UNIT 7 PERMUTATION GROUPS

Structure

7.1 INTRODUCTION

In this unit we discuss, in detail, a group that you studied in Sec. 2.5.2. This is the symmetric group. As you have often seen in previous units, the symmetric group S_n, as well as its subgroups, have provided us with a lot of examples. The symmetric groups and their subgroups are called permutation groups. It was the study of permutation groups and groups of transformations that gave the foundation to group theory.

In this unit we will present all the information about permutation groups that you have studied so far, as well as some more. We will discuss the structure of permutations, and look at even permutations in particular. We will show that the set of even permutations is a group called the alternating group. We will finally prove a result by the mathematician Cayley, which says that every group is isomorphic to a permutation group. This result is what makes permutation groups so important.

We advise you to read this unit carefully, because it gives you a concrete basis for studying and understanding the theory of groups, We also suggest that you go through Sec. 2.5.2 again, before tackling this unit.

Objectives

After reading this unit, you should be able to

- express any permutation in S_n as a product of disjoint cycles;
- find out whether an element of S_n is odd or even;
- prove that the alternating group of degree n is normal in S_n, and is of order $\frac{n!}{2}$;
- prove and use Cayley's theorem.

7.2 SYMMETRIC GROUP

From Sec. 2.5.2, you know that a permutation on a non-empty set X is a bijective function from X onto X. We denote the set of all permutations on X by S(X).

Let us recall some facts from Sec. 2.5.2.

Suppose X is a finite set having n elements. For simplicity, we take these elements to be 1, 2, . . . , n. Then, we denote the set of all permutations on these n symbols by S_n.

We represent any $f \in S_n$ in a 2-line form as

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

Now, there are n possibilities for f(1), namely, 1, 2, . . . , n. Once f(1) has been specified, there are (n − 1) possibilities for f(2), namely, $\{1, 2, \dots, n\} \setminus \{f(1)\}$. This is because f is 1-1. Thus, there are n(n − 1) choices for f(1) and f(2). Continuing in this manner, we see that there are n! different ways in which f can be defined, Therefore, S_n has n! elements.

Now, let us look at the algebraic structure of S(X), for any set X. The composition of permutations is a binary operation on S(X). To help you regain practice in computing the composition of permutations, consider an example.

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ be in S_4.

Then, to get $f \circ g$ we first apply g and then apply f.

$\therefore f \circ g(1) = f(g(1)) = f(4) = 3.$

$f \circ g(2) = f(g(2)) = f(1) = 2.$

$f \circ g(3) = f(g(3)) = f(3) = 1.$

$f \circ g(4) = f(g(4)) = f(2) = 4.$

$\therefore f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

We show this process diagrammatically in Fig. 1.

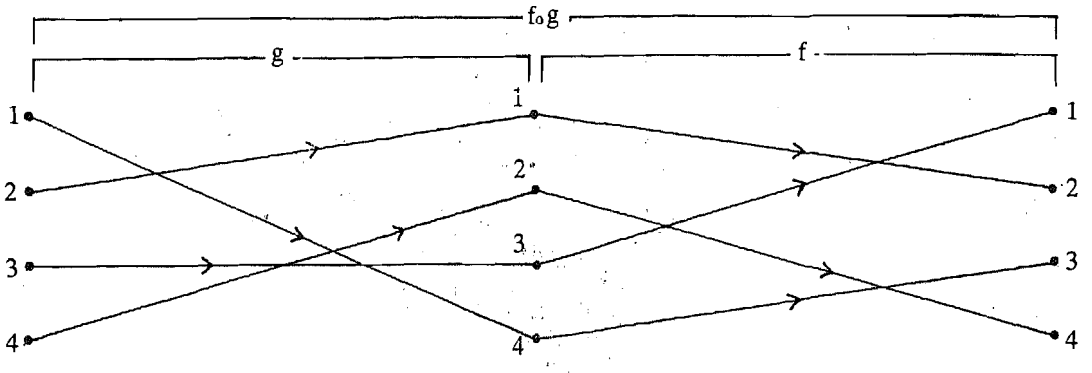

Fig. 1 : (1 2 4 3) ∘ (1 4 2) in S_4

Now, let us go back to $S(X)$, for any set X. We have proved the following result in Sec. 2.5.2.

Theorem 1 : Let X be a non-empty set. Then the system $(S(X), \circ)$ forms a group, called the symmetric group of X.

Thus, S_n is a group of order n!. We call S_n the symmetric group of degree n. Note that if $f \in S_n$, then

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \ldots & f(n) \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Now, with the experience that you have gained in previous units, try the following exercise.

E 1) Show that $(S_n, \circ)$ is a non-commutative group for $n \geq 3$.
(Hint : Check that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ don't commute.)

At this point we would like to make a remark about our terminology and notation.

Remark : From now on we will refer to the composition of permutations as multiplication of permutations. We will also drop the composition sign. Thus, we will write $f \circ g$ as fg.

The two-line notation that we have used for a permutation is rather cumbersome. In the next section we will see how to use a shorter notation.

7.3 CYCLIC DECOMPOSITION

In this section we will first see how td write permutations conveniently, as a product of cycles. Let us first see what a cycle is.

Consider the permutation $f = \begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}$. Choose any one of the symbols, say 1.

Now, we write down a left hand bracket followed by 1 : (1

Since f maps 1 to 3, we write 3 after 1 : (1 3

Since f maps 3 to 4, we write 4 after 3 : (1 3 4

Since f maps 4 to 2, we write 2 after 4 : (1 3 4 2

Since f maps 2 to 1 (the symbol we started with), we close the brackets after the symbol

(1 3 4 2)

Thus, we write f = (1 3 4 2). This means that f maps each symbol to the symbol on its right, except for the final symbol in the brackets, which is mapped to the first.

If we had chosen 3 as our starting symbol we would have obtained the expression (3 4 2 1) for f. However, this means exactly the same as (1 3 4 2), because both denote the permutation which we have represented diagrammatically in Fig. 2.
Such a permutation is called a 4-cycle, or a cycle of length 4. Fig. 2 can give you an indication as to why we give this name.

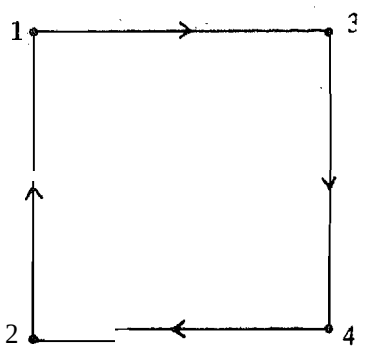

Fig. 2 : (1 3 4 2)

Let us give a definition now.
Definition : A permutation $f \in S_n$ is called an r-cycle (or cycle of length r) if there are r distinct integers $i_1, i_2, i_3, \ldots, i_r$ lying between 1 and n such that
$f(i_1) = i_2, f(i_2) = i_3, \ldots\ldots, f(i_{r-1}) = i_r, f(i_r) = i_1$.
and $f(k) = k \ \forall\ k \notin \{i_1, i_2, \ldots, i_r\}$.

Then, we write $f = (i_1\ i_2 \ldots\ldots i_r)$.

In particular, 2-cycles are called **transpositions**. For example, the permutation $f = (2\ 3) \in S_3$ is a transposition. Here f(1) = 1, f(2) = 3 and f(3) = 2.

Later in this section you will see that transpositions play a very important role in the theory of permutations.

Now consider any 1-cycle (i) in S_n. It is simply the identity permutation
$I = \begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ 1 & 2 & \ldots\ldots & n \end{pmatrix}$, since it maps i to i and the other $(n-1)$ symbols to themselves.
Let us see some examples of cycles in S_3. (1 2 3) is the 3-cycle that takes 1 to 2, 2 to 3 and 3 to 1. There are also 3 transpositions in S_3, namely, (1 2), (1 3) and (2 3).

The following exercise will help you to see if you've understood what a cycle is.

E 2) Write down 2 transpositions, 2 3-cycles and a 5-cycle in S_5.

Now, can we express any permutation as a cycle? No. Consider the following example from S_5. Let g be the permutation defined by

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

If we start with the symbol 1 and apply the procedure for obtaining a cycle to g, we obtain (1 3 4) after three steps, Because g maps 4 to 1, we close the brackets, even though we have not yet written down all the symbols. Now we simply choose another symbol that has not appeared so far, say 2, and start the process of writing a cycle again. Thus, we obtain another cycle (2 5). Now, all the symbols are exhausted.

$\therefore g = (1\ 3\ 4)\ (2\ 5)$.

We call this expression for g a **product** of a 3-cycle and a transposition. In Fig. 3 we represent g by a diagram which shows the 3-cycle and the 2-cycle clearly.

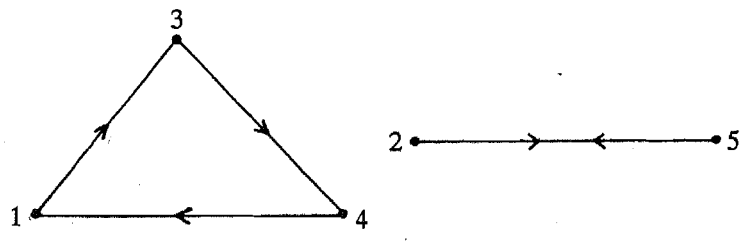

Fig. 3 : (1 3 4) (2 5)

Because of the arbitrary choice of symbol at the beginning of each cycle, there are many ways of expressing g. For example,

$g = (4\ 1\ 3)\ (2\ 5) = (2\ 5)\ (1\ 3\ 4) = (5\ 2)\ (3\ 4\ 1)$.

That is, we can write the product of the separate cycles in any order, and the choice of the starting element within each cycle is arbitrary.

So, you see that g can't be written as a cycle; it is a product of disjoint cycles.
Definition: We call two cycles **disjoint** if they have no symbol in common. Thus, disjoint cycles move disjoint sets of elements, (Note that $f \in S_n$ moves a symbol i if $f(i) \neq i$. We say that f **fixes** i if $f(i) = i$.)

So, for example, the cycles (1 2) and (3 4) in S_4 are disjoint. But (1 2) and (1 4) are not disjoint, since they both move 1.

Note that iff and g are disjoint, then $fg = gf$, since f and g move disjoint sets of symbols.

Now let us examine one more example. Let h be the permutation in S_5 defined by

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

Following our previous rules, we obtain

$h = (1\ 4\ 5)\ (2)\ (3)$,

because each of the symbols 2 and 3 is left unchanged by h. By convention, we don't include the 1-cycles (2) and (3) in the expression for h unless we wish to emphasize them, since they just represent the identity permutation. Thus, we simply write $h = (1\ 4\ 5)$.

If you have understood our discussion so far, you will be able to solve the following exercises.

E 3) Express each of the following permutations as products of disjoint cycles in the manner demonstrated above.

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

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

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

E 4) Do the cycles (1 3) and (1 5 4) commute? Why?

What you have seen in E 3 is true in general. We state the following result.
Theorem 2 : Every permutation $f \in S_n$, $f \neq I$, can be expressed as a product of disjoint cycles.

The proof of this statement is tedious. It is the same process that you have applied in E 3. So we shall not do it here.

Now we will give you some exercises in which we give some interesting properties of permutations.

E 5) Show that every permutation in S_n is a cycle iff $n < 4$.

E 6) Iff $= (i_1\ i_2 \ldots i_r) \in S_n$, then show that
$f^{-1} = (i_r\ i_{r-1} \ldots i_2\ i_1)$.

E 7) Iff is an r-cycle, then show that $o(f) = r$, i.e., $f^r = I$ and $f^s \neq I$, if $s < r$.
(Hint : If $f = (i_1\ i_2 \ldots i_r)$, then $f(i_1) = i_2$, $f^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_r$.)

And now let us see how we can write a cycle as a product of transpositions. Consider the cycle (1 5 3 4 2) in S_5. You can check that this is the same as the product (1 2) (1.4) (1 3) (1 5). Note that these transpositions are not disjoint. In fact, all of them move the element 1.

The same process that we have just used is true for any cycle. That is, any r-cycle
$(i_1\ i_2 \ldots \ldots i_r)$ can be written as $(i_1\ i_r)\ (i_1\ i_{r-1}) \ldots \ldots (i_1\ i_2)$, a product of transpositions.

$(i_1\ i_2 \ldots i_r)$
$= (i_1\ i_r)\ (i_1\ i_{r-1}) \ldots (i_1\ i_2)$

Note that, since the transpositions aren't disjoint, they need not commute.

Try the following exercise now.

E 8) Express the following cycles as products of transpositions:
a) (1 3 5), b) (5 3 1), c) (2 4 5 3).

Now we will use Theorem 2 to state a result which shows why transpositions are so important in the theory of permutations.

Theorem 3 : Every permutation in S_n ($n \geq 2$) can be written as a product of transpositions.

Proof: The proof is really very simple. By Theorem 2 every permutation, apart from I, is a product of disjoint cycles. Also, you have just seen that every cycle is a product of transpositions. Hence, every permutation, apart from I, is a product of transpositions.

Also, I = (1 2) (1 2). Thus, I is also a product of transpositions. So, the theorem is proved.

Let us see how Theorem 3 works in practice. The permutation in E 3(a) is (1 5 3 2 4). This is the same as (1 4) (1 2) (1 3) (1 5).

similarly, the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$

= (1 3 4) (2 6 5) = (1 4) (1 3) (2 5) (2 6).

Now you can try your hand at this process.

E 9) Write the permutation in E 3(b) as a product of transpositions.

E 10) Show that (1 2 . . . . 10) = (1 2) (2 3) . . . . . (9 10).

The decomposition given in Theorem 3 leads us to a subgroup of S_n that we will now discuss.

7.4 ALTERNATING GROUP

You have seen that a permutation in S_n can be written as a product of transpositions. From E 10 you can see that the factors in the product are not uniquely determined. But all such representations have one thing in common—if a permutation in S_n is the product of an odd number of transpositions in one such representation, then it will be a product of an odd number of transpositions in any such representation. Similarly, if $f \in S_n$ is a product of an even number of transpositions in one representation, then f is a product of an even number of transpositions in any such representation. To see this fact we need the concept of the signature or sign function.

Definition : The signature of $f \in S_n$ ($n \geq 2$) is defined to be

$$\text{sign } f = \prod_{\substack{i,j=1 \\ i<j}} \frac{f(j) - f(i)}{j - i}$$

For example, for $f = (1\ 2\ 3) \in S_3$,

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

$$= \left(\frac{3-2}{1}\right)\left(\frac{1-2}{2}\right)\left(\frac{1-3}{1}\right) = 1.$$

Similarly, if $f = (1\ 2) \in S_3$, then

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

$$= \left(\frac{1-2}{1}\right)\left(\frac{3-2}{2}\right)\left(\frac{3-1}{1}\right) = -1.$$

Henceforth, whenever we talk of sign f, we shall assume that $f \in S_n$ for some $n \geq 2$.

$\prod_{i=1}^{m} \alpha_i = \alpha_1 \alpha_2 \ldots \alpha_m$

Try this simple exercise now.

E 11) What is the signature of I E S,?

Have you noticed that the signature defines a function
sign : $S_n \to Z$? We will now show that this function is a homomorphism.

Theorem 4 : Let f, g E S,. Then sign (f ∘ g) = (sign f) (sign g).

Proof : By definition,

$$\text{sign } fog = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{f(g(j)) - f(g(i))}{j - i}$$

$$= \prod_{i,j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \prod_{i,j} \frac{g(j) - g(i)}{j - i}$$

Now, as i and j take all possible pairs of distinct values from 1 to n, so do g(i) and g(j), since g is a bijection.

$$\therefore \prod_{i<j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} = \text{sign } f.$$

∴ sign (fog) = (sign f) (sign g).

Now we will show that Im (sign) = {1, − 1}.

Theorem 5 : a) If t ∈ S, is a transposition, then sign t = − 1.
b) sign f = 1 or − 1 ∀ f ∈ S,.
c) Im (sign) = (1, − 1).

Proof: a) Lett = (p q), where p < q.

Now, only one factor of sign t involves both p and q, namely,

$$\frac{t(q) - t(p)}{q - p} = \frac{p - q}{q - p} = 1.$$

Every factor of sign t that doesn't contain p or q equals 1, since

$$\frac{t(i) - t(j)}{i - j} = \frac{i - j}{i - j} = 1, \text{ if } i, j \neq p, q.$$

The remaining factors contain either p or q. but not both. These can be paired together to form one of the following products.

$$\frac{t(i) - t(p)}{i - p} \cdot \frac{t(i) - t(q)}{i - q} = \frac{i - q}{i - p} \cdot \frac{i - p}{i - q} = 1, \text{ if } i > q,$$

$$\frac{t(i) - t(p)}{i - p} \cdot \frac{t(q) - t(i)}{q - i} = \frac{i - q}{i - p} \cdot \frac{p - i}{q - i} = -1, \text{ if } q > i > p,$$

$$\frac{t(p) - t(i)}{p - i} \cdot \frac{t(q) - t(i)}{q - i} = \frac{q - i}{p - i} \cdot \frac{p - i}{q - i} = 1, \text{ if } i < p.$$

Taking the values of all the factors of sign t, we see that sign t = − 1.

b) Let f ∈ S,. By Theorem 3 we know that $f = t_1 t_2 \ldots t_r$ for some transpositions $t_1, \ldots, t_r$ in S_n.

∴ sign f = sign $(t_1 t_2 \ldots t_r)$
= (sign t_1) (sign t_2) . . . . . sign (t_r), by Theorem 4.
= $(-1)^r$, by (a) above.
∴ sign f = 1 or − 1.

c) We know that Im (sign) ⊆ {1, − I}.
We also know that sign t = −1, for any transposition t; and sign I = 1.
∴ {1, − 1) ⊆ Im {sign).
∴ Im (sign) = (1, − 1}.

Now, we are in a position to prove what we said at the beginning of this section.

Theorem 6 : Let $f \in S_n$ and let
$f = t_1 t_2 \ldots . t_r = t_1' t_2' \ldots t_s'$
be two factorisations of f into a product of transpositions. Then either both r and s are even integers, or both are odd integers.

Proof : We apply the function
sign : $S_n \to \{1, -1\}$ to $f = t_1 t_2 \ldots . t_r$.
By Theorem 5 we see that
sign f = (sign t_1) (sign t2) . . . . . (sign t_r) = $(-1)^r$.
$\therefore$ sign $(t_1' t_2' \ldots t_s') = (-1)^r$, substituting $t_1' t_2' \ldots t_s'$ for f.
that is, $(-1)^s = (-1)^r$.
This can only happen if both s and r are even, or both are odd.

So, we have shown that for $f \in S_n$, the number of factors occurring in any factorisation of f into transpositions is always even or always odd. Therefore, the following definition is meaningful.

Definition : A permutation $f \in S_n$ is called even if it can be written as a product of an even number of transposition. f is called odd if it can be represented as a product of an odd number of transpositions.

sign f = 1 iff f is even.

For example, (1 2) $\in$ S3 is an odd permutation. In fact, any transposition is an odd permutation. On the other hand, any 3-cycle is an even permutation, since
(i j k) = (i k) (i j).

Now, see if you've understood what odd and even permutations are,

---

E 12) Which of the permutation in E 8 and E 9 are odd?

E 13) If f, g E S_n are odd, then is f o g odd tool

E 14) Is the identity permutation odd or even?

Now, we define an important subset of S_n, namely,
$A_n = (f \in S_n \mid f \text{ is even})$.

We'll show that $A_n \triangle S_n$, and that $o(A_n) = \frac{n!}{2}$, for $n \geq 2$.

Theorem 7 : The set A_n of even permutations in S_n forms a normal subgroup of S_n of order $\frac{n!}{2}$.

Proof : Consider the signature function,
sign : $S_n \to (1, -1\}$.
Note that $\{1, -1)$ is a group with respect to multiplication. Now Theorem 4 says that sign is a group homomorphism and Theorem 5 says that Im (sign) = $(1, -1\}$. Let us obtain Ker (sign).
Ker (sign) $= \{f \in S_n \mid \text{sign } f = 1\}$
$= (f \in S_n \mid f \text{ is even})$
$= A_n$.
$\therefore A_n \triangleq S_n$.
Further, by the Fundamental Theorem of Homomorphism
$S_n/A_n \simeq \{1, -1\}$.

$\therefore o(S_n/A_n) = 2$, that is, $\frac{o(S_n)}{o(A_n)} = 2$.

$\therefore o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}$.

Note that this theorem says that the number of even permutations in S_n equals the number of odd permutations in S_n.

Theorem 7 leads us to the following definition.

Definition : A_n, the group of even permutations in S_n, is called the alternating group of degree n.

Let us look at an example that you have already seen in previous units, A_3. Now, Theorem 7 says that $o(A_3) = \frac{3!}{2} = 3$. Since $(1\ 2\ 3) = (1\ 3)(1\ 2)$, $(1\ 2\ 3) \in A_3$. Similarly, $(1\ 3\ 2) \in A_3$. Of course, $I \in A_3$.
$\therefore A3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

A fact that we have used in the example above is that **an r-cycle is odd if r is even, and even if r is odd.** This is because $(i_1 i_2 \ldots . i_r) = (i_1 i_r)\ (i_1 i_{r-1}) \ldots . . . (i_1 i_2)$, a product of $(r - 1)$ transpositions. Use this fact to do the following exercise.

E 15) Write down all the elements of A_4.

Now, for a moment, let us go back to Unit 4 and Lagrange's theorem. This theorem says that the order of the subgroup of a finite group divides the order of the group. We also said that if $n \mid o(G)$, then G need not have a subgroup of order n. Now that you know what A_4 looks like, we are in a position to illustrate this statement.

We will show that A_4 has no subgroup of order 6, even though $6 \mid o(A_4)$. Suppose such a subgroup H exists. Then $o(H) = 6$, $o(A_4) = 12$. $\therefore |A_4 : H| = 2$. $\therefore H \trianglelefteq A4$ (see Theorem 3, Unit 5). Now, A_4/H is a group of order 2. Therefore, by E 8 of Unit 4,
$(Hg)^2 = H\ \forall\ g \in A_4$. (Remember H is the identity of A_4/H.)
$\therefore g^2 \in H\ \forall\ g \in A_4$.
Now, $(1\ 2\ 3) \in A_4$. $\therefore (1\ 2\ 3)^2 = (1\ 3\ 2) \in H$.
Similarly, $(1\ 3\ 2)^2 = (1\ 2\ 3) \in H$. By the same reasoning $(1\ 4\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 3)$, $(1\ 3\ 4)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$ are also distinct element of H. Of course, $I \in H$.
Thus, H contains at least 9 elements.
$\therefore o(H) \geq 9$. This contradicts our assumption that $o(H) = 6$.
Therefore, A_4 has no subgroup of order 6.

We use A_4 to provide another example too. (See how useful A_4 is!) In Unit 5 we'd said that if $H \trianglelefteq N$ and $N \trianglelefteq G$, then H need not be normal in G. Well, here's the example.
Consider the subset $V_4 = \{I, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$ of A_4.

E 16) Check that (V_4, o) is a normal subgroup of A_4.

Now, let $H = \{I, (1\ 2)(3\ 4)\}$. Then H is a subgroup of index 2 in V_4. $\therefore H \trianglelefteq V_4$.
So, $H \trianglelefteq V_4$, $V_4 \trianglelefteq A_4$. But $H \not\trianglelefteq A_4$. Why? Well, $(1\ 2\ 3) \in A_4$ is such that

$$(1\ 2\ 3)^{-1}\ (1\ 2)\ (3\ 4)\ (1\ 2\ 3) = (1\ 3)(2\ 4) \notin H.$$

And now let us see why permutation groups are so important in group theory.

7.5 CAYLEY'S THEOREM

Most finite groups that first appeared in mathematics were groups of permutations. It was the English mathematician Cayley who first realised that every group has the algebraic structure of a subgroup of $S(X)$, for some set X. In this section we will discuss Cayley's result and some of its applications.

Theorem 8 (Cayley): Any group G is isomorphic to a subgroup of the symmetric group $S(G)$.

Proof: For $a \in G$, we define the left multiplication function
$f_a : G \to G : f_a(x) = ax$.
f_a is 1-1, since
$f_a(x) = f_a(y) \implies ax = ay \implies x = y\ \forall\ x, y \in G$.
f_a is onto, since any $x \in G$ is $f_a(a^{-1}x)$.
$\therefore f_a \in S(G)\ \forall\ a \in G$.
(Note that $S(G)$ is the symmetric group on the set G.)

Now we define a function $f : G \to S(G) : f(a) = f_a$.
We will show that f is an injective homomorphism. For this we note that
$(f_a \circ f_b)(x) = f_a(bx) = abx = f_{ab}(x) \; \forall \; a, b \in G$.
$\therefore f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b) \; \forall \; a, b \in G$.
That is, f is a homomorphism.
Now, $\text{Ker } f = \{a \in G \mid f_a = I_G\}$
$= \{a \in G \mid f_a(x) = x \; \forall \; x \in G\}$
$= \{a \in G \mid ax = x \; \forall \; x \in G\}$
$= \{e\}$.
Thus, by the Fundamental Theorem of Homomorphism,
$G/\text{Ker } f \simeq \text{Im } f \leq S(G)$,
that is, G is isomorphic to a subgroup of $S(G)$.

As an example of Cayley's theorem, we will show you that the Klein 4-group K_4 (ref. Example 7, Unit 3) is isomorphic to the subgroup V_4 of S_4. The multiplication table for K_4 is

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

E 17j Check that $f_e = I$, $f_a = (e\ a)\ (b\ c)$, $f_b = (e\ b)\ (a\ c)$, $f_c = (e\ c)\ (a\ b)$.

On solving E 17 you can see that
$K_4 \simeq \{1, (e\ a)\ (b\ c), (e\ b)\ (a\ c), (e\ c)\ (a\ b)\}$. Now, just replace the symbols e, a, b, c by 1, 2, 3, 4 and you'll get V_4.
$\therefore K_4 \simeq V_4$.

Try the following exercise now.

E 18) Obtain the subgroup of S_4, to which Z_4 is isomorphic. Is $Z_4 \simeq A_4$?

So, let us see what we have done in this unit.

7.6 SUMMARY

In this unit we have discussed the following points.

1. The symmetric group $S(X)$, for any set X, and the group S_n in particular.
2. The definitions and some properties of cycles and transpositions.
3. Any non-identity permutation in S_n can be expressed as a disjoint product of cycles.
4. Any permutation in S_n $(n \geq 2)$ can be written as a product of transpositions.
5. The homomorphism sign : $S_n \to \{1, -1\}$, $n \geq 2$.
6. Odd and even permutations.
7. A_n, the set of even permutations in S_n is a normal subgroup of S_n of order $\frac{n!}{2}$, for $n \geq 2$.
8. Any group is isomorphic to a permutation group.

7.7 SOLUTIONS/ANSWERS

E 1) Since $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$,

these two permutations don't commute.
$\therefore S_3$ is non-abelian.
In Unit 6 (after Example 4) we showed how $S_3 \leq S_n \; \forall \; n \geq 3$.
$\therefore S_n$ will be non-abelian $\forall \; n \geq 3$.

E 2) There can be several answers.
Our answer is (1 2), (2 4); (1 3 5), (1 2 3), (2 5 1 4 3).

E 3) a) (1 5 3 2 4)
b) (1 8 5) (2 4) (3 7 6)
c) (1 4) (2 5)

E 4) No. Because

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

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

E 5) You know that all the elements of S_1, S_2 and S_3 are cycles. So, if $n < 4$, every permutation is a cycle in S_n.
Conversely, we will show that if $n \geq 4$, then there is a permutation in S_n which is not a cycle. Take the element (1 2) (3 4). This is an element of $S_n \; \forall \; n \geq 4$, but it is not a cycle.

E 6) Since $(i_1\, i_2 \ldots i_r)\,(i_r\, i_{r-1} \ldots i_2\, i_1) = I = (i, i_{r-1} \ldots i_2\, i_1)\,(i_1\, i_2 \ldots i_r)$,
$(i_1\, i_2 \ldots, i_r)^{-1} = (i_r\, i_{r-1} \ldots i_2\, i_1)$.

E 7) Let $f = (i_1\, i_2 \ldots i_r)$.
Then $f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{r-1}) = i_r, f(i_r) = i_1$.
$\therefore f^2(i_1) = f(i_2), f^3(i_1) = f(i_3) = i_4, \ldots, f^r(i_1) = f(i_r) = i_1$.
Similarly, $f^r(i_k) = i_k \; \forall \; k = 2, \ldots, r$.
$\therefore f^r = I$.
Also, for $s < r$, $f^s(i_1) = i_{s+1} \neq i_1 \therefore f^s \neq I$.
$\therefore o(f) = r$.

E 8) a) (1 5) (1 3)
b) (5 1) (5 3)
c) (2 3) (2 5) (2 4)

E 9) (1 5) (1 8) (2 4) (3 6) (3 7)

E 10) For any three symbols i, j and k,
(i j) (j k) = (i j k).
Then, if m is yet another symbol,
(i j k) (k m) = (i j k m), and so on.
$\therefore$ (1 2) (2 3). . . . (9 10)
= (1 2 3) (3 4). . . . (9 10)
= (1 2 3 4) . . . . (9 10)
= (1 2 3 . . . . 10)

E 11) $\text{sign } I = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{I(j) - I(i)}{j - i} = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{j - i}{j - i} = 1$.

E 12) The permutations in E 8(c) and E 9 are odd.

E 13) sign (f) = sign (g) = − 1.
∴ sign $(f \circ g) = (-1)(-1) = 1$.
∴ $f \circ g$ is even.

E 14) sign I = 1. ∴ I is even.

E 15) We know that $o(A_4) = \frac{4!}{2} = 12$. Now $I \in A_4$. Then, all the 3-cycles are in A_4.

They are (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3).
Then we have all the possible disjoint products of two transpositions. They are
(1 2) (3 4), (1 3) (4 2), (1 4) (2 3).
So we have obtained all the 12 elements of A_4.

E 16) By actual multiplication you can'see that V_4 is closed with respect to $\circ$, and each element of V_4 is its own inverse.
∴ $V_4 \leq A_4$.
Again, by actual multiplication, you can see that
$f^{-1}gf \in V_4 \; \forall \; f \in A_4$ and $g \in V_4$.
∴ $V_4 \trianglelefteq A4$.

E17) $f_e(x) = ex = x \; \forall \; x \in K_4$. ∴ $f_e = I$.
Now, $f_a(e) = a$, $f_a(a) = e$, $f_a(b) = c$, $f_a(c) = b$.
∴ f_a = (e a) (b c).
Similarly, f_b = (e b) (a c) and f_c = (e c) (a b).

E 18) We know that $Z_4 = \langle \bar{1} \rangle$ and $o(\bar{1}) = 4$. Therefore, the subgroup of S_4 isomorphic to Z_4 must be cyclic of order 4.
It is generated by the permutation $f_{\bar{1}}$.
Now $f_{\bar{1}}(x) = \bar{1} + x \; \forall \; x \in Z_4$.
∴ $f_{\bar{1}}$ = $(\bar{1}\ \bar{2}\ \bar{3}\ \bar{4})$, which is the same as (1 2 3 4).
∴ $Z_4 \simeq \langle (1\ 2\ 3\ 4) \rangle$, which is certainly not isomorphic to A_4.