$

6.23. List all possible orders of an element of $\mathcal{A}_6$.

Table 6.2 Table of the group $(A, *)$

$*$	x	y	z	g	h	k
x	x	y	z	g	h	k
y	y	x	k	h	g	z
z	z	h	x	k	y	g
g	g	k	h	x	z	y
h	h	z	g	y	k	x
k	k	g	y	z	x	h

6.24. Show that $C(\mathfrak{S}_n) = \{e\}$, for each $n \geq 3$.

6.25. How many cycles of order 3 are in $\mathfrak{S}_5$? How many cycles of order 3 are in $\mathfrak{S}_6$?

6.26. How many permutations in $\mathfrak{S}_5$ are of the form of a product of two transpositions?

6.27. Let $n \in \mathbb{N}$, and consider the group $\mathfrak{S}_n$. Let ϕ and ψ be two disjoint permutations in $\mathfrak{S}_n$. Show that if $\phi\psi = e$, then $\phi = \psi = e$.

6.28. Let $G = (\mathfrak{S}_3, \circ)$, $A = \{x, y, z, g, h, k\}$, and $f : A \to G$ be the bijective map given by $f(x) = e$, $f(y) = (1\ 2)$, $f(z) = (1\ 3)$, $f(g) = (2\ 3)$, $f(h) = (1\ 2\ 3)$, $f(k) = (1\ 3\ 2)$. Let $(A, *)$ be the group defined in Exercise 5.21. Show that the group structure on A is given by Table 6.2.

References

Carter, N. C. (2009). *Visual group theory.* Mathematical Association of America.

De Temple, D., & Webb, W. (2014). *Combinatorial reasoning, an introduction to the art of counting.* John Wiley & Sons, Inc.