

§15 Symmetric Groups

For any nonempty set X , the set S_X of all one-to-one mappings from X onto X is a group under the composition of functions. (Example 7.1(d)). In particular, choosing X to be the set $\{1, 2, \dots, n\}$ of the first n natural numbers, we get a group $S_{\{1, 2, \dots, n\}}$. We abbreviate this group as S_n .

15.1 Definition: Let $n \in \mathbb{N}$. The group of all one-to-one mappings from $\{1, 2, \dots, n\}$ onto $\{1, 2, \dots, n\}$ is called the *symmetric group (on n letters)* and is written S_n . The elements of S_n are called *permutations (of $1, 2, \dots, n$)*.

The reader should not confuse the symmetric group with the symmetry group of a figure in the Euclidean plane.

15.2 Theorem: S_n is a group of order $n!$.

Proof: Let $\pi \in S_n$ be a permutation of $1, 2, \dots, n$. Then 1π is one of the numbers $1, 2, \dots, n$. Since π is one-to-one, $1\pi \neq 2\pi$, so 2π is one of the remaining $n - 1$ numbers among $1, 2, \dots, n$ after 1π has been determined. Since π is one-to-one, $1\pi \neq 3\pi$ and $2\pi \neq 3\pi$, so 3π is one of the remaining $n - 2$ numbers among $1, 2, \dots, n$ after 1π and 2π have been determined. Proceeding in this way, we see that, for any $k = 1, 2, \dots, n$, the number $k\pi$ must be one of the numbers among $1, 2, \dots, n$ which are distinct from $1\pi, 2\pi, \dots, (k - 1)\pi$. Hence there are n choices for 1π ; and $n - 1$ choices for 2π ; ...; and $n - (k - 1)$ choices for $k\pi$; ...; and $n - (n - 1)$ choices for $n\pi$; and all these choices give a permutation of $1, 2, \dots, n$. Therefore there are

$$n.(n - 1).(n - 2). \dots .2.1 = n!$$

permutations in S_n .

□

We introduce a notation for permutations. Let $n \in \mathbb{N}$ and $\pi \in S_n$. Then π is a mapping $\pi: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ and can be exhibited by associating any number in $\{1, 2, \dots, n\}$ with its image by an arrow. Thus $\pi \in S_n$ for which $1\pi = 3, 2\pi = 1, 3\pi = 2, 4\pi = 5, 5\pi = 4$ can be displayed as

$$\begin{array}{l} 1 \quad \rightarrow 3 \\ 2 \rightarrow 1 \\ 3 \rightarrow 2 \\ 4 \rightarrow 5 \\ 5 \rightarrow 4, \end{array}$$

or, in order to save space, as

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 3 & 1 & 2 & 5 & 4 & \end{array}$$

We simplify this notation further by deleting the arrows and enclosing the two rows of numbers in parentheses. Thus we arrive at

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

for our π . In general, we write any $\sigma \in S_n$ as

$$\begin{pmatrix} \dots & a & \dots \\ \dots & a\sigma & \dots \end{pmatrix}$$

In this notation, there are two rows of n elements and n columns of two elements. The rows consist of the numbers $1, 2, \dots, n$. The image under σ of any $a \in \{1, 2, \dots, n\}$ is written just below a in the second row. This notation is due to A. Cauchy (1789-1857).

The order of the columns is immaterial in this notation. For example

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

are all equal permutations in S_6 .

The identity permutation $\iota \in S_n$ maps any a to a , so the rows will be identical. Thus

$$\iota = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

The inverse of any $\sigma \in S_n$ is found easily. By definition, σ^{-1} is the function (permutation) that maps $a\sigma$ to a , for all $a \in \{1, 2, \dots, n\}$. Let σ be $\begin{pmatrix} \dots & a & \dots \\ \dots & a\sigma & \dots \end{pmatrix}$. Then, under σ^{-1} , any element in the second row is mapped to the number just above it. σ^{-1} is therefore obtained by interchanging the rows of σ . For instance, in S_7 , we have

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 3 & 5 & 4 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 6 & 3 & 5 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$, which may also be written as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 5 & 4 & 2 & 1 \end{pmatrix}$. Two permutations in S_n , say π and σ , are

multiplied as follows. We have $\pi = \begin{pmatrix} \dots & a & \dots \\ \dots & a\pi & \dots \end{pmatrix}$ and $\sigma = \begin{pmatrix} \dots & b & \dots \\ \dots & b\sigma & \dots \end{pmatrix}$. What is $\pi\sigma$? By definition, $\pi\sigma$ is the permutation that maps a to $(a\pi)\sigma$, for all a in $\{1, 2, \dots, n\}$. To evaluate $(a\pi)\sigma$, we locate a in the first row of π , then read the number below it, which is $a\pi$, and locate this $a\pi$ in the first row of σ . The number below it is $(a\pi)\sigma$. We do this for $a = 1, 2, \dots, n$ and in each case, write the number we obtain below a . Enclosing this configuration in parentheses, we get $\pi\sigma$ in double row notation. Here is an example.

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

In the first permutation, below 1, we see 5 and in the second permutation, below 5, we see 4. So, in the product, below 1, we write 4. Then, in the first permutation, below 2, we see 3 and in the second permutation, below 3, we see 5. So, in the product, below 2, we write 5:

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

The remaining entries are found by the same method and we get

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

The product of three or more permutations is evaluated in the same way:

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

We now introduce a more efficient notation for permutations. The permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 6 & 2 & 7 \end{pmatrix}$ in S_7 is a mapping given explicitly as

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

A more compact description of σ can be given as

$$1 \rightarrow 4 \rightarrow 3 \rightarrow 1; \quad 2 \rightarrow 5 \rightarrow 6 \rightarrow 2; \quad 7 \rightarrow 7,$$

or as

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

We drop the arrows and enclose the numbers in a "cycle" within parentheses, in the order indicated by the arrows in a "cycle". Thus we get

$$(143)(256)(7)$$

after juxtaposing the parentheses. The meaning of this symbolism is as follows. Each number a is mapped, under σ , to the number that follows it in the parenthetical expression ("cycle") which contains a . If a happens to be the last entry in a "cycle", then the first number in that "cycle" is considered to follow a . For example,

$$(15234)(6897) \in S_9$$

is the permutation by which 1 is mapped to 5, 5 to 2, 2 to 3, 3 to 4, 4 to 1, 6 to 8, 8 to 9, 9 to 7, 7 to 6. Thus

$$(15234)(6897) = \begin{pmatrix} 1 & 5 & 2 & 3 & 4 & 6 & 8 & 9 & 7 \\ 5 & 2 & 3 & 4 & 1 & 8 & 9 & 7 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 4 & 1 & 2 & 8 & 6 & 9 & 7 \end{pmatrix}.$$

Here (15234) can also be written as (23415) or as (34152), (41523), (52341). Similar remarks are valid for (6897).

An arbitrary permutation $\pi \in S_n$ is written as follows. We open a parenthesis and write down an arbitrary number $a \in \{1, 2, \dots, n\}$. If $a\pi = a$, we close the parenthesis and obtain the expression (a) . If $a\pi = b \neq a$, we write b after a . Now we have (ab) . Here $b\pi \neq b$, because $b\pi \neq a\pi$ (π is one-

to-one). If $b\pi = a$, we close the parenthesis and obtain the expression (ab) . If $b\pi = c \neq b$, we write c after b . Now we have (abc) . Here $c\pi \neq b, c$, because π is one-to-one. We evaluate $c\pi$. If $c\pi = a$, close the parenthesis and obtain the expression (abc) . If $c\pi = d \neq a$, we repeat our procedure, each time writing down the image of a number after that number. Since we have n numbers at our disposal, we meet, after at most n steps, one of the numbers for a second time. If this happens when we have the expression

$$(abc\dots g$$

where a, b, c, \dots, g are all distinct, but $g\pi$ is one of them, we conclude that $g\pi \neq b, c, \dots, g$, since $b = a\pi, c = b\pi, \dots$ and π is one-to-one. Hence $g\pi = a$. We close the parenthesis and obtain the expression $(abc\dots g)$.

If a, b, c, \dots, g exhaust all the numbers $1, 2, \dots, n$, we are done. Otherwise, we select an arbitrary number from $1, 2, \dots, n$ that is distinct from a, b, c, \dots, g . Let us call it h . We open a new parenthesis starting with h and repeat our procedure. After finitely many steps, we get an expression of the form

$$(abc\dots g)(h\dots k)\dots(t\dots x),$$

where $\{a, b, c, \dots, g, h, \dots, k, \dots, t, \dots, x\} = \{1, 2, \dots, n\}$. We call each one of the expressions $(abc\dots g), (h\dots k), \dots, (t\dots x)$ a "cycle".

We will presently give a rigorous definition of a cycle and prove that every permutation can be written as a product of disjoint cycles. But let us consider some examples first.

Let us write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 7 & 1 & 5 & 4 & 9 & 8 & 3 \end{pmatrix}$ in cycle notation. This is done in the following steps, which are carried out mentally at once in practice.

$$\begin{array}{cccc} (1 & (12 & (126 & (1264 \\ (1264) & (1264)(3 & (1264)(37 & \\ (1264)(379) & (1264)(379) & (1264)(379)(5 & \\ (1264)(379)(5) & (1264)(379)(5)(8) & (1264)(379)(5)(8) & \end{array}$$

In this notation, the order of the cycles is not important. We can write the permutation above also as

$$(5)(379)(8)(1264) \text{ or as } (379)(5)(1264)(8).$$

Besides, one can start a cycle with any number in that cycle. Our permutation can thus be written as

$$(5)(793)(8)(6412) \text{ or as } (937)(5)(2641)(8).$$

The identity permutation is given by $(1)(2)(3)\dots(n)$. For obvious reasons, we prefer to write ι instead of $(1)(2)(3)\dots(n)$ for the identity permutation.

The inverse of a permutation is found easily. Let $\sigma \in S_n$, $a, b \in \{1, 2, \dots, n\}$. In the cycles of σ , the number $a\sigma$ follows a . By definition, $b\sigma^{-1}$ is that number a for which $a\sigma = b$. Hence $b\sigma^{-1}$ is the number which is followed by b . Stated otherwise, $b\sigma^{-1}$ is the number that comes just before b in the cycles of σ . So σ^{-1} consists of the same cycles, but the entries being written in the *reverse* order. For example,

$$[(12)(357)(64)]^{-1} = (21)(753)(46), [(326)(15)(4)]^{-1} = (623)(51)(4).$$

Two permutations in S_n , say π and σ , are multiplied as follows. We have $\pi = (\dots a a\pi \dots)$ and $\sigma = (\dots a a\sigma \dots)$. What is $\pi\sigma$? By definition, $\pi\sigma$ is the permutation that maps a to $(a\pi)\sigma$, for all $a \in \{1, 2, \dots, n\}$. To evaluate $(a\pi)\sigma$, we locate a in the cycle of π containing a , then read the number that follows it, which is $a\pi$, and locate this $a\pi$ in the cycle of σ . The number that follows it is $(a\pi)\sigma$. Opening a parenthesis with an arbitrary number a , we find $(a\pi)\sigma = a(\pi\sigma)$ in this way, and write it after a . So we get an expression $(ab \dots)$, say. We find $b(\pi\sigma) = c$. We write $(abc \dots)$. We repeat this process until we get a . Then we close our cycle. At this step, we have $(abc\dots g)$, say. If there are numbers among $1, 2, \dots, n$ not used up in this cycle, we select an arbitrary one of them and obtain a second cycle starting with that number. We continue in this fashion until all the numbers $1, 2, \dots, n$ are used up.

Let us compute the product $(1256)(347).(157)(24)(3)(6)$ in S_7 . We start with the smallest number 1, for example. We write (1 . Now 1 is followed by 2 in the first permutation and 2 is followed by 4 in the second permutation. Thus we get (14 . Now 4 is followed by 7 in the first permutation and 7 is followed by 1 in the second permutation. We close our first cycle. We have (14). We open a new cycle with 2, for example. Now 2 is followed by 5 in the first permutation and 5 is followed by 7 in the second permutation. We have (14)(27 . Continuing

in this way, we find $(1256)(347).(157)(24)(3)(6) = (14)(273)(56)$.

Another example:

$$(152)(3476).(1724)(563) = (1654273).$$

We make a convention. Whenever there appears a cycle consisting of a single number, we suppress it. Hence, whenever a number j does not appear in the cycles of a permutation σ , we understand $j\sigma = j$. With this convention, we write shortly

$$\begin{array}{ll} (123)(47) & \text{for } (123)(47)(5)(6) \text{ in } S_7, \\ (245)(3876) & \text{for } (245)(3876)(1) \text{ in } S_8. \end{array}$$

This convention simplifies multiplication: if a number does not appear in the cycles of one or more of the factors, it is mapped to itself by the permutations in question. For example,

$$\begin{array}{ll} (123).(12) & = (23) \\ (254).(12)(34) & = (25341). \end{array}$$

The way we multiply permutations, either in double row or in cycle notation, reflects the fact that we write functions to the right of the elements. If we had written functions on the left, then $\pi\sigma$ would mean: first σ , then π . A product would be evaluated in double row notation by reading the permutations from right to left. In the cycle notation, we would be reading the cycles from right to left, but the numbers in the cycles from left to right. Writing our functions on the right, we avoid backward or inconsistent reading. We read everything in the correct order.

The alert reader will have noticed that the same symbol in cycle notation stands for many different permutations. Thus $(123)(45)$ stands for $(123)(45)$ in S_5 , for $(123)(45)(6)$ in S_6 , for $(123)(45)(6)(7)$ in S_7 , etc. So an isolated symbol $(123)(45)$ is ambiguous. Also, our thumb rule for finding inverses in the cycle notation works only when the cycles are disjoint. It is time that we discuss these points rigorously.

15.3 Definition: Let $\sigma \in S_n$ and $m \in \{1, 2, \dots, n\}$. When $m\sigma = m$, we say that m is fixed by σ or that σ fixes m . When $m\sigma \neq m$, then m is said to be moved by σ or σ is said to move m .

15.4 Definition: Let $\pi, \sigma \in S_n$. If the set of numbers moved by π and the set of numbers moved by σ are disjoint, then π and σ are called *disjoint permutations*. We also say π is *disjoint from* σ in this case.

15.5 Lemma: Let $\alpha, \beta \in S_n$ and $k \in \{1, 2, \dots, n\}$. Assume α, β are disjoint.

(1) If k is moved by α , then $k\alpha$ is also moved by α .

(2) If k is moved by α and fixed by β , then $k\alpha$ is fixed by β .

Proof: (1) If k were fixed by α , so that $(k\alpha)\alpha = k\alpha$, we would apply α^{-1} to both sides of this equation and get $k\alpha = (k\alpha)\alpha\alpha^{-1} = k\alpha\alpha^{-1} = k$, contrary to the hypothesis that k is moved by α . So $k\alpha$ is moved by α .

(2) $k\alpha$ is moved by α according to part (1). If $k\alpha$ were moved by β , then $k\alpha$ would be moved both by α and by β , contrary to the hypothesis that α and β are disjoint permutations. Thus $k\alpha$ is fixed by β . \square

We can now prove that disjoint permutations always commute.

15.6 Theorem: If $\sigma, \tau \in S_n$ are disjoint permutations, then $\sigma\tau = \tau\sigma$.

Proof: We must show $m(\sigma\tau) = m(\tau\sigma)$ for all $m \in \{1, 2, \dots, n\}$. Since σ and τ are disjoint, for each $m \in \{1, 2, \dots, n\}$, there are three possibilities:

I. m is moved by σ , fixed by τ .

II. m is fixed by σ , moved by τ .

III. m is fixed by σ , fixed by τ .

In case I, $m\sigma$ fixed by τ by Lemma 15.5(2) (with m, σ, τ in place of k, α, β), hence $(m\sigma)\tau = m\sigma$ and

$$\begin{aligned} m(\sigma\tau) &= (m\sigma)\tau = m\sigma, \\ m(\tau\sigma) &= (m\tau)\sigma = m\sigma \quad (\text{as } m \text{ is fixed by } \tau), \end{aligned}$$

so $m(\sigma\tau) = m(\tau\sigma)$.

In case II, $m\tau$ fixed by σ by Lemma 15.5(2) (with m, τ, σ in place of k, α, β), hence $(m\tau)\sigma = m\tau$ and

$$\begin{aligned} m(\sigma\tau) &= (m\sigma)\tau = m\tau \quad (\text{as } m \text{ is fixed by } \sigma), \\ m(\tau\sigma) &= (m\tau)\sigma = m\tau, \end{aligned}$$

so $m(\sigma\tau) = m(\tau\sigma)$.

In case III, we have

$$\begin{aligned} m(\sigma\tau) &= (m\sigma)\tau = m\tau = m, \\ m(\tau\sigma) &= (m\tau)\sigma = m\sigma = m, \end{aligned}$$

so $m(\sigma\tau) = m(\tau\sigma)$.

In all three cases, we have $m(\sigma\tau) = m(\tau\sigma)$. Since this holds for all m in the set $\{1, 2, \dots, n\}$, we conclude $\sigma\tau = \tau\sigma$. \square

In order to prepare our way for a formal definition of cycle, let us examine the permutation

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

in S_{10} . Informally, we write this as $(1432)(567)(8)(9,10)$ and call (1432) , (567) , (8) , $(9,10)$ "cycles" (we use a comma to avoid confusion when we have a number with more than one digits). The idea is to consider (1432) etc. as a permutation by itself. Then

$$(1432)(567)(8)(9,10)$$

is a product of four permutations. We observe that $\{1432\}$, $\{567\}$, $\{8\}$, $\{9,10\}$ are pairwise disjoint subsets of $\{1,2,3,4,5,6,7,8,9,10\}$ and yield a partition of $\{1,2,3,4,5,6,7,8,9,10\}$. So there is an equivalence relation on $\{1,2,3,4,5,6,7,8,9,10\}$ with these subsets as equivalence classes (Theorem 2.5). We want to find this equivalence relation.

15.7 Lemma: *Let π be a permutation in S_n . We put, for $a, b \in \{1, 2, \dots, n\}$,*

$$a \mathfrak{T} b$$

if and only if there is an integer $k \in \mathbb{Z}$ such that $a\pi^k = b$. Then \mathfrak{T} is an equivalence relation on $\{1, 2, \dots, n\}$.

Proof: (i) For all $a \in \{1, 2, \dots, n\}$, we have $a\pi^0 = a$, with $0 \in \mathbb{Z}$. So $a \mathfrak{T} a$ for all a and \mathfrak{T} is reflexive.

(ii) If $a \mathfrak{T} b$, then $a\pi^k = b$ for some $k \in \mathbb{Z}$, so $b\pi^{-k} = a$ with $-k \in \mathbb{Z}$ and therefore $b \mathfrak{T} a$. So \mathfrak{T} is symmetric.

(iii) If $a \mathfrak{T} b$ and $b \mathfrak{T} c$, then $a\pi^k = b$ and $b\pi^m = c$ for some $k, m \in \mathbb{Z}$, then $a\pi^{k+m} = a\pi^k\pi^m = b\pi^m = c$, with $k + m \in \mathbb{Z}$ and therefore $a \mathfrak{T} c$. So \mathfrak{T} is transitive. \square

The reader will check easily that $\{1432\}$, $\{567\}$, $\{8\}$, $\{9,10\}$ are the equivalence classes of \mathfrak{T} in $\{1,2,3,4,5,6,7,8,9,10\}$ if π denotes the permutation

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

we treated above. So the equivalence relation of Lemma 15.7 seems promising.

15.8 Lemma: *Let $\pi \in S_n$ and let $A \subseteq \{1,2, \dots, n\}$ be an equivalence class under the equivalence relation of Lemma 15.7. We define π_A by*

$$b\pi_A = \begin{cases} b\pi & \text{if } b \in A \\ b & \text{if } b \notin A \end{cases}$$

for $b \in \{1,2, \dots, n\}$. Then π_A is a permutation in S_n and, whenever x and y are moved by π_A , there is an integer k such that $x\pi_A^k = y$.

Proof: By definition of \mathfrak{T} , there holds $x \mathfrak{T} x\pi$ for all $x \in \{1,2, \dots, n\}$ and $x\pi$ belongs to the equivalence class of x . So the equivalence class of x and the equivalence class of $x\pi$ are identical. Hence $x\pi \in A$ if and only if $x \in A$.

Using this remark, we prove, for any $n \in \mathbb{N}$, that $x\pi^n = x\pi_A^n$ for all $x \in A$. This is true when $n = 1$. If it is true for $n = k - 1$, we have, for any $x \in A$,

$$\begin{aligned} x\pi_A^k &= (x\pi_A)\pi_A^{k-1} \\ &= (x\pi)\pi_A^{k-1} \\ &= (x\pi)\pi^{k-1} \\ &= x\pi^k, \end{aligned}$$

and it is true for $n = k$. Thus it is true for all $n \in \mathbb{N}$.

In particular, it is true for $m = o(\pi)$ and

$$x\pi_A^m = \begin{cases} x\pi^m & \text{if } x \in A \\ x & \text{if } x \notin A \end{cases} = x,$$

hence $\pi_A^{m-1}\pi_A = \iota = \pi_A\pi_A^{m-1}$. By Theorem 3.17(2), π_A is one-to-one and onto. Thus $\pi_A \in S_n$.

Finally, if x and y are moved by π_A , then necessarily $x, y \in A$ in view of the definition of π_A , so there is an integer $k \in \mathbb{Z}$ with $x\pi^k = y$ and thus $x(\pi_A)^k = y$ by what we proved above (since $x \in A$). This completes the proof. \square

15.9 Theorem: Let $\pi \in S_n$ and let A_1, A_2, \dots, A_h be the equivalence classes of $\{1, 2, \dots, n\}$ under the equivalence relation \mathfrak{K} in Lemma 15.7.

Let

$\pi_{A_1}, \pi_{A_2}, \dots, \pi_{A_h}$ be the associated permutations as in Lemma 15.8.

(1) $\pi_{A_1}, \pi_{A_2}, \dots, \pi_{A_h}$ are pairwise commuting permutations in S_n .

(2) $\pi = \pi_{A_1}\pi_{A_2}\cdots\pi_{A_h}$.

Proof: (1) The equivalence classes A_1, A_2, \dots, A_h are pairwise disjoint sets. Now π_{A_i} either moves no number at all (this happens if and only if A_i has exactly one element), or moves only the numbers in A_i . Therefore, the numbers moved by π_{A_i} and π_{A_j} make up disjoint sets whenever $i \neq j$. So the permutations $\pi_{A_1}, \pi_{A_2}, \dots, \pi_{A_h}$ are pairwise disjoint permutations (Definition 15.4) and they commute by Theorem 15.6.

(2) We have $\pi_{A_1}\pi_{A_2}\cdots\pi_{A_h} = \pi_{A_{1'}}\pi_{A_{2'}}\cdots\pi_{A_{h'}}$ for any arrangement $1', 2', \dots, h'$ of the numbers $1, 2, \dots, h$. (Lemma 8.12). We want to show

$b\pi = b\pi_{A_1}\pi_{A_2}\cdots\pi_{A_h}$ for all $b \in \{1, 2, \dots, n\} = A_1 \cup A_2 \cup \dots \cup A_h$. So let b be in $\{1, 2, \dots, n\}$. Renumbering A_1, A_2, \dots, A_h if need be, we may assume, without loss of generality that $b \in A_h$. Then $b \notin A_1, b \notin A_2, \dots, b \notin A_{h-1}$ and thus $b\pi_{A_1} = b\pi_{A_2} = \dots = b\pi_{A_{h-1}} = b$ by the definition of these functions. Thus $b\pi_{A_1}\pi_{A_2}\cdots\pi_{A_h} = b_{A_h}$ and the proof will be complete when we show $b\pi = b_{A_h}$. But this follows immediately from the definition of π_{A_h} since $b \in A_h$. \square

In our example, the associated permutations are

$$(1432)(5)(6)(7)(8)(9)(10) = (1432)$$

$$\begin{aligned}
(567)(1)(2)(3)(4)(8)(9)(10) &= (567) \\
(8)(1)(2)(3)(4)(5)(6)(7)(9)(10) &= (8) (= \iota) \\
(9,10)(1)(2)(3)(4)(5)(6)(7)(8) &= (9,10).
\end{aligned}$$

In view of this, we define cycles as the associated permutations. Cycles will be distinguished from other permutations by the property stated in Lemma 15.8.

15.10 Definition: A permutation $\pi \in S_n$ is called a *cycle* if, for all x, y in $\{1, 2, \dots, n\}$ that are moved by π , there is an integer k such that $x\pi^k = y$.

The identity permutation is vacuously a cycle. Lemma 15.8 states that π_A is a cycle when A is an equivalence class under the equivalence relation in Lemma 15.7. Since the cycles are disjoint, we may reformulate Theorem 15.9 as follows.

15.9 Theorem: *Every permutation π in S_n can be written as a product of disjoint cycles. These cycles are completely determined by π , and they commute in pairs.* □

Let σ be a cycle in S_n distinct from ι . Let a_1, a_2, \dots, a_m be the numbers moved by σ . Since σ is one-to-one, $a_1\sigma, a_2\sigma, \dots, a_m\sigma$ are all distinct and we may assume the numbering so chosen that

$$a_1\sigma = a_2, a_2\sigma = a_3, \dots, a_{m-1}\sigma = a_m, a_m\sigma = a_1.$$

In this case, we write $(a_1 a_2 \dots a_m)$ for σ . Then m is called the *length* of the cycle $(a_1 a_2 \dots a_m)$ and $(a_1 a_2 \dots a_m) = \sigma$ is called an *m-cycle*. The identity permutation is called a *1-cycle*.

With this notation, we have

$$a_1\sigma = a_2 \neq a_1, a_1\sigma^2 = a_3 \neq a_1, \dots, a_1\sigma^{m-1} = a_m \neq a_1$$

and so $\sigma \neq \iota, \sigma^2 \neq \iota, \dots, \sigma^{m-1} \neq \iota$. On the other hand,

$$a_1\sigma^m = a_1 \quad \text{and} \quad a_k\sigma^m = a_1\sigma^{k-1}\sigma^m = a_1\sigma^m\sigma^{k-1} = a_1\sigma^{k-1} = a_k$$

for all $k = 1, 2, \dots, n$. So σ^m fixes a_1, a_2, \dots, a_m . But σ fixes the numbers among $1, 2, \dots, n$ which are distinct from a_1, a_2, \dots, a_m , and then σ^m fixes

them, too. Hence $b\sigma^m = b$ for all $b \in \{1, 2, \dots, n\}$. Thus m is the smallest natural number such that $\sigma^m = \iota$. Using Lemma 11.4, we obtain the following Theorem, which is also true when $m = 1$.

15.11 Theorem: *The order of a cycle is its length. In other words, if $\sigma = (a_1 a_2 \dots a_m)$, then $o(\sigma) = m$.* \square

15.12 Remarks: (1) The inverse of a cycle $\sigma = (a_1 a_2 \dots a_m) \in S_n$, for which

$a_1\sigma = a_2, a_2\sigma = a_3, \dots, a_{m-1}\sigma = a_m, a_m\sigma = a_1$ and which fixes any other number in $\{1, 2, \dots, n\}$ (if any) is by definition the mapping π whose effect on a_1, a_2, \dots, a_m is given by $a_m\pi = a_{m-1}, \dots, a_3\pi = a_2, a_2\pi = a_1, a_1\pi = a_m$ and which fixes the other numbers (if any). Thus $\sigma^{-1} = \pi$ is the cycle

$$(a_m a_{m-1} \dots a_2 a_1).$$

(2) Let $\pi \in S_n$ be written as $\pi = \pi_{A_1} \pi_{A_2} \dots \pi_{A_h}$ with the notation of Theorem 15.9. A cycle π_{A_i} is the identity if there is only one number in A_i . Then the cycle π_{A_i} may be deleted from the product.

(3) If $\pi = \pi_{A_1} \pi_{A_2} \dots \pi_{A_h}$ is the representation of π as a product of disjoint cycles, then $\pi = \pi_{A_h} \dots \pi_{A_2} \pi_{A_1}$ and so $\pi^{-1} = \pi_{A_1}^{-1} \pi_{A_2}^{-1} \dots \pi_{A_h}^{-1}$. But this is true only when A_i are disjoint. In any case, it is safer to reverse the order of the cycles as well as the ordering of the numbers in each cycle when we want to find the inverse of a product of cycles, as this is valid also in the case the cycles are not pairwise disjoint and is a more consistent procedure: you reverse everything. For example,

$$[(15)(243)(687)]^{-1} = (786)(342)(51).$$

(4) The ambiguity in cycle notation is harmless, as it will be either clear from the context which symmetric group we are working in, or the results will be independent of the symmetric group.

In the rest of this paragraph, we determine the order of a permutation written as a product of disjoint cycles. We start with a general lemma.

15.13 Lemma: *Let G be a group and $a, b \in G$. Suppose $ab = ba$ and assume that $o(a)$ and $o(b)$ are finite. Suppose further that $\langle a \rangle \cap \langle b \rangle = \{1\}$. Then $o(ab)$ is finite. In fact, $o(ab)$ is the least common multiple of $o(a)$ and $o(b)$: we have $o(ab) = [o(a), o(b)]$.*

Proof: First we show that $(ab)^k = 1$ if and only if $o(a)|k$ and $o(b)|k$ (where $k \in \mathbb{Z}$). Indeed, if $o(a)|k$ and $o(b)|k$, then $a^k = 1$ and $b^k = 1$ (Lemma 11.6) and so $(ab)^k = a^k b^k = 1 \cdot 1 = 1$ (Lemma 8.14(3); here we use $ab = ba$). Conversely, if $(ab)^k = 1$, then $a^k b^k = 1$, so $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = \{1\}$. So we have $a^k = 1 = b^{-k}$, and $a^k = 1 = b^k$, and thus $o(a)|k$ and $o(b)|k$. Therefore $(ab)^k = 1$ if and only if $o(a)|k$ and $o(b)|k$.

Then, by Lemma 11.4,

$$\begin{aligned}
 o(ab) &= \text{smallest number in } \{k \in \mathbb{N} : (ab)^k = 1\}, \\
 &\quad \text{provided this set is not empty,} \\
 &= \text{smallest number in } \{k \in \mathbb{N} : o(a)|k \text{ and } o(b)|k\}, \\
 &\quad \text{provided this set is not empty,} \\
 &= \text{the least common multiple of } o(a) \text{ and } o(b), \text{ as} \\
 &\quad \text{the set is not empty,} \\
 &= [o(a), o(b)] \quad \square
 \end{aligned}$$

Generally speaking, we cannot determine the order of a and b from $o(a)$ and $o(b)$ alone. $o(ab)$ depends also on the role the elements a, b play in the group. (See §14, Ex.15.) Lemma 15.13 is one of the rare situations where $o(ab)$ is determined in terms of $o(a)$ and $o(b)$.

Lemma 15.13 will be used to find the order of a product of disjoint permutations. We need the following result.

15.14 Lemma: (1) *If σ_1 and τ , as well as σ_2 and τ are disjoint permutations in S_n , then $\sigma_1\sigma_2$ and τ are disjoint.*

(2) *If $\sigma_1, \sigma_2, \dots, \sigma_m$ are disjoint from τ , then $\sigma_1\sigma_2 \dots \sigma_m$ and τ are disjoint.*

(3) If σ and τ are disjoint, then σ^{-1} and τ are disjoint.

(4) If σ and τ are disjoint, then σ^m and τ are disjoint for all $m \in \mathbb{Z}$.

(5) If σ and τ are disjoint, then σ^m and τ^r are disjoint for all $m, r \in \mathbb{Z}$.

Proof: (1) By hypothesis, any $k \in \{1, 2, \dots, n\}$ that is moved by τ is fixed by σ_1 and σ_2 . So $k\tau \neq k$ implies $k\sigma_1 = k$ and $k\sigma_2 = k$. So $k\tau \neq k$ implies $k(\sigma_1\sigma_2) = (k\sigma_1)\sigma_2 = k\sigma_2 = k$ and $\sigma_1\sigma_2$ fixes every number that τ moves. Hence $\sigma_1\sigma_2$ and τ are disjoint. (The argument is valid also when $\tau = \iota$.)

(2) This follows from (1) by induction on m . The details are left to the reader.

(3) Let $k \in \{1, 2, \dots, n\}$ be moved by τ . We wish to show that k is fixed by σ^{-1} . Since σ and τ are disjoint, k is fixed by σ . So $k\sigma = k$. Applying σ^{-1} to both sides, we get $(k\sigma)\sigma^{-1} = k\sigma^{-1}$, hence $k = k\sigma^{-1}$ and k is fixed by σ^{-1} . Therefore σ^{-1} and τ are disjoint.

(4) Let $m \in \mathbb{N}$. Choosing $\sigma_1, \sigma_2, \dots, \sigma_m$ all equal to σ in (2), we deduce that σ^m and τ are disjoint. Now applying (3) with σ^m, τ in place of σ, τ , we get that $\sigma^{-m} = (\sigma^m)^{-1}$ is disjoint from τ , for any $m \in \mathbb{N}$. As $\tau^0 = \iota$ is trivially disjoint from τ , we conclude that σ^m and τ are disjoint for all $m \in \mathbb{Z}$.

(5) When σ and τ are disjoint and $m, r \in \mathbb{Z}$, then σ^m and τ are disjoint by (4), and using (4) with r, τ, σ^m respectively in place of m, σ, τ , we deduce that τ^r and σ^m are disjoint. Hence σ^m and τ^r are disjoint for all $m, r \in \mathbb{Z}$. \square

15.15 Theorem: Let σ and τ be disjoint permutations in S_n . Then

$$o(\sigma\tau) = [o(\sigma), o(\tau)].$$

Proof: We use Lemma 15.13. Since σ and τ are disjoint, $\sigma\tau = \tau\sigma$ by Theorem 15.6. Also, $o(\sigma)$ and $o(\tau)$ are finite since S_n is a finite group by Theorem 15.2. We must also show that $\langle\sigma\rangle \cap \langle\tau\rangle = \{\iota\}$. When we do this, the hypotheses of Lemma 15.13 will be satisfied and it will yield $o(\sigma\tau) = [o(\sigma), o(\tau)]$. So we show $\langle\sigma\rangle \cap \langle\tau\rangle \leq \{\iota\}$.

Suppose $\langle\sigma\rangle \cap \langle\tau\rangle \not\leq \{\iota\}$. Then there is an $\alpha \in \langle\sigma\rangle \cap \langle\tau\rangle$ with $\alpha \neq \iota$ and $\alpha = \sigma^m = \tau^r$ for some integers m, r . Since $\alpha \neq \iota$, there is a $j \in \{1, 2, \dots, n\}$ such that $j\alpha \neq j$. So j is moved by σ^m and also by τ^r . On the other hand, σ^m and

τ^r are disjoint by Lemma 15.14(5) and there cannot be any number in $\{1, 2, \dots, n\}$ which is moved both by σ^m and by τ^r . This is a contradiction. Thus $\langle \sigma \rangle \cap \langle \tau \rangle \leq \{1\}$. As remarked above, this completes the proof. \square

15.16 Theorem: Let $\sigma_1, \sigma_2, \dots, \sigma_m$ be pairwise disjoint permutations in S_n . Then $o(\sigma_1 \sigma_2 \dots \sigma_m) = [o(\sigma_1), o(\sigma_2), \dots, o(\sigma_m)]$.

Proof: By induction on m . The case $m = 2$ is treated in Theorem 15.15. The inductive step is left to the reader. \square

15.17 Theorem: The order of $\sigma \in S_n$ is the least common multiple of the lengths of the disjoint cycles in the representation of σ as a product of disjoint cycles.

Proof: The disjoint cycles are pairwise disjoint and the order of a cycle is its length (Theorem 15.11). The claim follows now immediately from Theorem 15.16.

\square

For instance. $(134)(275698)$ has order 6, $(124)(3756)$ has order 12 and $(34)(79)(12586)$ has order 10.

Exercises

- Evaluate $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.
- Evaluate $(1253)(24315)$, $(1542)(376)(1754)$ and $(1243)(345)(265)(1452)(135)^{-1}(3246)$.

3. Write the permutations in Ex. 1 in cycle notation. Carry out the multiplication in cycle notation and compare the results.
4. Write the permutations in Ex. 2 in double row notation. Carry out the multiplication in double row notation and compare the results.
5. Write all elements in S_1, S_2, S_3, S_4 .
6. Construct multiplication tables of S_1, S_2, S_3, S_4 .
7. Find the orders of all elements in S_3 and S_4 .
8. Show that $V_4 := \{ \iota, (12)(34), (13)(24), (14)(23) \}$ is a subgroup of S_4 .
9. Show that $D := \{ \iota, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432) \}$ is a subgroup of S_4 . Prove that it is a dihedral group in the sense of Definition 14.7.
10. Find all subgroups of S_3 and S_4 .
11. Let $H \leq S_n$. For $a, b \in G$, put $a \stackrel{H}{\sim} b$ if and only if there is a $\sigma \in H$ such that $a\sigma = b$. Show that $\stackrel{H}{\sim}$ is an equivalence relation on $\{1, 2, \dots, n\}$. (Lemma 15.7 is a special case when $H = \langle \pi \rangle$.)
12. Let a_1, a_2, \dots, a_m be pairwise commuting elements of finite order in a group G such that $\langle a_i \rangle \cap \langle a_j \rangle = \{1\}$ whenever $i \neq j$. Show that $o(a_1 a_2 \dots a_m) = [o(a_1), o(a_2), \dots, o(a_m)]$. This gives an alternative proof of Theorem 15.16.
13. For $\sigma \in S_4$, we put $\sigma V_4 := \{ \sigma\pi : \pi \in V_4 \}$ and $V_4 \sigma := \{ \pi\sigma : \pi \in V_4 \}$ (Ex. 8). Find σV_4 and $V_4 \sigma$ when $\sigma = \iota$, $\sigma = (12)$, $\sigma = (123)$, $\sigma = (12)(34)$, $\sigma = (1234)$.
14. For $H \subseteq S_4$, $\sigma \in S_4$, we put $\sigma H := \{ \sigma\pi : \pi \in H \}$ and $H\sigma := \{ \pi\sigma : \pi \in H \}$. Thus σH and $H\sigma$ are subsets of S_4 .
 Let $H_1 = \{ \iota, (13), (24), (12)(34) \}$. Check whether $(12)H_1 = H_1(12)$, $(13)H_1 = H_1(13)$, $(123)H_1 = H_1(123)$, $(12)(34)H_1 = H_1(12)(34)$, $(1234)H_1 = H_1(1234)$.
 Let $H_2 = \{ \iota, (12), (34), (12)(34) \}$. Check whether $(12)H_2 = H_2(12)$, $(13)H_2 = H_2(13)$, $(123)H_2 = H_2(123)$, $(12)(34)H_2 = H_2(12)(34)$, $(1234)H_2 = H_2(1234)$.
 Compare to Ex. 13.

15. Show that, for any $\sigma \in S_n$, there holds $\sigma^{-1}(123)\sigma = (abc)$ with suitable a, b, c . How are a, b, c related to σ ? (Work out some specific examples.) Generalize your conclusion to $\sigma^{-1}\pi\sigma$.