Section 6.3 Permutation Groups

Purpose of Section: To introduce the idea of a permutation of a set and how a composition of permutations acts as a binary relation on the set, which gives rise to a group, called the **symmetric group** S_n.

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 our 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 correspondence (bijection) from a set onto itself. For example, a permutation of elements of the set $A = \{1, 2, 3, ..., n\}$ can be thought of a one-to-one mapping of this set onto itself, represented by

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

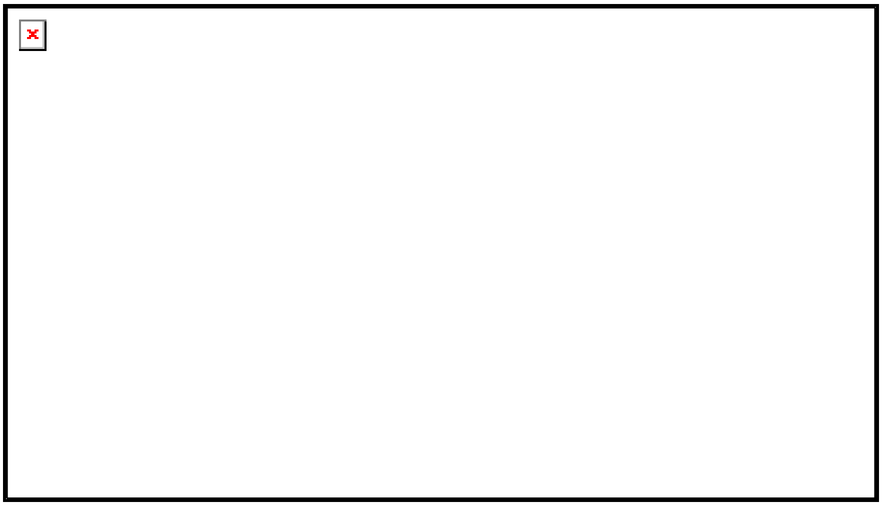
which gives the image k^p of each element $k \in A$ in the first row as the element directly below it in the second row.

For example, a typical permutation of the four elements $A = \{1, 2, 3, 4\}$ is

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

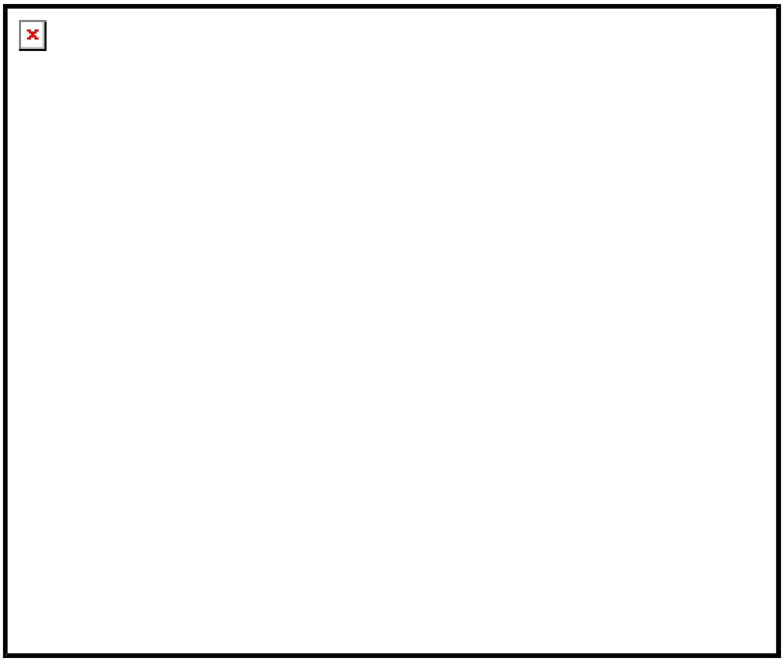
A good way to think about this permutation is to think of a tomato, strawberry, lemon, and apple, arranged from left to right in positions we call 1, 2, 3, and 4. If we apply the permutation P mapping, we get the new arrangement shown in Figure 1.

The tomato that was originally in position 1 has moved to position 2, the strawberry that was in position 2 has moved to position 3, and so on. The important thing to know is that although the individual items have moved, the positions 1, 2, 3, and 4 remain the same.



Permutation mapping
Figure 1

Another way to think of a permutation is with a directed graph, as drawn in Figure 2. In the directed graph, we can see quite visually the rotational movement of the fruit, as everything is shifted to the right, and the apple at the end goes to the front of the line. Again, think of the fruit as moving but the positions are fixed.



Visualization of a permutation
Figure 2

Product of Permutations Starting with the permutation:

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

suppose we follow this permutation by a second permutation Q.In other words, the composition of the permutation P followed by a second permutation Q, which gives rise to a "reshuffling of a reshuffling." This leads us to the definition of the product of two permutations.

Definition: The composition of permutations P and Q is the **product** of P and Q, and denoted[1] by PQ.

The product of the permutations P and Q is

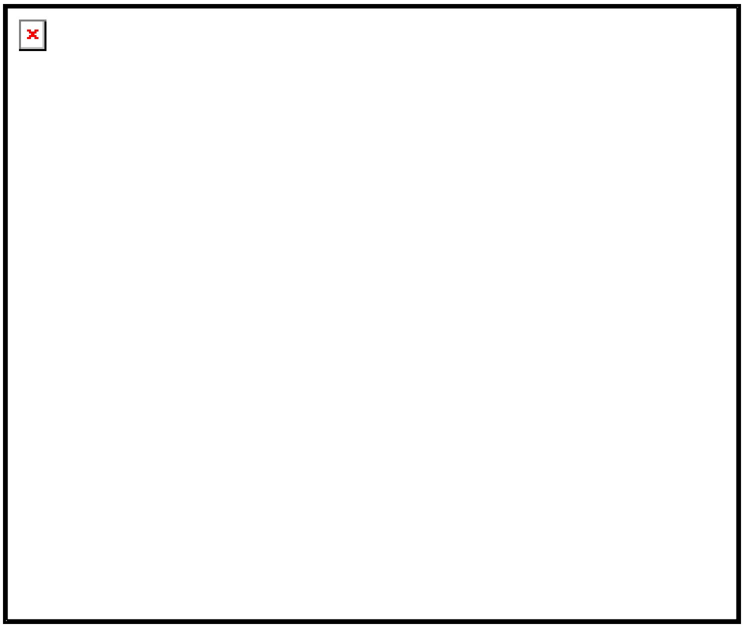
$$PQ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

.

History: The idea of a permutation or arrangement of things has received attention in various cultures throughout history In the *Chinese Book of Changes*, attention is given to "arrangements" of the mystic trigrams. The Greek historian Plutarch writes that the philosopher Xenocrates (350 B.C.) computed the number of possible syllables as 1,000,000,000,000, which hints at taking permutations of syllables.

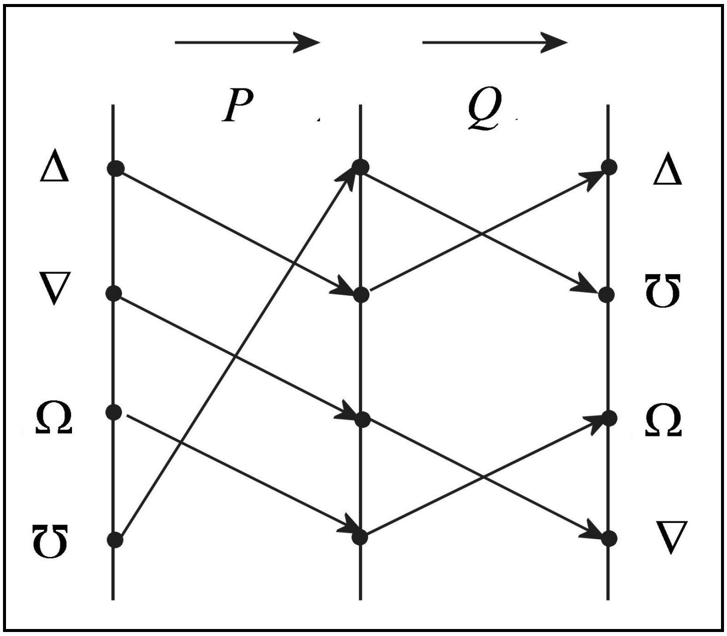
Figure 3 illustrates the movement of the four the fruit

[1] In compositions of functions $(f \circ g)(x) = f[g(x)]$ 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."



Product (composition) of two permutations
Figure 3

A second visualization of this product is shown in Figure 4. This time we use Greek symbols.



Another representation of the product of permutations
Figure 4

Example 1 Multiplying Permutations Find the product PQ of

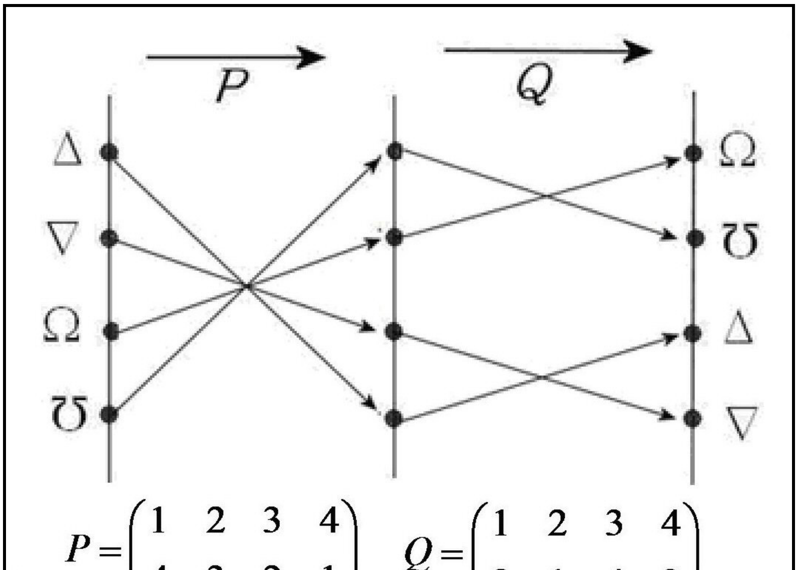
$$P=\begin{pmatrix}1 & 2 & 3 & 4\\4 & 3 & 2 & 1\end{pmatrix},\quad Q=\begin{pmatrix}1 & 2 & 3 & 4\\2 & 1 & 4 & 3\end{pmatrix}$$

Solution: We illustrate the product in Figure 5. Note that

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

Product of permutations
Figure 5

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



Composition of two permutations
Figure 6

If we carry out the permutations P,Q in Example 1 in the opposite order, we find

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

which leads us to believe that it makes no difference in the order the permutations are performed. However, this is not true in general as the following example shows.

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

Inverses of Permutations

If a permutation P maps k into k^P, then its **inverse** P^{-1} maps k^P back onto k. In other words, the inverse of a permutation can be found by simply interchanging the top and bottom rows of the permutation P. For convenience in reading, we reorder the top row 1,2, n from left to right. For example

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

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 the **Cauchy cycle** (or **cyclic**) notation. To illustrate how this works, consider the permutation[2]

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

[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 $\{325614\}$.

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 to 5, so we write $(135$. Then P maps 5 back to 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 to itself so we have a 1-cycle (2). Finally, we see that P maps 4 to 6 so we write $(46$ and since 6 maps back to 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) to streamline the notation.

Example 2: Cycle Notation Each of the following permutations is displayed in both 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 as $(\ )$.

> **Important 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 a glance.

Products of Permutations in Cycle Notation

When taking the product to permutations expressed in cycle notation, one reads from left to right and thinks of each cycle as a function and the entire product as the composition of functions. The process is best explained with an example. Consider the product of four cycles

$$(145)(23)(24)(51)=(1234)(5)=(1234)$$

Starting with 1 in the left-most cycle we see it maps to 4, whereupon we move to the second cycle which does not contain 4 so we move to the third cycle which maps 4 to 2, whereupon we move to the last cycle that does not contain a 2 so we conclude that the product 1 maps to 2, whereupon we start the product permutation as $(12...)$. We then carry out the same process starting at the leftmost permutation to find the image of 2, whereupon the first cycle does not contain 2 so we move to the second cycle and see that 2 maps to 3, and since none of the remaining cycles contain 3, we conclude the product maps 2 maps to 3, so we write the product as $(123...)$. Continuing this process, we obtain the final product of (1234).

Example 3 Permutations in Cycle Form For the set

$$A=\{1,2,3,4,5\}$$

we have the following products.

a) $(1532)(14)(35)=(1452)(3)=(1452)$

b) $(1234)(1432)=(1)(2)(3)(4)=(\ )$

c) $(1342)^{-1}=(1243)$

d) $(14)^{-1}=(14)$ since $(14)(14)=(1)(2)=(\ )$

e) $(125)(34)=(43)(512)=(34)(125)$ (all the same)

Note that in the inverse permutation the orientation goes in the opposite direction; i.e. counterclockwise versus clockwise). Although the commutative law does not hold in general for permutations, there are cases where permutations do commute. For example, if two cycles share no common element, then the order can be switched as in the case $(123)(45)=(45)(123)$. However $(13)(12)\neq(12)(13)$.

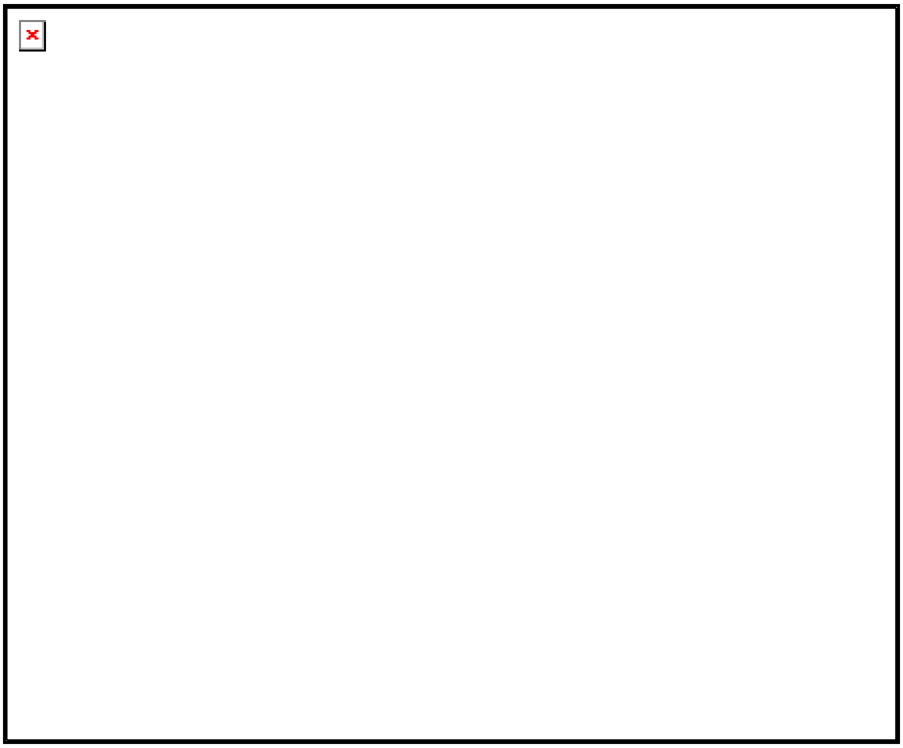
Transpositions

A permutation that interchanges just two elements of a set and leaves all others unchanged is called a **transposition** (or **2-cycle**). For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}=(24)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}=(23)$$

are transpositions. What may not be obvious is that any permutation can be written as the product of transpositions. In other words, any permutation of elements can be carried out by repeated interchanges of two elements. For example, Figure 7 shows four girls 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 the end girl to move to the left position, which is a result of the following permutation.



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 equation is

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

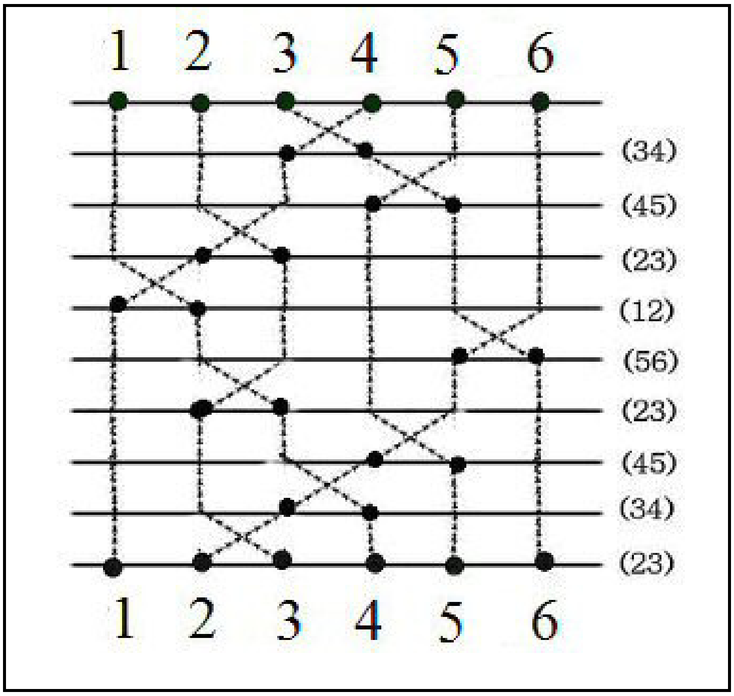
To see how this works, watch how they move in Figure 8.

Permutation as a product of transpositions
Figure 8

Example 4: Factoring Permutations as Transpositions

Observe that the following permutation can be expressed as a series of transpositions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} = (34)(45)(23)(12)(56)(23)(45)(34)(23)$$



Permutation as the product of transpositions
Figure 9

Example 5: Permutation Group The following permutations are written as the product of transpositions.

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

Symmetric Group S_n

We now show that the set of all permutations of a set forms a group.

Theorem 1 The set of all permutations of the set $A = \{1,2,3,...,n\}$ with n members whose group operation is the composition of permutations is a group. The group is called the **symmetric group** S_n on n elements, and the order of the group is $|S_n| = n!$.

Proof: To show that the symmetric group is indeed a group, we need to verify the group axioms of closure, identity, inverse, and associativity.

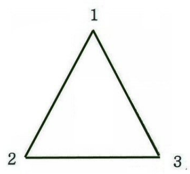
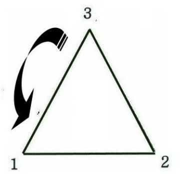
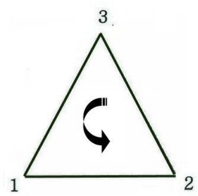
Closure: Each permutation is a one-to-one mapping from $A = \{1,2,...,n\}$ onto itself, so repeated permutations PQ is also a one-to-one mapping of $\{1,2,...,n\}$ onto itself.

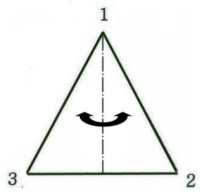
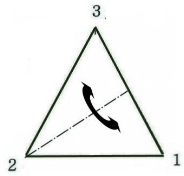
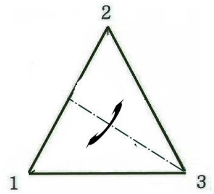
Identity: The permutation that assigns every member to itself serves as the identity of the group.
Unique Inverse: Permutations are bijections and every bijection has a unique inverse.

Associative Law: The group operation is associative since it is the composition of functions which are always are 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 is the same as the symmetric group S_3 of all permutations of the three vertices $\{1,2,3\}$ of a triangle. Figure 10 shows the relation between the symmetries of an equilateral triangle and the permutations of its vertices.

Group of Permutations of $\{1,2,3\}$	Group of Symmetries of an Equilateral Triangle	Interpretation
$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $(1)(2)(3)$		Do nothing
$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ (123)		Counterclockwise rotation of 120^0
$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ (132)		Counterclockwise rotation of 240^0

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ (23)		Flip through vertex 1
$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ (13)		Flip through vertex 2
$P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ (12)		Flip through vertex 3

Abstract equivalence of S_3 and D_3

Figure 10

Cayley Table for S_3.

The six permutations of a set of three elements $A = \{1, 2, 3\}$ and the six symmetries of an equilateral triangle are listed in Table 1.

Permutation	Cyclic Notation	Triangle Symmetry
$P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$e = (\ )$	$e = R_0$
$P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$(123) = (12)(13)$	R_{120}
$P = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$(132) = (13)(12)$	R_{240}
$P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	(23)	V
$P = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	(13)	F_{ne}
$P = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	(12)	F_{nw}

$S_3 \approx D_3$

Table 1

The Cayley table for the group S_3 is shown in Figure 11.

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

Figure 11

Problems

1. **Finding Permutations** Given the permutations

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

find:

a) PQ

b) P^{-1}

c) QP^{-1}

d) P^2

e) $(PQ)^{-1}$

2. **Permutation Identity** For permutations

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

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

3. **Cycle Notation** Fill in the blanks in the permutation

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

represented by the following cyclic products.

a) (13)(24)
b) (123)(45)
c) (1432)
d) (1)(2)(35)(4)
e) (135)(42)

4. **Composition of Permutations** Given the permutations:

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

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

5. **Product of Transpositions** Write the permutation (12345) as the product of transpositions. Verify your answer by placing five objects in a row and shuffling them both as the given permutation and as the compositions of transpositions.

6. **Symmetric Group** S_2 Find the Cayley table for the group of permutations on the set $A = \{1, 2\}$. Is the group Abelian?

7. **Transpositions** Verify the following products.

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

8. **Transpositions Commutate?** Do transpositions commute in general? For the set $\{1, 2, 3\}$, is it true that

$$(12)(13) = (13)(12)\,?$$

9. **Decomposition Into Transitions** Show the decomposition of the permutation (12345) can be written as any of the three forms:

$$\begin{aligned}(12345) &= (12)(13)(14)(15)\\ &= (15)(25)(35)(45)\\ &= (23)(24)(25)(21)\end{aligned}$$

Cartesian (or Direct) Product of Groups

It is possible to piece together smaller groups to form larger groups. If H and G are groups, their Cartesian product[3] is

$$H \times G = \{(h, g) : h \in H, g \in G\}$$

where the group operation $*$ in $H \times G$ is

$$(h, g) * (h', g') = (hh', gg') \ .$$

where hh' is the group operation in group H and gg' is the group operation in group G. The following problems illustrate some Cartesian products of groups.

10. **Cartesian Product of the Klein 4-Group** Find the Cayley table for the group whose set is $\mathbb{Z}_2 \times \mathbb{Z}_2$ and group operation $*$ is defined by

$$(a,b) * (c,d) = ((a+c) \bmod 2,\ (b+d) \bmod 2)$$

Show the Cayley table is the same as the multiplication table for the Klein four-group of symmetries of a rectangle.

11. **Cartesian Product Group** Find the Cayley table for the group whose set is the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_3$ and the group operation $*$ is

$$(a,b) * (c,d) = ((a+c) \bmod 2,\ (b+d) \bmod 3)$$

12**. Even and Odd Permutations and the 15-Puzzle** There are many ways to write a permutation as a composition of simple transpositions. For example, the following permutation of five elements can be written either as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (45)(35)(24)(12)(23)$$

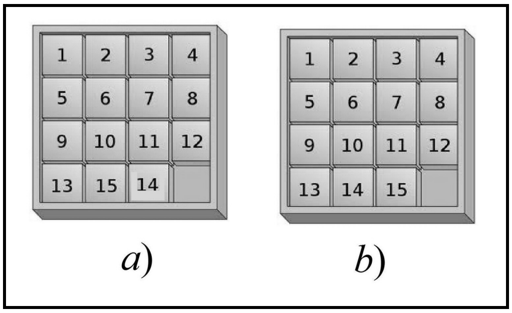
[3] The Cartesian product is often written $H \oplus G$ .. The Cartesian product can be extended to the product on any number of groups, like $G_1 \times G_2 \times \cdots \times G_n$.

or

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (24)(13)(15)$$

Although the above permutation can be written as the different compositions of transpositions, for a given permutation the number of transpositions will always be an even number or an odd number. If the number of transpositions of a permutation is odd, the permutation is called an **odd permutations**; and if the number of transpositions is an even number, the permutation is called an **even permutation**.. Check to see that of the six permutations of the set $\{1,2,3\}$, three are even and three are odd.

13. **Fifteen Puzzle** The 15-puzzle consists of 15 numbered squares on a 4×4 grid with one of the squares missing. The idea is to start with the arrangement in Figure 12a) and slide the squares around any way you desire so that the 14-square and 15-square are interchanged with the blank square returned to the lower right as demonstrated in Figure 12b). Show it is impossible to go from the arrangement in Figure 12a) to the arrangement in Figure 12b) by answering the following questions.



The famous 15-puzzle
Figure 12

a) Calling the blank square 16, convince yourself that every movement of a square is a transposition of the numbers $\{1,2,3,...,15,16\}$.

b) Carry out the sequence of transpositions

(12 16)(11 16)(15 16)(12 16)

to get a feel for the movement of the empty square.

c) Realize that to interchange squares 14 and 15, we must carry out the transposition (14 15) on the set {1, 2, 3,.., 15,16}.

d) Realize that to interchange squares 14 and 15, we must carry out a series of n transpositions

$$(14\ 15) = (a_1\ 16)\ (a_2\ 16) \cdots (a_{n-1}\ 16)\ (a_n\ 16)$$

where $1 \le a_i \le 15$. Realize that since the empty square 16 returns to its original position at the lower-right, it must move up and down an equal number of times, and left and right an equal number of times, thus making n, the number of transpositions to be an even number.

f) Observe that the equation

$$(14\ 15) = (a_1\ 16)(a_2\ 16)\cdots(a_{n-1}\ 16)(a_n\ 16)$$

cannot hold since there is 1 transposition on the left (odd number) and an even number of transpositions on the right-hand side. Hence, it is impossible to move from the arrangement in Figure 12a) to the arrangement in Figure 12b).

ΓΣΘΨΞΠΩ