Section 6.3 Groups of Permutations: The Symmetric Group

Purpose of Section: To introduce the idea of a permutation and show how the set of all permutations of a set of n elements, equipped with the composition of permutations as an operation, form a group, called the **symmetric group** S_n on n elements.

Permutations and Their Products

In Section 2.3 we introduced the concept of a permutation (or arrangement) of a set of objects. We now return to the subject, but now the focus is different, instead of thinking of a permutation as an arrangement of objects (which it is of course), we think of a permutation as a one-to-one function (bijection) from a set onto itself. For example, a permutation of elements of the set $A = \{1,2,3,...,n\}$ is thought of a one-to-one mapping of this set onto itself, which we represent by

$$P = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ 1^P & 2^P & \cdots & k^P & \cdots & n^P \end{pmatrix}$$

which gives the image k^p of each element $k \in A$ in the first row as the element directly below in the second row.

A good way to think about permutations is the following. Consider the set of four elements $A = \{1,2,3,4\}$ whose elements we permute with the permutation

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

Carrying out the "shuffles" described by P, what will be the new arrangement of the numbers $\{1,2,3,4\}$? Many beginning students do not interpret this permutation correctly, so we give you a simple explanation. A good way to think about this permutation is to think of four boxes labeled "1". "2", "3", and "4" where *initially* inside each box contains a marble labeled with the same number; that is, box 1 contains a ball labeled 1, box 2 contains a marble labeled 2, and so on. The permutation P "shuffles" the marbles as shown in Figure 1. That is, the marble in box 1 moves to box 2, the marble in box 2 moves to box 3, the marble in box 3 moves to box 4, and the marble in box 4 moves to box 1. The boxes stay fixed, the marbles inside the boxes move according to the permutation, the net result being the permutation moves members of A according to

$$P:(1,2,3,4)\rightarrow(4,1,2,3)$$

not $(2,3,4,1)$.

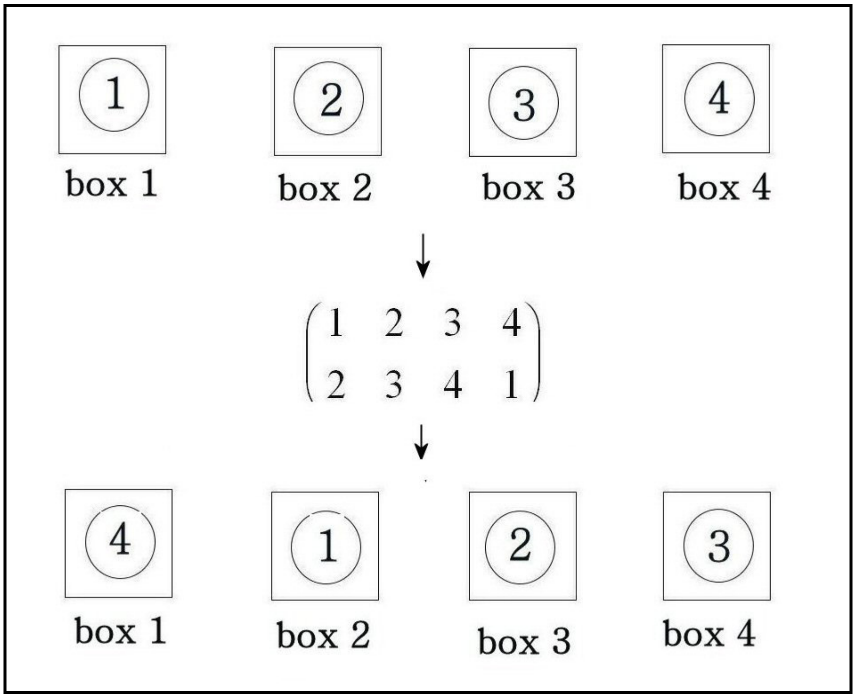
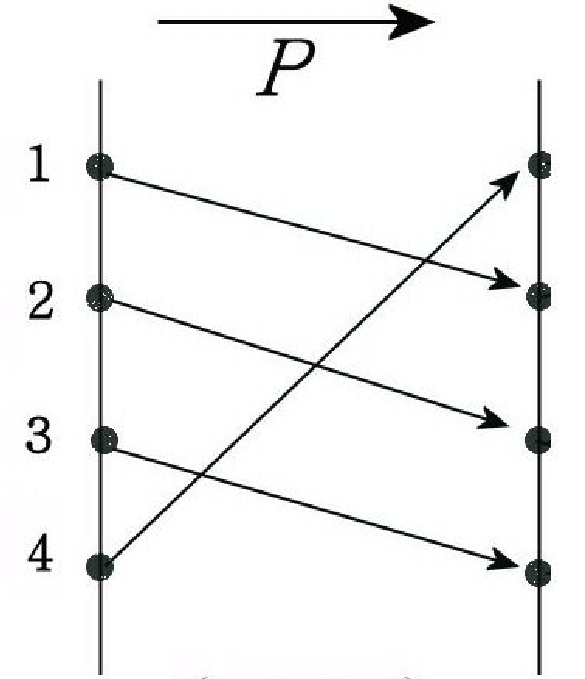


Illustration of a Permutation Function
Figure 1

Another way to interpret this permutation is with a directed graph as drawn in Figure 2. Four people are standing, say from top to bottom, on four stair steps of a stairs, where the permutation results in a "rotational" movement, the top three people moving down one step, and the person at the bottom moving all the way to the top step.



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

Visualization of a Permutation
Figure 2

Product of Permutations We now introduce a second permutation

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

and carry out permutation P followed by permutation Q. In other words, the composition of two functions; permutation P followed by permutation Q, which gives a "reshuffling of a reshuffling" which defines the product of two permutations.

Definition: The composition of two permutations of a set, P followed by Q is defined as the (permutation) **product** of P **and** Q, denoted[1] by PQ.

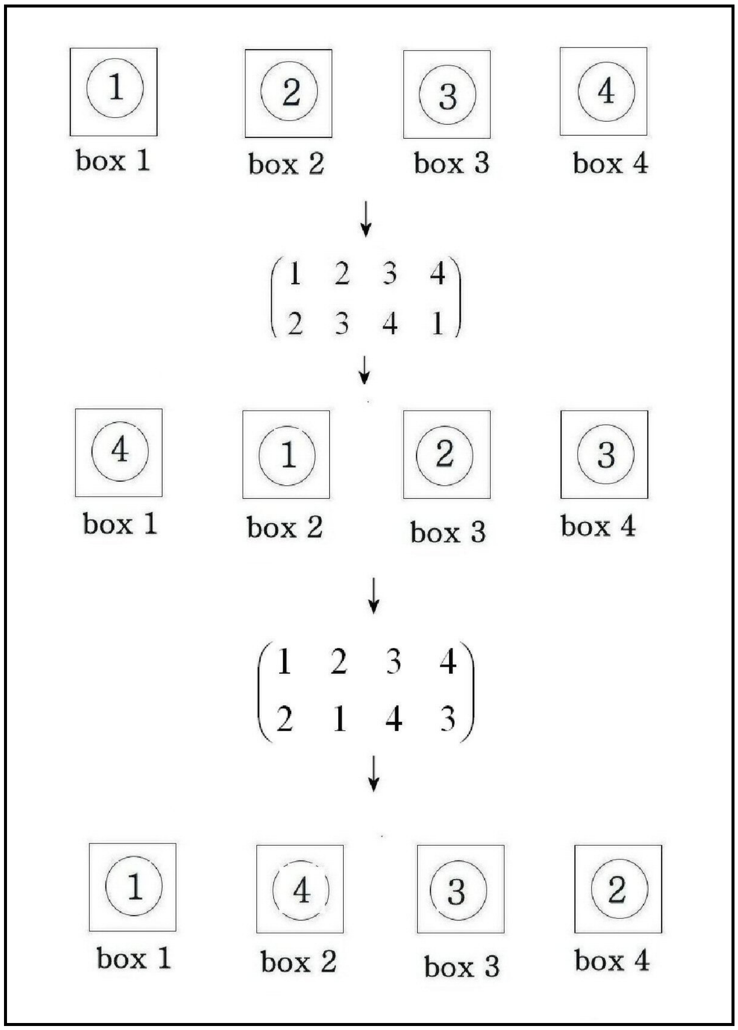
In this example, the product of the compositions is

---

[1] In compositions of functions $(f \circ g)(x) = f\left[g(x)\right]$ we evaluate from "right to left", evaluating the function g first and f second. Here, in the case of permutation functions, we have decided to evaluate from "left to right" to keep things in the spirit of "products" of members of a group which one generally things of "multiplying from left to right.

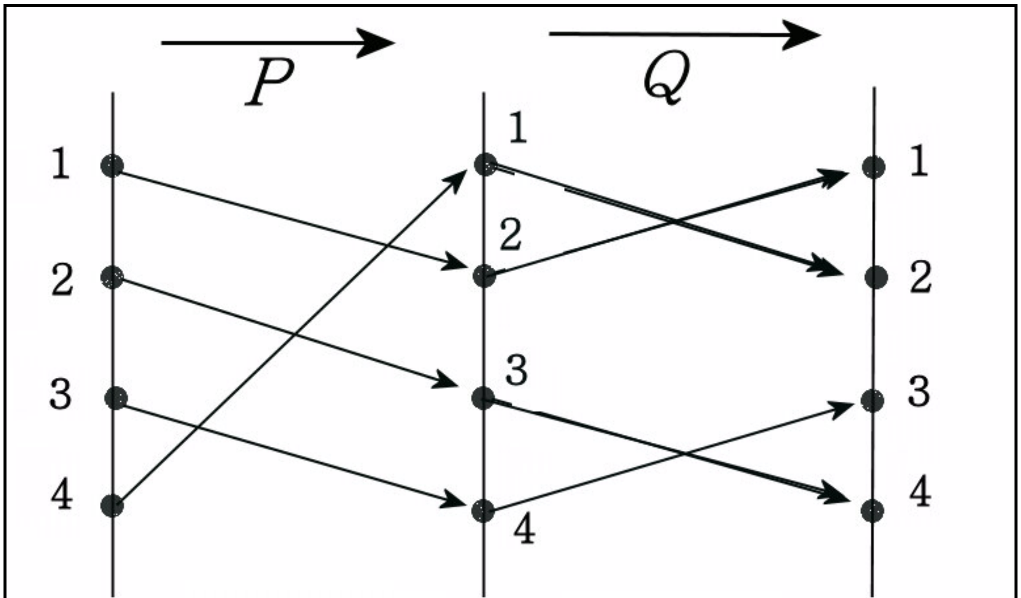
$$PQ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

So now, how do the four marbles in the four boxes end up after two shuffles? Figure 3 illustrates the movement of the marbles in the boxes.



Product (composition) of Two Permutations
Figure 3

A second visualization of this product is shown in Figure 4. The four marbles end up in order 1,4,3,2. (Don't confuse boxes with marbles, the marbles move, the boxes stay fixed. The numbers in the permutations refer to the boxes, not the marbles.



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

Another Representation of the Product of Permutations
Figure 4

Example 1 Find the product PQ where

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \ Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Solution: Figure 5 illustrates this product. Note $P: 1 \to 4$ followed by $Q: 4 \to 3$, the net result being $PQ: 1 \to 3$. In other words, we have

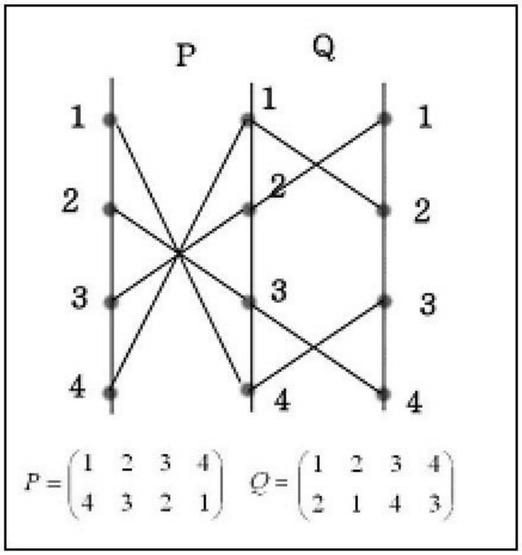
$$PQ(1) = 3, \ PQ(2) = 4, \ PQ(3) = 1, \ PQ(4) = 2$$

or

$$PQ = \overset{P}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}} \overset{Q}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Product of Permutations
Figure 5

The graph illustration of the product is shown in Figure 6.



Composition of Two Permutations
Figure 6

Inverses of Permutations

If a permutation P maps k into k^P, then the **inverse permutation** P^{-1} maps k^P back into k. In other words, the inverse of a permutation can be found by simply interchanging the top and bottom rows of the permutation P and (for convenience in reading) reordering the top row in numerical order $1,2, \cdots n$. For example

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \Rightarrow Q^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$
$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \Rightarrow P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

The reader can verify that

$$PP^{-1} = QQ^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Cycle Notation for Permutations

A more streamlined way to display permutations is by the use of **cycle** (or **cyclic**) notation. To illustrate how this works, consider the permutation[2]

[2] Sometimes only the bottom row of the permutation is given since the first row is ambiguous. Hence, the permutation listed here could be expressed as {325614}.

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

To write this permutation in cyclic notation, we start at the upper left-hand corner with 1 and write $(1$ and then follow it with its image $1^P = 3$, that is $(13$. Next, note that P maps 3 into 5, so we write $(135$. Then P maps 5 back into the original 1 so we have our first cycle (135). We then continue on with 2 (next unused element in the first row) and observe that P maps 2 into itself so we have a 1-cycle (2). Finally, we see that P maps 4 into 6 so we write $(46$ and since 6 maps back into 4 we have our final cycle, the 2-cycle (46). Hence P is written in what is called the **product** of three cycles; a 3-cycle, a 1-cycle, and a 2-cycle,

$$P = (135)(2)(46) = (135)(46)$$

where we dropped the 1-cycle (2), which is often done in order to streamline the notation.

Let's now see if we can go backwards from cycle notation to recover the original form of the permutation. For example, consider

$$(14)(23) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

We start with the left-most cycle, where we see that 1 maps into 4 and 4 maps back into 1. This will fill in two columns of P. If the first cycle does not exhaust the elements of the set, where in this example we still have the cycle (23), we continue the same process and then continue until all cycles have been used. This process will reconstruct the permutation P from its cycle notation, except we must know if any 1-cycles were dropped in the cycle notation.

Margin Note If you wanted to dial the telephone number 413-2567 but accidentally dialed 314-5267, then you permuted the digits according to $(25)(34)$.

Example 2

The following permutations are displayed both in function and cycle notation. Make sure you can go "both ways" in these equations.

$$a)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 6 & 1 \end{pmatrix} = (12456)(3)$$

$$b)\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

$$c)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = (1)(2)(345) = (345)$$

$$d)\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

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

Note the identity permutation in Example $1\,e)$ is sometimes written $(\ )$.

Margin Note: The cycle notation was introduced by the French mathematician Cauchy in 1815. The notation has the advantage that many properties of permutations can be seen from an glance.

Example 3 (Product of Permutations in Cycle Form)

Find the product PQ if $P = (125)(34)$ $\quad Q = (13)(45)$.

Solution

Applying (in succession) the permutation P first, then Q second, we see that 1 gets mapped into 2 by P, then into itself by Q, and hence the composition maps 1 into 2. Next, the number 2 gets mapped into 5 by P and then into 4 by Q, and so the composition maps 2 into 4, and so on. Carrying out this process, we arrive at the composition in cycle form

$$PQ = (124)(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \qquad \blacksquare$$

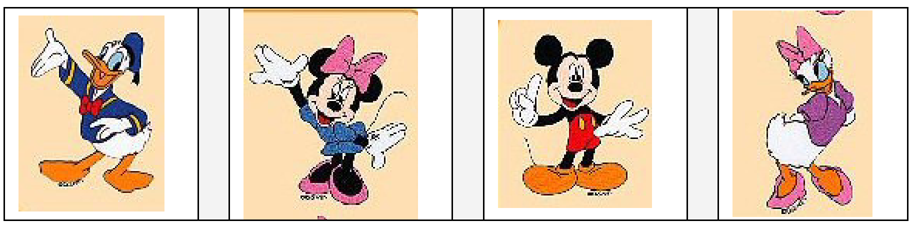
Transpositions

A permutation that interchanges two elements of a set and leaves all others unchanged is called a **transposition.** For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4)$$

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

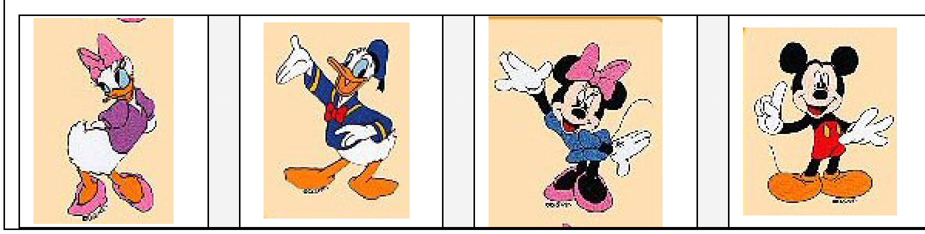
are all transpositions. What may not be obvious is that any permutation is the product of transpositions. In other words, any permutation of elements of a set can be carried out by repeated interchanges of two elements. For example, Figure 7 shows Donald Duck, Minnie Mouse, Mickey Mouse, and Daisy Duck lined up from left to right waiting to get their picture taken. The photographer asks the three on the left to move one place to their right, and Daisy Duck to move to the left position, which is a result of the following permutation.



$$\downarrow$$

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$$

$$\downarrow$$

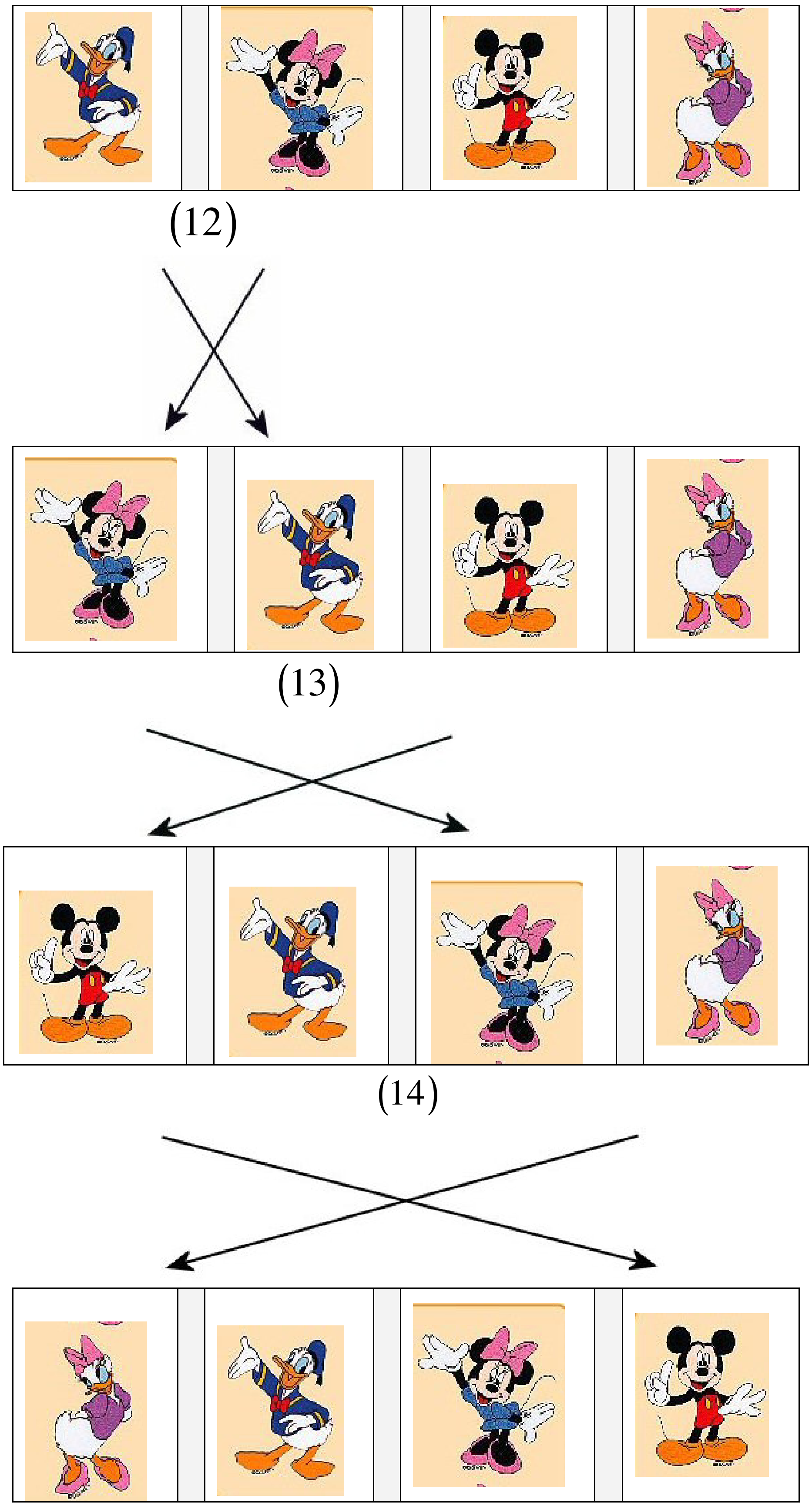


Rotation Permutation
Figure 7

The question then arises, is it possible to carry out this maneuver by repeated interchanges of members two at a time? The answer is yes, and the answer is

$$(1234) = (12),(13),(14)$$

To see how this works, watch how they move.


(12)
(13)
(14)

Example 4: The following permutations are written as the product of transpositions, but not necessarily in the same way. The reader can check these out.

$$(1234\cdots n)=(12)(13)(14)\cdots(1n)$$
$$(4321)=(43)(42)(41)$$
$$(15324)=(15)(13)(12)(14)$$

Symmetric Group S_n

We now see that the set of $n!$ permutations of a set of n elements, where the product of two permutations is taken as their compositions, is a group, called the **symmetric group** S_n.

Theorem 1 If A is a set of n elements, then the set of all permutations of the set is a group, where the group product of two permutations P and Q is defined as the composition of P *followed* by Q, and denoted[3] PQ. The group is called the **symmetric group** S_n on n elements, and the order of the group is $|S_n|=n!$.

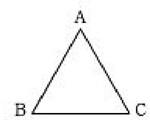
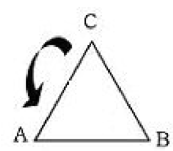
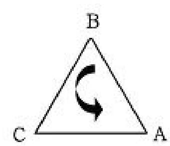
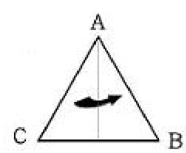
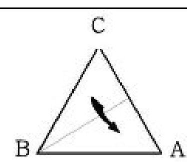
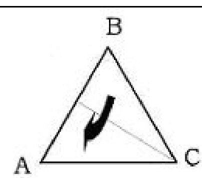
Proof: Group multiplication is closed since each permutation (or shuffling) is a one-to-one mapping from $A=\{1,2,...,n\}$ onto itself, so repeated permutations PQ is also a one-to-one mapping of $\{1,2,...,n\}$ onto itself. The identity of the group is the identity mapping, i.e. the permutation that doesn't change anything. Also, every permutation has a unique inverse since permutations are one-to-one mappings from $\{1,2,...,n\}$ onto itself. Also, multiplication is associative since the composition of two functions is associative. Hence, the axioms of a group are satisfied. ∎

Symmetric Group S_3

In Section 6.2 we constructed the group of rotational and reflective symmetries of an equilateral triangle, called the dihedral group D_3. What we didn't realize at the time was that this dihedral group can also be interpreted as the symmetric group S_3 of all permutations of the three vertices $\{A,B,C\}$ of the triangle. Figure 5 shows the relation between the symmetries of an equilateral triangle and the permutations of the vertices. Note that the

[3] Normally, the composition of two functions, P followed by Q, is denoted $Q\circ P$ (read right to left), but since we are focusing on group "products" we write the composition in *product* form PQ.

composition (i.e. multiplication) of permutations acts exactly like the composition of symmetries of an equilateral triangle. When the elements of two groups can be placed in a one-to-one correspondence where the multiplication in one group is analogous to the multiplication in the other group, the groups are called "abstractly equal" or **isomorphic**.

Group of Permutations of $\{A,B,C\}$	Group of Symmetries of an Equilateral Triangle	Interpretation
$P_1 = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ $(A)(B)(C)$		Do nothing
$P_2 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ (ABC)		Counterclockwise rotation of 120^0
$P_3 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$ (ACB)		Counterclockwise rotation of 240^0
$P_4 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ $(A)(BC)$		Flip through vertex A
$P_5 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$ $(AC)(B)$		Flip through vertex B
$P_6 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$ $(AB)(C)$		Flip through vertex C

Abstract Equivalence of S_3 and D_3

Figure 5

Cayley Table for S_3.

The six permutations of a set of three elements $A = \{1,2,3\}$, written in cycle notation are listed in Table 1.

Permutation	Cyclic Notation
$P:123 \to 123$	$e = (\ )$
$P:123 \to 132$	(23)
$P:123 \to 213$	(12)
$P:123 \to 231$	(123)
$P:123 \to 312$	(132)
$P:123 \to 321$	(13)

Elements of S_3

Table 1

The product PQ is the composition of P followed by Q. For example the product $PQ = (23)(12)$ is found by performing $P = (23)$ first and $Q = (12)$ second. Since $P:1 \to 1$ and $Q:1 \to 2$ and so $PQ:1 \to 2$. Also $P:2 \to 3$ followed by $Q:3 \to 3$ and so $PQ:2 \to 3$. Finally $P:3 \to 2$ and $Q:2 \to 1$ and so $PQ:3 \to 1$. In other words $PQ = (23)(12) = (123)$ as illustrated Table 2, where as customary we suppress the writing of single cycles.

PQ		Q					
		$e = (\ )$	(123)	(132)	(12)	(13)	(23)
P	$e = (\ )$	e	(123)	(132)	(12)	(13)	(23)
	(123)	(123)	(132)	e	(23)	(12)	(13)
	(132)	(132)	e	(123)	(13)	(23)	(12)
	(12)	(12)	(13)	(23)	e	(123)	(132)
	(13)	(13)	(23)	(12)	(132)	e	(123)
	(23)	(23)	(12)	(13)	(123)	(132)	e

Symmetric Group S_3

Table 2

Problems

1. Given the permutations

$$P=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix},\ Q=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$$

find:

a) PQ
b) P^{-1}
c) QP^{-1}
d) $P^2 = PP$
e) $(PQ)^{-1}$

2. For permutations

$$P=\begin{pmatrix}a & b & c & d\\ A & B & C & D\end{pmatrix},\ Q=\begin{pmatrix}e & f & g & h\\ E & F & G & H\end{pmatrix}$$

prove or disprove $(PQ)^{-1} = Q^{-1}P^{-1}$.

3. Find the permutation

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

represented by the following cyclic products

a) (13)(13)
b) (123)(45)(125)(45)
c) (1432)
d) (1)(2)(53)(4)
e) (135)(42)

4. **(Composition of Permutations)** For the following permutations

$$P=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 4 & 5 & 1\end{pmatrix},\ \ Q=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 1 & 3 & 5\end{pmatrix},\ R=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 5 & 3 & 1 & 4\end{pmatrix}$$

a) Show that $PQ \neq QP$
b) Verify $(PQ)R = P(QR)$
c) Verify $(PQ)^{-1} = Q^{-1}P^{-1}$

5. **(Subgroup of S_3)** For the group S_3 of permutations of a set of three elements drawn in Table 2, select the subset $\{e,(123),(132)\}$ and show that this set with the same product rule also forms a group, called a subgroup of S_3. Using the interpretation that the permutations in S_3 also represents the symmetries of an equilateral triangle, what is the interpretation of this subgroup? Are there any other subgroups of S_3?

6. **(Cycles as the Product of 2-cycles)** A two-cycle is an exchange of two elements of a set, such as the permutation (23) of interchanging 2 and 3, leaving the other elements of the set unchanged. Every permutation of a finite set can be written (not uniquely) as the product of 2-cycles. Write the permutation (12345) as the product or composition of 2-cycles.

7. **(Symmetric Group S_2)**

Given the set $A = \{1,2\}$.

a) Construct the Cayley table for the group of permutations on A.
b) What is the order of this group?
c) Is the group Abelian?
d) What is the inverse of each element of the group?

8. **(Transpositions)** Verify the products

$a)$ $(1234\cdots n) = (12)(13)(14)\cdots(1n)$
$b)$ $(214) = (21)(24) = (24)(12)$
$c)$ $(4321) = (43)(42)(41)$
$d)$ $(15324) = (15)(13)(12)(14)$

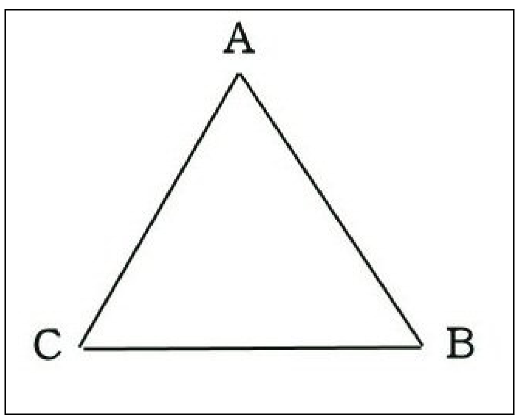
9. **(Even and Odd Transpositions)** In any symmetric group, the permutations can be "factored" as into an even or odd number of transitions. If the number of transitions is even, the permutation is called an **even** permutation, if the number of transpositions is odd the permutation is called **odd.** The symmetric group S_3 has six elements. There are three even and three odd permutations,

Find them. Hint: The identity permutation has 0 transitions, hence it is called an even permutation.

10. **(Subgroups of S_3)** The dihedral group D_3 of symmetries of an equilateral triangle, which is the same as the symmetric group S_3 of permutations of 3 objects, is displayed in the Cayley table in Figure 6. There are four subgroups of order 2 in this group, and one subgroup of order 3. Can you find them? Hint: We have denoted counterclockwise rotation of 120 degrees by r, hence r^2 is 240 degree rotation, and flips through the three vertices by A,B,C.

PQ		Q					
		$e=(\ )$	r	r^2	A	B	C
P	$e=(\ )$	e	r	r^2	A	B	C
	r	r	r^2	e	C	A	B
	r^2	r^2	e	r	B	C	A
	A	A	B	C	e	r	r^2
	B	B	C	A	r^2	e	r
	C	C	A	B	r	r^2	e

Figure 6



Six Symmetries of an Equilateral Triangle