Chapter 5
Permutation Groups

In this chapter, we construct some groups whose elements are called permutations. Often, an action produced by a group element can be regarded as a function, and the binary operation of the group can be regarded as function composition. The symmetric group on a set is the group consisting of all bijections from the set to itself with function composition as the group operation. These groups will provide us with examples of finite non-abelian groups.

5.1 Inverse Functions and Permutations

In this section, we study certain groups of functions called permutation groups.

Theorem 5.1 *If $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then their compositions are associative, i.e., $(h \circ g) \circ f = h \circ (g \circ f)$.*

Proof It is straightforward. ■

Definition 5.2 For any non-empty set X, the *identity function* is the function $id_X : X \to X$ defined by $id_X(x) = x$, for all $x \in X$.

Clearly, if $f : X \to Y$ is any function, then $f \circ id_X = f$ and $id_X \circ f = f$.

Definition 5.3 Let $f : X \to Y$ be a function. We say that f has an *inverse function* if there exists a function $g : Y \to X$ such that $f \circ g = id_Y$ and $g \circ f = id_X$.

Theorem 5.4 *If a function $f : X \to Y$ has an inverse, then this inverse is unique.*

Proof Suppose that g and h are both inverses for f. Then, we have $g \circ f = h \circ f = id_X$ and $f \circ g = f \circ h = id_Y$. Thus, we obtain

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_5

$$h = h \circ id_Y = h \circ (f \circ g) = (h \circ f) \circ g = id_X \circ g = g.$$

This yields that the inverse of f is unique. ■

The inverse of f is denoted by f^{-1}.

Theorem 5.5 *A function $f : X \to Y$ has an inverse if and only if f is a bijection.*

Proof Assume that f is a bijection. We define a function $g : Y \to X$ as follows:

$$g(y) = x \iff f(x) = y.$$

Since f is one to one, it follows that g is a function. Now, by the definition, $f \circ g = id_Y$ and $g \circ f = id_X$.

Conversely, suppose that f has an inverse f^{-1}. First, we show that f is one to one. If $f(x_1) = f(x_2)$, then

$$x_1 = id_X(x_1) = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = id_X(x_2) = x_2,$$

hence f is one to one. In order to show that f is onto, take any $y \in Y$. Then,

$$y = id_Y(y) = f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x),$$

where $x = f^{-1}(y)$. So, f is onto. ■

Theorem 5.6 *If $f : X \to Y$ and $g : Y \to Z$ are bijections, then so is the function $g \circ f$.*

Proof Suppose that f and g have inverse functions f^{-1} and g^{-1}, respectively. Then, we obtain $(g \circ f)(f^{-1} \circ g^{-1}) = id_Z$ and $(f^{-1} \circ g^{-1})(g \circ f) = id_X$. Hence, the inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$. Consequently, by Theorem 5.5, $g \circ f$ is a bijection. ■

Definition 5.7 Let X be a non-empty set. A bijective function from X to itself is called a *permutation* of X.

For an arbitrary non-empty set X we define S_X to be the set of all permutations.

Theorem 5.8 *The set S_X of all permutations of X is a group under composition of functions.*

Proof We check the group axioms for S_X. By Theorem 5.6, if $f, g \in S_X$, then $f \circ g \in S_X$. The associativity axioms holds by Theorem 5.1. The identity element is id_X. Finally, the definition of an inverse function shows that if f^{-1} is the inverse of f, then f is the inverse of f^{-1}. Consequently, f^{-1} is a bijection. ■

Since the composition of functions is not commutative, it follows that S_X is not abelian, for $|X| \geq 3$.

Let us make a small example to understand better the connection between the intuition and the formal definition.

Example 5.9 Let $X = \{\bigcirc, \blacksquare, \triangle\}$. Then, the permutations that belong to S_X are:

$$id_X : \begin{cases} \bigcirc \to \bigcirc \\ \blacksquare \to \blacksquare \\ \triangle \to \triangle \end{cases} \qquad f_1 : \begin{cases} \bigcirc \to \blacksquare \\ \blacksquare \to \bigcirc \\ \triangle \to \triangle \end{cases}$$

$$f_2 : \begin{cases} \bigcirc \to \blacksquare \\ \blacksquare \to \triangle \\ \triangle \to \bigcirc \end{cases} \qquad f_3 : \begin{cases} \bigcirc \to \triangle \\ \blacksquare \to \blacksquare \\ \triangle \to \bigcirc \end{cases}$$

$$f_4 : \begin{cases} \bigcirc \to \bigcirc \\ \blacksquare \to \triangle \\ \triangle \to \blacksquare \end{cases} \qquad f_5 : \begin{cases} \bigcirc \to \triangle \\ \blacksquare \to \bigcirc \\ \triangle \to \blacksquare \end{cases}$$

Exercises

1. Define $f : \mathbb{N} \to \mathbb{N}$ by $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 7$, $f(7) = 1$, and $f(n) = n$ for any other $n \in \mathbb{N}$. Show that $f \circ f \circ f \circ f \circ f = id_{\mathbb{N}}$. What is f^{-1} in this case?
2. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function. For each of the following cases, find a left and a right inverses if exist.

   (a) $f(x) = \begin{cases} x & \text{if } x \text{ is even} \\ 2x + 1 & \text{if } x \text{ is odd} \end{cases}$

   (b) $f(x) = \begin{cases} x/3 & \text{if } x \equiv 0 (\text{mod } 3) \\ x + 1 & \text{otherwise.} \end{cases}$
3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = ax + b$, where $aandb$ are integers. Find the necessary and sufficient conditions on a and b such that $f \circ f = id_{\mathbb{Z}}$.
4. Let $f : X \to X$ be a function such that $f(f(x)) = x$, for all $x \in X$. Prove that f is a symmetric relation on X.
5. A function $f : X \to Y$ is said to be *left cancellable* if for any set Z and for any mappings g and h from Z to X such that $f \circ g = f \circ h$, then $g = h$. Prove that a function $f : X \to Y$ is left cancellable if and only if f is one to one.
6. A function $f : X \to Y$ is said to be *right cancellable* if for any set Z and for any mappings g and h from Y to Z such that $g \circ f = h \circ f$, then $g = h$. Prove that a function $f : X \to Y$ is right cancellable if and only if f is onto.
7. Given two sets X and Y we declare $X \prec Y$ (X is smaller than Y) if there is a mapping of Y onto X but no mapping of X onto Y. Prove that if $X \prec Y$ and $Y \prec Z$, then $X \prec Z$.
8. If X is a finite set and f is a one to one function of X, show that for some positive integer n,

$$\underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}} = id_X.$$

9. If X has m elements in Exercise 8, find a positive integer n (in terms of m) that works simultaneously for all one to one mappings of X into itself.
10. If $a \in X$ and $H = \{f \in S_X \mid f(a) = a\}$, show that H is a subgroup of S_X.
11. Let X be an infinite set and let H be the set of all permutations $f \in S_X$ such that $f(a) \neq a$ for at most a finite number of $a \in X$.

    (a) Prove that H is a subgroup of S_X;
    (b) Show that if $f \in S_X$, then $f^{-1}Hf = H$.

12. If X has three or more elements, show that we can find $f, g \in S_X$ such that $f \circ g \neq g \circ f$.
13. Observe that for any positive integer x, we have $x = 2^m(2n+1)$, for some non-negative integers m and n. This means that we can define $f : \mathbb{N} \to (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$ such that $f(x) = (m, n)$, as indicated above. Prove that f is one to one and onto.
14. **(Schröder–Bernstein Theorem).** Let X and Y be two sets such that

    (a) For a subset A of X, there is a one to one correspondence between A and Y;
    (b) For a subset B of Y, there is a one to one correspondence between B and X.

    Prove that there exists a one to one correspondence between A and Y.
15. Let G be a group and let a be a fixed element of G. Show that the map $f_a : G \to G$, given by $f_a(x) = ax$, for $x \in G$, is a permutation of the set G.

5.2 Symmetric Groups

In this section we briefly introduce some basic concepts and constructions that we will need later. Permutations are usually studied as combinatorial objects, we will observe that they have a natural group structure.

Definition 5.10 The group S_X is called the *symmetric group* or *permutation group* on the set X.

The group of permutations of the set $X = \{1, \ldots, n\}$ is denoted by S_n.

Theorem 5.11 *The order of S_n is equal to $n!$.*

Proof We count how many permutations of $\{1, 2, \ldots, n\}$ exist. We have to fill the boxes

			$\ldots$	
1	2	3		n

with numbers $1, 2, \ldots, n$ with no repetitions. For box 1, we have n possible choices. When one number has been chosen, for box 2, we have $n - 1$ choices, and so on.

Consequently, we have

$$n(n-1)(n-2)\dots 2\cdot 1 = n!$$

permutations and so the order of S_n is $|S_n| = n!$. ■

We can describe a permutation $\sigma \in S_n$ in several ways. A convenient notation for specifying a given permutation $\sigma \in S_n$ is

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix},$$

where a_k is the image of k under σ, for each $0 \le k \le n$. In this case, we write $k\sigma = a_k$. Accordingly, regarding this notation one must be absolutely sure as to what convention is being followed in writing the product of two permutations. If $\tau, \sigma \in S_n$, then we reiterate that $\sigma\tau$ will always mean: *first apply σ and then τ.*

Example 5.12 Let

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

be two permutations in S_5. Then, we have

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix},$$
$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}, \quad \tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

There is another notation commonly used to specify permutations. It is called cycle notation.

Definition 5.13 Let $1 \le k \le n$ and let $a_1, a_2, \dots, a_k$ be k disjoint integers between 1 and n. The *cycle* $(a_1\ a_2\ \dots\ a_k)$ denotes the permutation of S_n that sends

$$\begin{aligned} &a_1 \to a_2, \\ &a_2 \to a_3, \\ &\vdots \\ &a_{k-1} \to a_k, \\ &a_k \to a_1, \end{aligned}$$

and leaves the remaining $n-k$ numbers fixed. We say that the *length of the cycle* $(a_1\ a_2\ \dots\ a_k)$ is k.

It is clear that our choice of starting point for the cycle is not important. Thus, $(a_1\ a_2\ \dots\ a_k) = (a_2\ \dots\ a_k\ a_1)$. The inverse of a cycle is a cycle. More precisely,

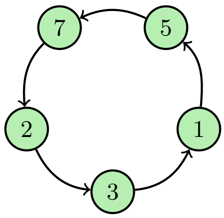

Fig. 5.1 An illustration of cycle notation

$$(a_1\ a_2\ \ldots\ a_k)^{-1} = (a_k\ a_{k-1}\ \ldots\ a_1).$$

Example 5.14 As an illustration of cycle notation, let us consider the permutation

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

This assignment of values could be presented schematically as in Fig. 5.1.

Example 5.15 The cycle $(3\ 4\ 1\ 6)$ means the permutation where $3 \to 4$, $4 \to 1$, $1 \to 6$, $6 \to 3$, and all the other elements are fixed. So, $(3\ 4\ 1\ 6) \in S_7$ corresponds to

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

Example 5.16 Suppose that $(1\ 3\ 4\ 2)$ and $(2\ 5\ 3)$ are two cycles in S_5. Then

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

Example 5.17 We may write S_3, in Example 5.9, as

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

The following is Cayley table for S_3.

$\cdot$	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	id	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	id	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	id
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	id	(1 2 3)

Definition 5.18 Two cycles $(a_1\ a_2\ \dots\ a_k)$ and $(b_1\ b_2\ \dots\ b_l)$ are distinct if $\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots, b_l\} = \emptyset$.

Lemma 5.19 *If $\sigma = (a_1\ a_2\ \dots\ a_k)$ and $\tau = (b_1\ b_2\ \dots\ b_l)$ are distinct, then $\sigma\tau = \tau\sigma$.*

Proof Let $1 \le i \le k-1$. Since $a_i \notin \{b_1, \dots, b_l\}$, it follows that $a_i\tau = a_i$. Hence, we get

$$a_i(\tau\sigma) = a_i\sigma = a_{i+1}.$$

Also, since $a_{i+1} \notin \{b_1, \dots, b_l\}$, it follows that

$$a_i(\sigma\tau) = a_{i+1}\tau = a_{i+1}.$$

Similar arguments for each $1 \le j \le l$ show that

$$b_j(\tau\sigma) = b_{j+1}\sigma = b_{j+1} = b_j\tau = b_j(\sigma\tau)$$

and

$$a_k(\sigma\tau) = a_1\tau = a_1 = a_k\sigma = a_k(\tau\sigma),$$
$$b_l(\sigma\tau) = b_l\tau = b_1 = b_1\sigma = b_l(\tau\sigma).$$

Finally, if $j \in \{a_1, \dots, a_l, b_1, \dots, b_l\}$, then

$$j(\tau\sigma) = (j\tau)\sigma = j\sigma = j = j\tau = (j\sigma)\tau = j(\sigma\tau).$$

Therefore, for each $j \in \{1, \dots, n\}$ we have $j(\sigma\tau) = j(\tau\sigma)$. This yields that $\sigma\tau = \tau\sigma$. ■

Let $\sigma \in S_n$. For each $x, y \in \{1, 2, \dots, n\}$, we define the relation

$$x \equiv_\sigma y \ \Leftrightarrow\ x = x\sigma^k \text{ for some integer } k.$$

Lemma 5.20 *The relation $\equiv_\sigma$ is an equivalence relation.*

Proof Indeed, we have

(1) $x \equiv_\sigma x$ since $x = x\sigma^0$.

(2) If $x \equiv_\sigma y$, then $y = x\sigma^k$. Hence, $x = y\sigma^{-k}$. This implies that $y \equiv_\sigma x$.
(3) If $x \equiv_\sigma y$ and $y \equiv_\sigma z$, then $y = x\sigma^j$ and $z = y\sigma^k$ for some integers j, k. Hence, we obtain

$$z = y\sigma^k = x\sigma^j\sigma^k = x\sigma^{j+k}.$$

This implies that $x \equiv_\sigma z$.

■

This equivalence relation induces a decomposition of $\{1, 2, \ldots, n\}$ into disjoint subsets, namely the equivalence classes. Suppose that m_x is the smallest positive integer such that $x\sigma^{m_x} = x$. Then, the equivalence class of x under σ consists of the numbers $x, x\sigma, x\sigma^2, \ldots, x\sigma^{m_x-1}$.

Theorem 5.21 *Every permutation in S_n can be written as a cycle or as a product of disjoint cycles. Up to reordering the factors, this is unique.*

Proof Let σ be any permutation in S_n. Then, its cycles are of the form $(x\ x\sigma\ x\sigma^2\ \ldots\ x\sigma^{m_x-1})$. Since the cycles of σ are disjoint, it follows that the image of $a \in \{1, 2, \ldots, n\}$ under σ is the same as the image of a under the product, δ, of all distinct cycles of σ. Consequently, σ and δ have the same effect on each element of $\{1, 2, \ldots, n\}$. Therefore, $\sigma = \delta$. In this way, by Lemma 5.19, we observe that every permutation can be uniquely expressed as a product of disjoint cycles. ■

This factorization is called the *cycle decomposition* of σ. The *cycle structure* of σ is the number of cycles of each length in the cycle decomposition of σ. For each $k = 1, \ldots, n$ assume that m_k denote the number of cycles of length k. Then, we say that σ has cycle structure

$$\underbrace{1, \ldots, 1}_{m_1}, \underbrace{2, \ldots, 2}_{m_2}, \ldots, \underbrace{n, \ldots, n}_{m_n}.$$

As notation for cycle type, we abbreviate this to $1^{m_1}, 2^{m_2}, \ldots, n^{m_n}$.

Example 5.22 The permutation

$$\sigma = (1\ 2)(3\ 5\ 6)(4\ 8)$$

in S_8 has cycle structure consisting of one cycle of length 1, two cycles of length 2, and one cycle of length 3.

Theorem 5.23 *The number of permutations in S_n of cycle structure of the form $1^{m_1}, 2^{m_2}, \ldots, n^{m_n}$ is equal to*

$$\frac{n!}{m_1! \ldots m_n! 1^{m_1} 2^{m_2} \ldots n^{m_n}}.$$

Proof A permutation of the given cycle structure is produced by filling the integers $1, 2, \ldots, n$ into the following boxes:

$$\underbrace{\square\cdots\square}_{m_1}\ \underbrace{\square\square\cdots\square\square}_{m_2}\ \cdots\ \underbrace{\square\square\square\cdots\square\square\square}_{m_3}\ \cdots$$

There exist $n!$ ways of doing this. But some of these ways give the same permutation of S_n. We try to count them.

(1) There exist $m_1!$ permutations of cycles of length 1, $m_2!$ permutations of cycles of length 2, $m_3!$ permutations of cycles of length 3, and so on. So, we must divide by $m_1! \ldots m_n!$.
(2) Each cycle of length 2 can be written in two ways, i.e., $(a\ b) = (b\ a)$. Similarly, each cycle of length 3 can be written in three ways, i.e., $(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$, and so on. So we must divide by $1^{m_1} 2^{m_2} \ldots n^{m_n}$.

This completes the proof. ■

Definition 5.24 A cycle of length 2 is called a *transposition*.

Corollary 5.25 *Any cycle in S_n is a product of transpositions.*

Proof If $(a_1\ a_2\ \ldots\ a_k)$ is an arbitrary cycle in S_n, then

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_1\ a_3)\ldots(a_1\ a_n),$$

as desired. ■

Theorem 5.26 *Every permutation in S_n ($n \geq 2$) is either a transposition or a product of transpositions. In other words, S_n is generated by transpositions.*

Proof First, note that the identity permutation can be expressed as $(1\ 2)(1\ 2)$, so it is product of transpositions. By Theorem 5.21, we know that every permutation is a cycle or a product of cycles. By Corollary 5.25, since each cycle is a product of transpositions, it follows that S_n is generated by transpositions. ■

Theorem 5.27 *The symmetric group S_n is generated by $n - 1$ transpositions* $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$.

Proof By Theorem 5.26, we know that S_n is generated by transpositions. Now, if $(a\ b)$ be an arbitrary transposition, then

$$(a\ b) = (1\ a)(1\ b)(1\ a).$$

This yields the desired result. ■

Theorem 5.28 *The symmetric group S_n is generated by $n - 1$ transpositions* $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$.

Proof By Theorem 5.26, it suffices to show that each transposition $(a\ b)$ in S_n is a product of transpositions of the form $(i\ i+1)$, where $i < n$. Suppose that $a < b$. For the proof we use mathematical induction on $b - a$ that $(a\ b)$ is a product of transpositions $(i\ i+1)$. This is obvious when $b - a = 1$, because $(a\ b) = (a\ a+1)$ is one of the transpositions we want in the desired generating set. Now, suppose that $b - a = k > 1$ and the theorem is true for all transpositions moving a pair of integers whose difference is less than k. We have

$$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1).$$

The transpositions $(a\ a+1)$ and $(a\ a+1)$ lie in our desired generating set. For the transposition $(a+1\ b)$ we have $b-(a+1) = k-1 < k$. So, by assumption, $(a+1\ b)$ is a product of transpositions of the form $(i\ i+1)$, so $(a\ b)$ is as well. ■

Lemma 5.29 *A cycle of length m has order m.*

Proof It is straightforward. ■

Theorem 5.30 *The order of a permutation written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

Proof Suppose that $\sigma \in S_n$ and $\sigma = \sigma_1\sigma_2\ldots\sigma_k$, where the σ_i $(i = 1, \ldots, k)$ are disjoint cycles of length m_i. Let m be the least common multiple of $m_1, m_2, \ldots, m_k$. Since $m_i | m$ for each $1 \leq i \leq k$, it follows that

$$\sigma^m = (\sigma_1\sigma_2\ldots\sigma_k)^m = \sigma_1^m\sigma_2^m\ldots\sigma_k^m = id,$$

where id is the identity permutation in S_n. Consequently, the order of σ is at most m.

Now, suppose that $\sigma^r = id$. This implies that $\sigma_1^r\sigma_2^r\ldots\sigma_k^r = id$. Since σ_i $(i = 1, \ldots, k)$ are disjoint, it follows that $\sigma_i^r = id$. Since σ_i is of order m_i, it follows that $m_i | r$. This yields that $m | r$. Therefore, we conclude that σ is of order m. ■

Example 5.31 We want to determine the number of permutations in S_7 of order 3. By Theorem 5.30, it is enough to count the number of permutations of the form

(1) $(a\ b\ c)$,
(2) $(a\ b\ c)(x\ y\ z)$.

For the first case, there exist $7 \cdot 6 \cdot 5$ such triples. But this product counts the permutation $(a\ b\ c)$ three times. Thus, the number of permutations of the form (1) is equal to 70.

For the second case, there exist 70 ways to create the first cycle and $\frac{4\cdot3\cdot2}{3} = 8$ to create the second cycle. So, we have $70 \times 8 = 560$ ways. But this product counts $(a\ b\ c)(x\ y\ z)$ and $(x\ y\ z)(a\ b\ c)$ as distinct while they are equal permutations. Consequently, the number of permutations in S_7 of the form (2) is 280.

Therefore, we have $70 + 280 = 350$ permutations of order 3 in S_7.

Lemma 5.32 *Let σ be any permutation in S_n and let*

$$\sigma = (a_1 \ \dots \ a_i)(b_1 \ \dots \ b_j)\dots(c_1 \ \dots \ c_k)$$

be the cycle decomposition of σ. Then, for each $\tau \in S_n$, we have

$$\tau^{-1}\sigma\tau = (a_1\tau \ \dots \ a_i\tau)(b_1\tau \ \dots \ b_j\tau)\dots(c_1\tau \ \dots \ c_k\tau) \tag{5.1}$$

which is a product of disjoint cycles.

Proof We have

$$\begin{cases} (a_1\tau)\tau^{-1}\sigma\tau = a_1\sigma\tau = a_2\tau, \\ \qquad\vdots \\ (a_{i-1}\tau)\tau^{-1}\sigma\tau = a_{i-1}\sigma\tau = a_i\tau, \\ (a_i\tau)\tau^{-1}\sigma\tau = a_i\sigma\tau = a_1\tau, \end{cases}$$
$$\begin{cases} (b_1\tau)\tau^{-1}\sigma\tau = b_1\sigma\tau = b_2\tau, \\ \qquad\vdots \\ (b_{j-1}\tau)\tau^{-1}\sigma\tau = b_{j-1}\sigma\tau = b_j\tau, \\ (b_j\tau)\tau^{-1}\sigma\tau = b_j\sigma\tau = b_1\tau, \end{cases}$$
$$\vdots$$
$$\begin{cases} (c_1\tau)\tau^{-1}\sigma\tau = c_1\sigma\tau = c_2\tau, \\ \qquad\vdots \\ (c_{k-1}\tau)\tau^{-1}\sigma\tau = c_{k-1}\sigma\tau = c_k\tau, \\ (c_k\tau)\tau^{-1}\sigma\tau = c_k\sigma\tau = c_1\tau. \end{cases}$$

Moreover, if σ do not move integer d, then $\tau^{-1}\sigma\tau$ do not move $d\tau$. So, we see that the right side of (5.1) acts on every integer of $\{1, \dots, n\}$ in the same way as $\tau^{-1}\sigma\tau$. This completes the proof. ■

Now we are ready to cut down the size of a generating set for S_n to two.

Theorem 5.33 *The symmetric group S_n is generated by the transposition* $(1\ 2)$ *and the cycle* $(1\ 2\ \dots\ n)$.

Proof By Theorem 5.28, it is enough to show that the products of $(1\ 2)$ and $(1\ 2\ \dots\ n)$ give all transpositions of the form $(i\ i+1)$. We may take $n \geq 3$. Suppose that $\tau = (1\ 2\ \dots\ n)$. Then, by Lemma 5.32, we have

$$\tau^{-1}(1\ 2)\tau = (1\tau\ 2\tau) = (2\ 3),$$

and more generally for $i = 2, \dots, n-1$, we obtain

$$\tau^{-(i-1)}(1\ 2)\tau^{i-1} = (1\tau^{i-1}\ 2\tau^{i-1}) = (i\ i+1).$$

This completes the proof. ■

Theorem 5.34 *Two permutations in S_n are conjugate if and only if they have the same cycle structure up to ordering.*

Proof Suppose that σ and δ are conjugate. Then, there exists $\tau \in S_n$ such that $\tau^{-1}\sigma\tau = \delta$. Now, by Lemma 5.32, we conclude that σ and δ have the same cycle structure.

Conversely, suppose that

$$\begin{aligned}\sigma &= (a_1 \ \ldots \ a_i)(b_1 \ \ldots \ b_j)\ldots(c_1 \ \ldots \ c_k),\\ \delta &= (a'_1 \ \ldots \ a'_i)(b'_1 \ \ldots \ b'_j)\ldots(c'_1 \ \ldots \ c'_k),\end{aligned}$$

be two permutations of S_n with the same cycle structure. Now, we define τ to be the permutation of S_n which sends

$$\begin{gathered}a_1 \to a'_1, \ \ldots \ a_i \to a'_i,\\ b_1 \to b'_1, \ \ldots \ b_j \to b'_j,\\ \vdots\\ c_1 \to c'_1, \ \ldots \ c_k \to c'_k.\end{gathered}$$

By Lemma 5.32, $\tau^{-1}\sigma\tau$ and δ are the same permutation. ■

Definition 5.35 Two permutations σ and τ in S_n are said to be *similar* if there exists a one to one correspondence between the cycles of σ and τ such that the corresponding cycles have same length.

Corollary 5.36 *Two permutations in S_n are similar if and only if they are conjugate.*

Definition 5.37 A group G is *centerless* if $Z(G) = \{e\}$.

Theorem 5.38 *S_n is centerless if $n \geq 3$.*

$$Z(S_n) = \{id\}.$$

This means that the center of symmetric group is the subgroup comprising only the identity permutation.

Proof Suppose that σ is a non-identity permutation in $Z(S_n)$ and let $\sigma = \sigma_1\sigma_2\ldots\sigma_k$, where σ_is are distinct cycles with lengths l_is such that $l_k \leq \cdots \leq l_2 \leq l_1$. We consider the following two cases:

Case 1: Let $\sigma_1 = (a_1 \ a_2 \ \ldots \ a_m)$ with $m \geq 3$. Since $\sigma \in Z(S_n)$, it follows that $\sigma(a_1 \ a_2) = (a_1 \ a_2)\sigma$. Since σ_is are distinct, it follows that $\sigma_1(a_1 \ a_2) = (a_1 \ a_2)\sigma_1$, or equivalently

$$(a_1 \ a_2 \ \ldots \ a_m)(a_1 \ a_2) = (a_1 \ a_2 \ \ldots \ a_m)(a_1 \ a_2).$$

This is a contradiction, because in the left side of the equality we have $a_m \to a_1$ while in the right side we have $a_m \to a_2$.

Case 2: Let $\sigma_1 = (a_1\ a_2)$. Since $n \geq 3$, it follows that there exists a_3 such that $a_3 \neq a_1$ and $a_3 \neq a_2$. Since $\sigma \in S_n$, it follows that $\sigma(a_1\ a_2\ a_3) = (a_1\ a_2\ a_3)\sigma$, or equivalently

$$(a_1\ a_2)\sigma_2 \ldots \sigma_k(a_1\ a_2\ a_3) = (a_1\ a_2\ a_3)(a_1\ a_2)\sigma_2 \ldots \sigma_k.$$

Since a_1 and a_2 do not appear in cycles $\sigma_2, \ldots, \sigma_k$, it follows that in the left side of the last equality $a_1 \to a_3$ while in the right side $a_1 \to a_1$. This is again a contradiction.

Therefore, we conclude that $Z(S_n) = \{id\}$. ■

Exercises

1. Let

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

Compute each of the following:

(a) α^{-1};
(b) $\alpha\beta\alpha^{-1}$;
(c) $\alpha^3\beta$;
(d) $\alpha\beta^{-2}$.

2. Write each of the following permutations as a product of distinct cycles:

(a) $(3\ 4\ 5\ 6)(4\ 3)(1\ 2\ 3)$;
(b) $(1\ 2)(2\ 3)(2\ 4)(1\ 3\ 5)$.

3. Give the Cayley table for the cyclic subgroup of S_5 generated by

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

4. Determine eight elements in S_6 that commute with $(1\ 2)(5\ 6)(3\ 4)$. Do they form a subgroup of S_6?
5. Find five subgroups of S_5 of order 24.
6. Find the number of permutations in the set $\{\sigma \in S_5 \mid 2\sigma = 5\}$.
7. How many elements of order 6 are there in the symmetric group S_{11}?
8. Find all powers of the cycle $\sigma = (x_1\ x_2\ \ldots\ x_n)$.
9. Find all permutations in the symmetric group S_n which commute with the cycle $(x_1\ x_2\ \ldots\ x_n)$, where $x_1\ x_2\ \ldots\ x_n$ is a permutation of the numbers $1, 2, \ldots, n$.
10. Count the number of elements of S_n having at least one fixed point.

11. Given the permutations $\alpha = (1\ 2)(3\ 4)$ and $\beta = (1\ 3)(5\ 6)$. Find a permutation γ such that $\gamma^{-1}\alpha\gamma = \beta$. Is γ unique?
12. Prove that the permutations

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

are conjugate in the symmetric group S_6, and find the number $\gamma \in S_6$ such that $\gamma^{-1}\alpha\gamma = \beta$.
13. Show that the permutations in S_9 which send the numbers $2,\ 5,\ 7$ among themselves form a subgroup of S_9. What is the order of this subgroup?
14. If n is at least 3, show that for some $f \in S_n$, f cannot be expressed in the form $f = g^3$, for any $g \in S_n$.
15. What is the smallest positive integer n such that S_n has an element of order greater than $2n$?
16. Show that in S_7, the equation $x^2 = (1\ 2\ 3\ 4)$ has no solutions but the equation $x^3 = (1\ 2\ 3\ 4)$ has at least two.
17. Let X be the set $\mathbb{Z}_{31}$, and let $f : X \to X$ be the permutation $f(x) = 2x$. Decompose this permutation into disjoint cycles.
18. Let X be the set $\mathbb{Z}_{29}$, and let $f : X \to X$ be the permutation $f(x) = x^3$. Decompose this permutation into disjoint cycles.
19. Find the cycle decomposition of the permutation induced by the action of complex conjugation on the set of roots of $x^5 - x + 1$.
20. In S_4, find the subgroup generated by $(1\ 2\ 3)$ and $(1\ 2)$. Also, for this subgroup, find the corresponding subgroup $\sigma^{-1}H\sigma$, for $\sigma = (1\ 4)$.
21. Find necessary and sufficient conditions on the pair i and j in order that $\langle(1\ 2\ \ldots\ n),\ (i\ j)\rangle = S_n$.
22. Show that for all $1 < i \leq n$, we have $\langle(2\ 3\ \ldots\ n),\ (1\ i)\rangle = S_n$.
23. Determine a permutation $\sigma \in S_n$ such that for every $1 \leq i, j \leq n$,

$$i \leq j \Rightarrow i\sigma \leq j\sigma.$$

24. Find the maximum possible order for a permutation in S_n for $n = 5$, $n = 6$, $n = 7$, $n = 10$, and $n = 15$.
25. A permutation is called *regular* if it can be decomposed into disjoint cycles of the same length. Prove that every power of a cycle of length n in S_n is a regular permutation. Prove that the length of each of the disjoint cycles in this decomposition divides n.
26. Prove that every regular permutation is a power of some cycle.

5.3 Alternating Groups

The alternating groups are among the most important examples of groups. We study some of their properties in this section.

Theorem 5.39 *If a permutation σ can be expressed as a product of even number of transpositions, then every decomposition of σ into a product of transpositions must have an even number of transpositions. In symbols, if*

$$\sigma = \tau_1\tau_2\ldots\tau_k \text{ and } \sigma = \delta_1\delta_2\ldots\delta_m$$

where the τ's and the δ's are transpositions, then k and m are both even or both odd.

Proof We consider a polynomial p of n variable

$$\begin{aligned} p(a_1,\ldots,a_n) &= (a_1-a_2)(a_1-a_3)\ldots(a_1-a_n)\\ &\quad (a_2-a_3)(a_2-a_4)\ldots(a_2-a_n)\ldots(a_{n-1}-a_n)\\ &= \prod_{i<j}(a_i-a_j). \end{aligned}$$

If $\sigma \in S_n$, we define

$$\sigma^*\big(p(a_1,\ldots,a_n)\big) = \prod_{i<j}(a_{i\sigma}-a_{j\sigma}).$$

Suppose that $\tau = (r\ s)$ is a transposition with $r < s$. Then, we have

$$\tau^*\big(p(a_1,\ldots,a_n)\big) = \prod_{i<j}(a_{i\tau}-a_{j\tau}).$$

Note that $a_{r\tau} - a_{s\tau} = a_s - a_r = -(a_r - a_s)$, and if a_r and a_s do not exist in a factor, then this factor is fixed under τ. The other factors can be expressed in one of the following forms:

(1) $(a_s - a_k)(a_r - a_k)$, if $s < k$,
(2) $(a_k - a_s)(a_r - a_k)$, if $r < k < s$,
(3) $(a_k - a_s)(a_k - a_r)$, if $k < r$.

Therefore, we conclude that $\tau^*\big(p(a_1,\ldots,a_n)\big) = -f(a_1,\ldots,a_n)$.

If $\sigma = \tau_1\tau_2\ldots\tau_k$, where $\tau_1,\tau_2,\ldots,\tau_k$ are transpositions, then

$$\begin{aligned} \sigma^*\big(p(a_1,\ldots,a_n)\big) &= \big(\tau_1\tau_2\ldots\tau_k\big)^*\big(p(a_1,\ldots,a_n)\big)\\ &= (-1)^k p(a_1,\ldots,a_n). \end{aligned} \tag{5.2}$$

Similarly, if $\sigma = \delta_1\delta_2\ldots\delta_m$, where $\delta_1,\delta_2,\ldots,\delta_m$ are transpositions, then

$$\begin{aligned}\sigma^*\big(p(a_1,\ldots,a_n)\big) &= \big(\delta_1\delta_2\ldots\delta_m\big)^*\big(p(a_1,\ldots,a_n)\big)\\ &= (-1)^m p(a_1,\ldots,a_n).\end{aligned} \tag{5.3}$$

Comparing (5.2) and (5.3), we conclude that

$$(-1)^k = (-1)^m.$$

This implies that these two decompositions of σ as the product of transpositions are of the same parity. ■

Therefore, any permutation is either the product of an odd number of transpositions or the product of an even number of transpositions, and no product of an even number of transpositions can be equal to a product of an odd number of transpositions.

Definition 5.40 A permutation which can be expressed as a product of an even number of transpositions is called an *even permutation*. A permutation which can be expressed as a product of an odd number of transpositions is called an *odd transposition*.

If we define the sign of a permutation σ as

$$\operatorname{sgn}(\sigma) = \frac{p(a_{1\sigma},\ldots,a_{n\sigma})}{p(a_1,\ldots,a_n)},$$

then

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

If $\sigma, \delta \in S_n$, then

$$\begin{aligned}\operatorname{sgn}(\sigma\delta) &= \frac{p(a_{1\sigma\delta},\ldots,a_{n\sigma\delta})}{p(a_1,\ldots,a_n)}\\ &= \frac{p(a_{1\sigma\delta},\ldots,a_{n\sigma\delta})}{p(a_{1\sigma},\ldots,a_{n\sigma})}\cdot\frac{p(a_{1\sigma},\ldots,a_{n\sigma})}{p(a_1,\ldots,a_n)}\\ &= \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\delta).\end{aligned}$$

To summarize in words, the sign of the product is the product of sign,

$$\begin{aligned}&\text{even} \times \text{even} = \text{odd} \times \text{odd} = \text{even},\\ &\text{even} \times \text{odd} = \text{odd} \times \text{even} = \text{odd}.\end{aligned}$$

Theorem 5.41 *If A_n is the set of all even permutations, then A_n is a subgroup of S_n.*

Proof If $\sigma, \delta \in A_n$, then we have $\sigma\delta \in A_n$. Since A_n is a finite closed subset of the finite group S_n, it follows that A_n is a subgroup of S_n. ■

A_n is called the *alternating group* of degree n.

Theorem 5.42 *If $n > 1$, the order of A_n is equal to $n!/2$.*

Proof For each even permutation σ, the permutation $(1\ 2)\sigma$ is odd, and if $\sigma \neq \delta$, then $(1\ 2)\sigma \neq (1\ 2)\delta$. Hence, there are at least as many odd permutations as there are even ones. On the other hand, for each odd permutation σ, the permutation $(1\ 2)\sigma$ is even, and if $\sigma \neq \delta$, then $(1\ 2)\sigma \neq (1\ 2)\delta$. Hence, there are at least as many even permutations as there are odd ones. This yields that there exist equal numbers of even and odd permutations. Since $|S_n| = n!$, it follows that $|A_n| = n!/2$. ■

Theorem 5.43 *For each $n \geq 3$, A_n is generated by cycles of length* 3.

Proof Suppose that $\sigma \in A_n$. Then, σ is a product of even number of transpositions. Let a, b, c, and d are four different numbers between 1 and n. Then, we have

$$(a\ b)(a\ c) = (a\ b\ c),$$
$$(a\ b)(c\ d) = (a\ c\ b)(c\ b\ d).$$

This completes the proof. ■

Theorem 5.44 *For each $n \geq 3$, A_n is generated by cycles of the form $(1\ a\ b)$, where $2 \leq a, b \leq n$, and $a \neq b$.*

Proof If $\sigma \in A_n$, then σ is a product of transpositions. Since $(a\ b) = (1\ a)(1\ b)(1\ a)$ for each $2 \leq a, b \leq n$, and $a \neq b$, it follows that σ is a product of transpositions of the form $(1\ a)$. Since σ is even, the number of transpositions of the form $(1\ a)$ in σ is even. But for each $a \neq b$, we have $(1\ a)(1\ b) = (1\ a\ b)$. This completes the proof. ■

Theorem 5.45 *For each $n \geq 3$, A_n is generated by cycles of the form $(1\ 2\ a)$, where $2 \leq a \leq n$.*

Proof If $n = 3$, then $A_3 = \{id,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ is generated by $(1\ 2\ 3)$. So, we assume that $n \geq 4$.

Each cycle of length 3 in A_n containing 1 and 2 is generated by the cycle of the form $(1\ 2\ a)$, because $(1\ a\ 2) = (1\ 2\ a)^{-1}$.

For each cycle of length 3 in A_n containing 1 but not 2, we have

$$(1\ a\ b) = (1\ 2\ b)(1\ 2\ a)(1\ 2\ b)(1\ 2\ b).$$

Now, by Theorem 5.44, the proof completes. ■

Theorem 5.46 *For each $n \geq 3$, A_n is generated by consecutive cycles of the form $(a\ a+1\ a+2)$, where $1 \leq a \leq n-2$.*

Proof If $n = 3$, then $A_3 = \langle(1\ 2\ 3)\rangle$. If $n = 4$, then by Theorem 5.45, $A_4 = \langle(1\ 2\ 3), (1\ 2\ 4)\rangle$. Since

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

it follows that $A_4 = \langle(1\,2\,3), (2\,3\,4)\rangle$. Now, assume that $n \geq 5$. By Theorem 5.45, it suffices to show that $(1\,2\,a)$ can be obtained from a product of consecutive cycles of length 3. We apply mathematical induction on a. Let $a \geq 5$ and $(1\,2\,b)$ be a product of consecutive cycles of length 3, for $3 \leq b < a$. We have

$$(1\,2\,a) = (1\,2\,a-1)(1\,2\,a-2)(a-2\,a-1\,a)(1\,2\,a-1)(1\,2\,a-2).$$

Now, the inductive assumption show that $(1\,2\,a)$ is a product of consecutive cycles of length 3. ■

Theorem 5.47 *For each $n \geq 3$, A_n is generated by*

(1) $(1\,2\,3)$ *and* $(1\,2\,\ldots\,n)$ *if n is odd;*
(2) $(1\,2\,3)$ *and* $(2\,3\,\ldots\,n)$ *if n is even.*

Proof Note that if $n = 3$, then we are done. So, we suppose that $n \geq 4$.

(1) Let n be odd and $\tau = (1\,2\,\ldots\,n)$. Then, we conclude that $\tau \in A_n$. Moreover, for each $1 \leq a \leq n-3$, by Lemma 5.32, we get

$$\tau^{-a}(1\,2\,3)\tau^a = (1\tau^a\,2\tau^a\,3\tau^a) = (a+1\,a+2\,a+3) \in A_n.$$

Now, by Theorem 5.46, we are done.

(2) Let n is even and $\tau = (2\,3\,\ldots\,n)$. Then, we have $\tau \in A_n$. Also, for each $1 \leq a \leq n-3$, by Lemma 5.32, we obtain

$$\tau^{-a}(1\,2\,3)\tau^a = (1\tau^a\,2\tau^a\,3\tau^a) = (1\,a+2\,a+3) \in A_n.$$

Finally, since $(1\,a+1\,a+2)$ and $(1\,a\,a+1)$ are in A_n, we can write

$$(1\,a+1\,a+2)(1\,a\,a+1) = (a\,a+1\,a+2) \in A_n.$$

Now, by Theorem 5.46, the proof completes. ■

Theorem 5.48 *If $n \geq 5$, then all cycles of length 3 are conjugate in A_n.*

Proof Suppose that σ and δ are two cycles of length 3 in A_n. By Theorem 5.34, there exists a permutation $\tau \in S_n$ such that $\tau^{-1}\sigma\tau = \delta$. If $\tau \in A_n$, then we are done. So, suppose that $\tau \notin A_n$. Let $\sigma = (a\,b\,c)$. Since $n \geq 5$, it follows that there exist x and y not in $\{a, b, c\}$. We set $\theta = (x\,y)$. Since $\theta^{-1}\sigma\theta = \sigma$, it follows that $(\theta\tau)^{-1}\sigma(\theta\tau) = \delta$, where $\theta\tau \in A_n$. ■

Theorem 5.49 *For each $n \geq 4$, the center of A_n is*

$$Z(A_n) = \{id\}.$$

This means that A_n is centerless, for $n \geq 4$.

Proof We show that, for every non-identity permutation σ, there is a permutation in A_n that does not commute with σ.

Since σ is not the identity, it follows that σ maps an element a into b with $a \neq b$. Since $n \geq 4$, we can choose distinct c and d not equal to a and b. Now, we claim that the cycle $(b\ c\ d)$ does not commute with σ. Indeed, $\sigma(b\ c\ d)$ maps a into c, but $(b\ c\ d)\sigma$ maps a into b. Therefore, no σ other than the identity commutes with every element of A_n. In other words, no σ other than the identity is in the center of A_n. Thus, the only element of the center of A_n is the identity. ■

Exercises

1. Let σ and τ belong to S_n. Prove that $\sigma^{-1}\tau^{-1}\sigma\tau$ is an even permutation.
2. Prove that there is no permutation σ such that $\sigma^{-1}(1\ 3\ 4)\sigma = (1\ 2)(4\ 6\ 7)$.
3. Compute the order of each member of A_4. What arithmetic relationship do these orders have with the order of A_4?
4. Prove that A_5 has a subgroup of order 12.
5. Show that A_4 has no subgroup of order 6.
6. Show that the group A_5 contains no elements of order 4, and precisely 15 elements of order 2. How many elements of are there of orders 3, 6, respectively?
7. Show that A_8 contains an element of order 15.
8. Find a cyclic subgroup of A_8 that has order 4.
9. Find a non-cyclic subgroup of A_8 that has order 4.
10. Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n.
11. Let n be an even positive integer. Prove that A_n has an element of order greater than n if and only if $n \geq 8$.
12. Let n be an odd positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 13$.
13. Let n be an even positive integer. Prove that A_n has an element of order greater than $2n$ if and only if $n \geq 14$.
14. Let $H = \{\sigma^2 \mid \sigma \in S_4\}$ and $K = \{\sigma^2 \mid \sigma \in S_5\}$. Prove that $H = A_4$ and $K = A_5$.
15. Let $H = \{\sigma^2 \mid \sigma \in S_6\}$. Prove that $H \neq A_6$.
16. Why does the fact that the orders of the elements of A_4 are 1, 2, and 3 imply that $|Z(A_4)| = 1$?
17. For $n > 1$, let H be the set of all permutations in S_n that can be expressed as a product of a multiple of four transpositions. Show that $H = A_5$.
18. Consider S_n for a fixed $n \geq 2$ and let σ be a fixed odd permutation. Show that every odd permutation in S_n is a product of σ and some permutation in A_n.
19. Show that if σ is a cycle of odd length, then σ^2 is a cycle.
20. Show that every permutation in A_n is a product of cycles of length n.

5.4 Worked-Out Problems

Problem 5.50 Show that if $n \geq m$, then the number of cycles of length m in S_n is given by

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}. \tag{5.4}$$

Solution We count how many cycles of length m in S_n exist. We have to fill the boxes:

			$\dots$	
1	2	3		m

with the numbers $1, 2, \dots, n$ with no repetitions. We have n choice for the first box. Then, $n-1$ choice for the second box, $n-2$ choice for the third box, and so on. Finally, we have $n-m+1$ choice for the last box. So, there are $n(n-1)(n-2)\dots(n-m+1)$ choices for a cycle of length m, but we emphasis that some them are the same. For example, the following cycles are the same:

- If $m = 2$, then $(a\ b) = (b\ a)$ (2 equivalent notations);
- If $m = 3$, then $(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$ (3 equivalent notations);
- If $m = 4$, then $(a\ \ b\ \ c\ \ d) = (b\ \ c\ \ d\ \ a) = (c\ \ d\ \ a\ \ b) = (d\ \ a\ \ b\ \ c)$ (4 equivalent notations).

In general, by induction we deduce that for cycles of length m, there are m equivalent notations. Since we have $n(n-1)(n-2)\dots(n-m+1)$ choices to form a cycle of length m in which there are m equivalent notations, it follows that the number of cycles of length m in S_n is equal to (5.4). ■

Problem 5.51 If n is at least 4, show that every element of S_n can be written as a product of two permutations, each of which has order 2. (Experiment first with cycles.)

Solution First, we begin with an example. Let $(a_1\ a_2\ \dots\ a_7)$ be a cycle. We consider

$$\begin{aligned}\alpha &= (a_1\ a_7)(a_2\ a_6)(a_3\ a_5)\\ \beta &= (a_2\ a_7)(a_3\ a_6)(a_4\ a_5).\end{aligned}$$

Since α and β are products of disjoint transpositions, it follows that $o(\alpha) = o(\beta) = 2$. Moreover, it is easy to see that $\alpha\beta = (a_1\ a_2\ \dots\ a_7)$. Next, we generalize the above example to an arbitrary cycle $\sigma = (a_1\ a_2\ \dots\ a_n)$. We take

$$\begin{aligned}\alpha &= (a_1\ a_n)(a_2\ a_{n-1})\dots(a_i\ a_{n-i+1})\dots(a_m\ a_{n-m+1}),\\ \beta &= (a_2\ a_n)(a_3\ a_{n-1})\dots(a_{i+1}\ a_{n-i+1})\dots(a_{m+1}\ a_{n-m+1}),\end{aligned}$$

where $m = [n/2]$. Again, since α and β are products of disjoint transpositions, it follows that $o(\alpha) = o(\beta) = 2$. Now, we claim that $\sigma = \alpha\beta$. Since α and β are products

Table 5.1 A short table of values $p(n)$

n	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42

of disjoint transpositions, what they do to any one a_i is determined just by the transposition containing that a_i. Hence, for $i \leq m$, the transposition $(a_i\ a_{n-i+1})$ in α sends a_i to a_{n-i+1} and then the transposition $(a_{i+1}\ a_{n-i+1})$ in β sends a_{n-i+1} to a_{i+1}. In view of this, if $i \leq m$, then $\alpha\beta$ sends a_i to a_{i+1}. Now, if $i > m$, then we take $j = n - i + 1$. We have $j \leq m$ and $i = n - j + 1$. So, the transposition $(a_j\ a_{n-j+1})$ is in α and it sends $a_i = a_{n-j+1}$ to a_j and the transposition $(a_{j-1+1}\ a_{n-(j-1)+1}) = (a_j\ a_{n-j+2})$ in β sends a_j to a_{n-j+2}. But since $j = n - i + 1$, it follows that $n - j + 2 = i + 1$. Therefore, we observe that $\alpha\beta$ sends a_i to a_{i+1} when $i > m$. Consequently, $\sigma = \alpha\beta$.

Finally, suppose that σ is an arbitrary permutation. We can write $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$, where σ_is are disjoint cycles. According to the above argument, each of σ_i can be written as the product of two permutations α_i and β_i, where $o(\alpha_i) = o(\beta_i) = 2$, and α_i and β_i only permute the numbers appear in σ_i. Since σ_is are disjoint, if $j \neq i$, then α_i and β_i are disjoint from α_j and β_j. Consequently, α_i commutes with α_j and β_i, for all $i \neq j$. Therefore, we conclude that

$$\begin{aligned}\sigma = \sigma_1\sigma_2 \ldots \sigma_k &= \alpha_1\beta_1\alpha_2\beta_2 \ldots \alpha_k\beta_k \\ &= \alpha_1\alpha_2 \ldots \alpha_k\beta_1\beta_2 \ldots \beta_k.\end{aligned}$$

Since a product of disjoint transpositions has order 2, it follows that

$$o(\alpha_1\alpha_2 \ldots \alpha_k) = o(\beta_1\beta_2 \ldots \beta_k).$$

This completes the proof.

■

Problem 5.52 Let n be a positive integer. A sequence of positive integers $n_1, n_2, \ldots,$ n_k such that $n_1 \geq n_2 \geq \cdots \geq n_k$ and $n = n_1 + n_2 + \cdots + n_k$, is called a *partition of* n. Let $p(n)$ denote the number of partitions of n. Table 5.1 is a short table of values $p(n)$: Show that the number of conjugate classes in the symmetric group S_n is $p(n)$.

Solution Let σ be a permutation in S_n. We can write σ as a product of distinct cycles as follows:

$$(a_1\ a_2\ \ldots\ a_{k_1})(b_1\ b_2\ \ldots\ b_{k_2}) \ldots (c_1\ c_2\ \ldots\ c_{k_j})$$

such that $k_1 \geq k_2 \geq \cdots \geq k_j$ and $k_1 + k_2 + \cdots + k_j = n$. This is a unique expression, and so for each permutation we obtain a unique partition. By Corollary 5.36, two permutations are conjugate if and only if they are similar; in other words, they give rise to same partition. Hence, corresponding to a conjugate class we get a unique partition of n.

Conversely, let $n_1 \geq n_2 \geq \cdots \geq n_r$ and $n = n_1 + n_2 + \cdots + n_r$ be a partition of n. Then, there is a permutation τ which has a cycle decomposition of the type

$$(x_1\ x_2\ \ldots\ x_{n_1})(y_1\ y_2\ \ldots\ y_{n_2})\ldots(z_1\ z_2\ \ldots\ z_{n_r}).$$

Each $\delta \in S_n$ similar to τ is conjugate to τ, and every permutation in S_n conjugate to τ is similar to τ. In this way, for each permutation we can associate a unique conjugate class, namely, conjugate class of τ.

Therefore, there exists a one to one correspondence between conjugate classes in S_n and partitions of n. Consequently, the number of conjugate classes in S_n is equal to $p(n)$.

■

Problem 5.53 Let $s(n,k)$ denote the number of permutations in S_n which have exactly k cycles (including cycles of length 1). Show that

$$s(n,1) = (n-1)!$$

and for $k \geq 2$

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k).$$

Also, prove that

$$\sum_{k=1}^{n} s(n,k)x^k = x^{(n)} := x(x+1)\ldots(x+n-1).$$

The $s(n,k)$ are known as *Stirling numbers of the first kind*. The expression $x^{(n)}$ is known as the *nth upper factorial*.

Solution It is easy to see that $s(n,1) = (n-1)!$. In general, we sort the permutations in S_n with exactly k cycles into two parts, depending on whether the permutation contains the cycle (n) of length 1. There exist $s(n-1,k-1)$ permutations containing the cycle (n). The other permutations are formed by inserting n after any of the $n-1$ elements in the $s(n-1,k)$ permutations of $n-1$ elements into k cycles. Consequently, for $k \geq 2$, we obtain $s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k)$. Now, we can verify the formula for $s(n,k)$ by induction. It is easy to see that the formula holds for $n = 1$. Suppose the formula is true for $s(m,k)$, where $m < n$. Then, we have

$$
\begin{aligned}
&\sum_{k=1}^{n} s(n,k)x^k \\
&\quad = (n-1)!x + \sum_{k=2}^{n} s(n-1,k-1)x^k + (n-1)\sum_{k=2}^{n} s(n-1,k)x^k \\
&\quad = (n-1)!x + x\sum_{k=1}^{n-1} s(n-1,k)x^k \\
&\qquad\qquad + (n-1)\left(\sum_{k=1}^{n} s(n-1,k)x^k - (n-2)!x\right) \\
&\quad = (n-1)!x + xx^{(n-1)} + (n-1)\big(x^{(n-1)} - (n-2)!x\big) \\
&\quad = (x+n-1)x^{(n-1)} \\
&\quad = x^{(n)},
\end{aligned}
$$

as desired. ■

5.5 Supplementary Exercises

1. Let G be a group of order $2m$, let $g \in G$ have order 2, and let $\lambda_g : G \to G$ be defined by $g(x) = gx$. Show that λ_g is a product of m disjoint transpositions.
2. Show that the symmetry group of a rectangle which is not a square has order 4. By labeling the vertices, 1, 2, 3, 4 represents the symmetry group as a group of permutations of the set $\{1,\ 2,\ 3,\ 4\}$.
3. Prove that S_X is abelian if and only if $|X| \leq 2$.
4. Let H be a subgroup of S_n. Show that either H is a subset of A_n or exactly half of the elements of H are even permutation.
5. List the elements of the following subgroup in S_4:

$$\langle (1\ 4)(2\ 3),\ (1\ 2)(3\ 4)\rangle.$$

6. Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 8 & 3 & 1 & 6 & 9 & 4 & 10 & 12 & 13 & 5 & 11 & 15 & 16 & 14 & 2 & 7 \end{pmatrix} \in S_{16}.$$

   (a) Find its sign and its order. Compute the centralizer σ and compute the number of elements in this centralizer;
   (b) Write down σ^{1000} as a product of disjoint cycles.

7. Let G be a non-abelian group of order $2p$ for some prime $p \neq 2$. Prove that G contains exactly $p-1$ elements of order p and it contains exactly p elements of order 2.
8. If p is a prime number, show that in S_p there are $(p-1)! + 1$ elements x satisfying $x^p = e$.

9. In the symmetric group S_4 find two elements that neither commute with each other and are not conjugate to one another.
10. Let σ be the cycle $(1\ 2\ \dots\ m)$. Show that σ^k is also a cycle of length m if and only if k is relatively prime to m.
11. Which permutation of the set $X = \{x_1,\ x_2,\ x_3,\ x_4,\ x_5\}$ leave the polynomial $x_1 + x_2 - x_3 - x_4$ invariant? Find a polynomial in these variables which is left invariant under all permutations in the group $\langle (x_1\ x_2\ x_3\ x_4),\ (x_2\ x_4)\rangle$ but not by all of S_X.
12. If $\sigma \in A_n$, prove that

$$C_{A_n}(\sigma) = C_{S_n}(\sigma) \text{ or } |C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|.$$

13. If $\sigma = (1\ 2\ \dots\ m) \in S_n$, show that $|C_{S_n}(\sigma)| = (n-m)!m$.
14. Let $a(n, m)$ denote the number of permutations $\sigma \in S_n$ such that $\sigma^m = Id$ (with $a(0, m) = 1$). Show that

$$\sum_{n=0}^{\infty} \frac{a(n, m)}{n!} x^n = \exp\left(\sum_{d|m} \frac{x^d}{d}\right).$$

15. Let $n \geq 2$ and let A be the set of all permutations in S_n of the form

$$\sigma_k = \prod_{1 \leq i \leq k/2} (i\ k-i),$$

for $k = 3,\ 4,\ \dots,\ n+1$. Show that A generates S_n and that each $\sigma \in S_n$ can be written as a product of $2n-3$ or fewer elements from A.
16. Let p be a prime congruent to 1 (mod 4), and consider the set

$$X = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

Show that the function

$$(x, y, z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{if } x > 2y \end{cases}$$

is a permutation of order 2 on X with exactly one fixed point. Conclude that the permutation $(x, y, z) \mapsto (x, z, y)$ must also have at least one fixed point, and so $x^2 + 4y^2 = p$ for some positive integers x and y.
17. Find the permutation representation of a cyclic group of order n.
18. **(Stirling Numbers of the Second Kind).** In Problem 5.53, we have seen that the Stirling numbers $s(n, k)$ of the first kind count the number of ways to partition a set of size n into k disjoint non-empty cycles. The Stirling numbers of the second

kind, denoted by $S(n, k)$, count the number of ways to partition a set of size n into k non-empty disjoint subsets. It is clear that $S(n, 1) = 1$.

(a) Find $S(n, 2)$;
(b) For $n > 0$, show that $S(n, k) = kS(n-1, k) + S(n-1, k-1)$;
(c) Show that

$$x^n = \sum_{k=1}^{n} S(n, k) x^{(k)}.$$

19. In the symmetric group S_n, for each $k = 3, \ \ldots, \ n$, let

$$\sigma_k = \prod_{i=1}^{[\frac{k}{2}]} (i \ k-i),$$

for example

$$\begin{aligned}
\sigma_3 &= (1\ 2),\\
\sigma_4 &= (1\ 3),\\
\sigma_5 &= (1\ 4)(2\ 3),\\
\sigma_6 &= (1\ 5)(2\ 4),\\
\sigma_7 &= (1\ 6)(2\ 5)(3\ 4),\\
\sigma_8 &= (1\ 7)(2\ 6)(3\ 5).
\end{aligned}$$

Show that permutations $\sigma_1, \ \sigma_2, \ \ldots, \ \sigma_n$ generate S_{n-1}.

20. An *affine geometry* comprises a set X whose elements are called *points* together with various subsets of X called *lines* such that

(a) Each pair of distinct points is contained in exactly one line;
(b) Each pair of distinct lines has at most one point in common;
(c) Given a line L and a point P not on it, there exists exactly one line L' which contains P and has no point in common with L;
(d) There are at least two lines. Figure 5.2 gives a pictorial representation of an affine geometry with 4 points and 6 lines.

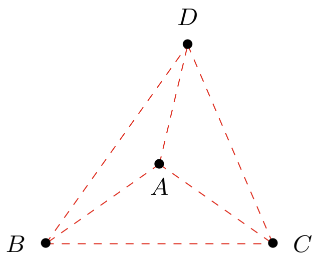

Fig. 5.2 Affine geometry

A *collineation* of an affine geometry is a permutation of the points of X which maps lines to lines. Show that the set of all collineations form a group under composition. What is the order of the collineation group of the above 4 element affine geometry?