ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Sciences

BMTC-134
ALGEBRA

Block

2

NORMAL SUBGROUPS AND GROUP HOMOMORPHISMS

Course Design Committee*

Prof. Rashmi Bhardwaj
G.G.S. Indraprastha University, Delhi

Dr. Sunita Gupta
University of Delhi

Prof. Amber Habib
Shiv Nadar University
Gautam Buddha Nagar

Prof. S. A. Katre
University of Pune

Prof. V. Krishna Kumar
NISER, Bhubaneswar

Dr. Amit Kulshreshtha
IISER, Mohali

Prof. Aparna Mehra
I.I.T., Delhi

Prof. Rahul Roy
Indian Statistical Institute, Delhi

Prof. Meena Sahai
University of Lucknow

Dr. Sachi Srivastava
University of Delhi

Prof. Jugal Verma
I.I.T., Mumbai

Faculty members
School of Sciences, IGNOU

Prof. M. S. Nathawat (Director)

Dr. Deepika

Mr. Pawan Kumar

Prof. Poornima Mital

Prof. Parvin Sinclair

Prof. Sujatha Varma

Dr. S. Venkataraman

* The Committee met in August, 2016. The course design is based on the recommendations of the Programme Expert Committee and the UGC-CBCS template.

Block Preparation Team

Prof. Parvin Sinclair (*Editor and Writer*)
School of Sciences
IGNOU

Course Coordinator: Prof. Parvin Sinclair

Acknowledgement:

i) To **Prof. Meena Sahai**, University of Lucknow, and **Dr. Pooja Yadav**, Kamla Nehru College, University of Delhi, for their detailed comments.

ii) To Sh. S. S. Chauhan, for the line diagrams, and the CRC, of this block.

iii) Some material of the earlier IGNOU undergraduate course, Abstract Algebra (MTE-06), has been used in this block.

BLOCK INTRODUCTION

This block is a continuation of Block 1, where we discussed various groups and their subgroups. In this block, we start by looking at certain subsets of a group which are closely linked with a given subgroup of the group. These are called cosets of the subgroup in the group. In Unit 5, you will study the cosets of a subgroup in a finite group, in particular. The focus is on an extremely useful theorem, called Lagrange's theorem.

In the next unit, Unit 6, you will study a particular kind of subgroup, called a normal subgroup. Here you will study many examples and properties of these subgroups. In this unit, you will also study the reason for the creation of such subgroups. This is closely linked with the next unit.

In Unit 7, you will really see the importance of normal subgroups. You will see that it is only the cosets of these subgroups that form a group, called a quotient group. In this unit, you will study many examples of quotient groups. You will also find out whether a quotient group of a group G has all the algebraic properties of G or not.

In the next unit of this block, Unit 8, we will introduce you to group homomorphisms, which are functions between groups that preserve the algebraic structure of their domains. Then you will study about bijective homomorphisms, called isomorphisms. This will lead us to the concept of algebraically indistinguishable systems. We say that such systems are isomorphic. This word was first used in 1870 by the French group theorist, Camille Jordan, to describe two groups that are not equal but have exactly the same algebraic behaviour. Finally, we will discuss the important Fundamental Theorem of Homomorphism, and its applications.

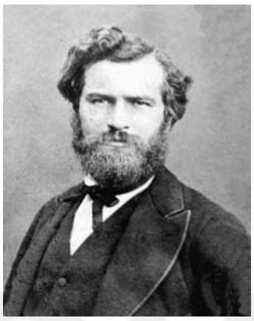

Fig.1: M. E. Camille Jordan (1838-1922)

In Unit 9, you will study groups of permutations, which you were introduced to in Unit 2. Permutation groups give you a concrete basis for the abstract group theory that you are studying. These groups are also important because of the fact that every group is isomorphic to a permutation group, as you will see. In fact, the beginnings of group theory lie in the study of permutations.

With this block we end the study of group theory. In the next two blocks, you will study another algebraic system, namely, a ring. You will see that this system is also a group. And hence, you will continue to use the concepts that you have studied in this block, and the previous one.

NOTATIONS AND SYMBOLS (used in Block 2)

Please **review the notations and symbols** given in Block 1 also.

$\text{Ker } f$	kernel of the homomorphism f
$\text{Im } f$	image of the homomorphism f
$\simeq$	is isomorphic to
$Hx(xH)$	the right (left) coset of H with representative x
A_n	the alternating group on n symbols
$Z(G)$	the centre of the group G
$H \lhd G$	H is normal in G
G/H	the quotient group of G by H
$[G, G], G'$	the commutator subgroup of G
$\text{Aut } G$	the group of automorphisms of G
$\text{Inn } G$	the group of inner automorphisms of G
$H \times K$	the internal direct product of the subgroups H and K

UNIT 5

LAGRANGE'S THEOREM

Structure

5.1 INTRODUCTION

In Unit 3, you have studied different kinds of subgroups. Also, in Unit 1 you have studied about the partitions formed by an equivalence relation. Here, we put these two ideas together. It turns out that given any group G and a subgroup H of the group, we can define an equivalence relation on G using H. In this unit, we will discuss this equivalence relation and consider the partition of G given by the equivalence classes concerned.

In Sec.5.2, you will study about the equivalence relations defined on a group, corresponding to each of its subgroups. You will also study the importance of the partitioning of a group into the equivalence classes, called cosets.

In Sec.5.3, we will use cosets to prove a very useful theorem about the order of a finite group vis-à-vis the order of any of its subgroups. The beginnings of this result were made in a research paper, on the solvability of algebraic equations, by the famous French mathematician, Lagrange (pronounced *la-graunj*). This is why this elementary theorem is known as Lagrange's theorem, though Lagrange only proved it for subgroups of S_n, it seems.

Fig.1: Joseph Louis Lagrange (1736-1813)

In Sec.5.4, you will get a feel of the importance of Lagrange's theorem. Here you will study some of its applications and consequences.

While studying the other units of this block, you will be using Lagrange's theorem frequently. So, study this unit carefully, towards meeting the following learning objectives, around which it has been created.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, left and right cosets of a subgroup;
- partition a group into disjoint cosets of a subgroup;
- state, prove and apply, Lagrange's theorem;
- disprove the converse of Lagrange's theorem.

5.2 COSETS

In Sec.3.4, Unit 3, you studied the product of two subsets of a group. We will now look at the case when one of the subsets is a singleton. In fact, we will look at the situation $\mathrm{H}\{\mathrm{x}\} = \{\mathrm{hx} \mid \mathrm{h} \in \mathrm{H}\}$, where H is a subgroup of a group G and $\mathrm{x} \in \mathrm{G}$. We will **denote $\mathbf{H\{x\}}$ by $\mathbf{Hx}$**.

For example, if $\mathrm{G} = \mathrm{S}_3$, $\mathrm{H} = <(1\ 2)>$ and $\mathrm{x} = (1\ \ 2\ \ 3)$, then $\mathrm{Hx} = \mathrm{H}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 2) \circ (1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\}$. This is an example of a right coset, as you will now see.

Definitions: Let H be a subgroup of a group G, and let $\mathrm{x} \in \mathrm{G}$.

i) The set $\mathrm{Hx} = \{\mathrm{hx} \mid \mathrm{h} \in \mathrm{H}\}$ is called a **right coset** of H in G. The element x is called **a representative** of Hx.

ii) The set $\mathbf{xH} = \{\mathrm{xh} \mid \mathrm{h} \in \mathrm{H}\}$ is called a **left coset of $\mathbf{H}$ in $\mathbf{G}$, represented by $\mathbf{x}$**.

Note that if the group operation is commutative, say $+$, then the right and left cosets of H in $(\mathrm{G}, +)$, represented by $\mathrm{x} \in \mathrm{G}$, are $\mathbf{H} + \mathbf{x} = \{\mathrm{h} + \mathrm{x} \mid \mathrm{h} \in \mathrm{H}\}$ and $\mathbf{x} + \mathbf{H} = \{\mathrm{x} + \mathrm{h} \mid \mathrm{h} \in \mathrm{H}\}$, respectively.

The term 'coset' was probably first used by the mathematician, G. A. Miller, in 1910. However, according to historical sources, it was the famous young French mathematician, Galois, who invented the concept in 1830. Let us look at some examples of this algebraic object.

Example 1: Show that H is a right as well as a left coset of a subgroup H in a group G.

Solution: Consider the right coset of H in G represented by e, the identity of G. Then $\mathrm{He} = \{\mathrm{he} \mid \mathrm{h} \in \mathrm{H}\} = \{\mathrm{h} \mid \mathrm{h} \in \mathrm{H}\} = \mathrm{H}$.
Hence, H is a right coset of H in G.
Similarly, $\mathrm{eH} = \mathrm{H}$, so that H is a left coset of H in G, represented by e.

***

Example 2: What are the right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$?

Solution: Here $\mathrm{H} = 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}$.
The right cosets of H are
$\mathrm{H} + 0 = \mathrm{H}$, using Example 1.

$H+1=\{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\},$
$H+2=\{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\},$
$H+3=\{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\},$
$H+4=\{\ldots, -8, -4, 0, 4, 8, 12, \ldots\}=H.$

Similarly, you can write out the elements of $H+5, H+6, \ldots,$ and see that $H+5=H+1, H+6=H+2,$ and so on.

You can also check that $H-1=H+3, H-2=H+2, H-3=H+1,$ and so on.

Thus, the distinct right cosets are $H, H+1, H+2$ and $H+3.$

***

Consider an important comment here.

Remark 1: Note that $0 \in H+x$ in Example 2 if and only if $x \in H.$ Thus, $H+x$ is not a subgroup of G unless $x \in H.$ For example, $H+1$ and $H+2$ are not subgroups of $G.$

Before giving more examples of cosets, let us discuss some properties of cosets. You have seen some of these in Example 2. These properties will make it easier for us to find the distinct right (or left) cosets of H in $G.$

Theorem 1: Let H be a subgroup of a group G and let $x, y \in G.$ Then

i) $x \in Hx,$

ii) $Hx = H \Leftrightarrow x \in H,$

iii) $Hx = Hy \Leftrightarrow xy^{-1} \in H.$

Proof: For any $x \in G, Hx = \{hx \mid h \in H\}.$

i) Since $e \in H, ex \in Hx,$ that is, $x \in Hx.$

ii) First, let us assume that $Hx = H.$ Then, since $x \in Hx, x \in H.$

Conversely, let us assume that $x \in H.$ We will show that $Hx \subseteq H$ and $H \subseteq Hx.$

$Hx = H \ \forall \ x \in H.$

Now any element of Hx is of the form $hx,$ where $h \in H.$ Since $h \in H$ and $x \in H, hx \in H.$
Thus, $Hx \subseteq H.$ …(1)
Again, for any $h \in H, h = (hx^{-1})x \in Hx,$ since $h \in H$ and $x^{-1} \in H.$
$\therefore\ H \subseteq Hx.$ …(2)
From (1) and (2), you can see that $Hx = H.$

iii) Let $Hx = Hy.$ Since $x \in Hx = Hy, \exists\, h \in H$ s.t. $x = hy.$
Therefore, $xy^{-1} = hyy^{-1} = h \in H.$
Conversely, let $xy^{-1} \in H.$ Then, by (ii), $Hxy^{-1} = H.$
So, for any $hx \in Hx, hxy^{-1} = h'$ for some $h' \in H.$ Thus, $hx = h'y \in Hy.$
So $Hx \subseteq Hy.$ …(3)
Similarly, you can prove that $Hy \subseteq Hx.$ …(4)
By (3) and (4), $Hx = Hy.$ ■

The properties listed in Theorem 1 are not only true for right cosets. Consider the following observation.

Remark 2: Along the lines of the proof of Theorem 1, you can prove that if H is a subgroup of G and $x, y \in G$, then

i) $x \in xH$,

ii) $xH = H \Leftrightarrow x \in H$,

iii) $xH = yH \Leftrightarrow x^{-1}y \in H$.

Let us now look at a few more examples of cosets. First we shall take Example 2 further, using Theorem 1 to generalise it. You know that any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, where $n \in \mathbb{Z}$. Let's see what the cosets of $n\mathbb{Z}$ are.

Example 3: For $n \in \mathbb{N}$, show that **the distinct right cosets of $\mathbf{n\mathbb{Z}}$ in $\mathbb{Z}$ are $\mathbf{n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1)}$.** Similarly, the distinct left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are $n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$.

Solution: Let us write $n\mathbb{Z} = H$, for convenience. Now H is one coset, as you have seen in Example 1. Then $H+1, H+2, \ldots, H+(n-1)$ are also right cosets. Also, from Theorem 1, you know that for $m_1, m_2 \in \mathbb{Z}$, $H+m_1 = H+m_2$ iff $m_1 - m_2 \in H = n\mathbb{Z}$, i.e., iff $n | (m_1 - m_2)$.
Now, for $0 \le i, j < n, i \ne j, n \nmid (i-j)$, since $0 < |i-j| < n$.
Thus, $H, H+1, H+2, \ldots, H+(n-1)$ are distinct right cosets of H in $\mathbb{Z}$.
However, since $n | (n-0)$, $H+n = H+0 = H$.
Similarly, $H+(n+1) = H+1$, and so on.
In fact, for any $m \in \mathbb{Z}$ s.t. $m \ge n$ or $m < 0$, by the division algorithm $\exists$ $q, r \in \mathbb{Z}$, such that $m = qn + r$, $0 \le r < n$. Then $n | (m-r)$.
Thus, $H+m = H+r$ for some $r = 0, 1, \ldots, n-1$.
Hence, $n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1)$ are all the distinct right cosets of $n\mathbb{Z}$ in $\mathbb{Z}$.

Note that m is *an element* of $\mathbb{Z}$, while $\overline{m}$ is *a subset* of $\mathbb{Z}$.

Similarly, you can prove that $n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$ are all the distinct left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$.
We denote $\mathbf{m+n\mathbb{Z}}$ or $\mathbf{n\mathbb{Z}+m}$ by $\overline{\mathbf{m}}$, where $m \in \mathbb{Z}$.

***

From Example 3, in particular, you know that the right cosets of $4\mathbb{Z}$ in $\mathbb{Z}$ are $\overline{0}, \overline{1}, \overline{2}, \overline{3}$, as you discovered in Example 2. For example, $4\mathbb{Z}+57 = 4\mathbb{Z}+1 = \overline{1}$, since $57 \equiv 1 (\text{mod } 4)$. Similarly, $4\mathbb{Z} - 26 \equiv 4\mathbb{Z}+2 = \overline{2}$, since $(-26) \equiv 2 (\text{mod } 4)$.

In Examples 2 and 3, you have looked for cosets in the abelian group $\mathbb{Z}$. Let us now consider the cosets in a non-abelian group.

Example 4: Let $G = S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ and let H be the cyclic subgroup of G generated by $(1\ 2\ 3)$. Obtain the left cosets of H in G. (You will see, in Unit 9, that H is A_3, the alternating group on 3 symbols.)

Solution: Two left cosets are
$H = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ and

$$\begin{aligned}(1\ 2)H &= \{(1\ 2),\ (1\ 2)\circ(1\ 2\ 3),\ (1\ 2)\circ(1\ 3\ 2)\}\\ &= \{(1\ 2),\ (2\ 3),\ (1\ 3)\}.\end{aligned}$$

Now, from Unit 2 you know that $(1\ 2)^{-1} = (1\ 2),\ (1\ 3)^{-1} = (1\ 3),\ (2\ 3)^{-1} = (2\ 3).$

Also $(1\ 2)^{-1}(1\ 3) = (1\ 2)(1\ 3) = (1\ 3\ 2) \in H.$

So, you can apply Theorem 1 to see that $(1\ 2)H = (1\ 3)H.$

Similarly, you can show that $(2\ 3)H = (1\ 3)H$ and $(1\ 2\ 3)H = H = (1\ 3\ 2)H.$

Thus, the distinct left cosets of H are H and $(1\ 2)H.$

***

A brief comment here about the example above.

Remark 3: Note that $S_3 = H \cup (1\ 2)H.$

You can also verify that $S_3 = H \cup (1\ 3)H = H \cup (2\ 3)H.$

Further, $H \cap (1\ 2)H = \emptyset,\ H \cap (1\ 3)H = \emptyset,$ and so on.

What do you see if you connect this information with 'partitions', which you studied about in Unit 1?

Let us now look at the cosets of a very important group, the **quaternion group.** In E29, Unit 2, you have seen that

$Q_8 = \{I,\ A,\ A^2,\ A^3,\ B,\ AB,\ A^2B,\ A^3B\}.$ We can also write

$Q_8 = \{\pm I,\ \pm A,\ \pm B,\ \pm C\},$ where

$$I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ A = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\ B = \begin{bmatrix}0 & i\\ i & 0\end{bmatrix},\ C = \begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix} \text{ and } i = \sqrt{-1}.$$

Here the following relations hold between the elements of Q_8:

$$\begin{aligned}&(-I)^2 = I,\ A^2 = B^2 = C^2 = -I,\\ &AB = C = -BA,\ BC = A = -CB,\ CA = B = -AC.\end{aligned}$$

Note that Q_8 is a non-abelian group under matrix multiplication. With this recap of Q_8, consider the following example.

Example 5: Show that the subgroup $H = \langle A \rangle$ has only two distinct right cosets in Q_8. How many distinct left cosets does it have in Q_8, and why?

Solution: $H = \langle A \rangle = \{I,\ A,\ A^2,\ A^3\} = \{I,\ A,\ -I,\ -A\},$ since $o(A) = 4.$

Therefore, $HB = \{B,\ C,\ -B,\ -C\},$ using the relations given above.

Using Theorem 1(ii), you can see that

$H = HI = HA = H(-I) = H(-A).$

Now $A^{-1} = A^3 = -A.$ Similarly, $B^{-1} = -B,\ C^{-1} = -C.$ So, $BC^{-1} = -BC = -A \in H.$

Hence, using Theorem 1(iii), you can see that $HB = HC.$

On the same lines, verify that $HB = H(-B) = H(-C).$

Therefore, H has only two distinct right cosets in Q_8, namely, H and $HB.$

Note that $Q_8 = H \cup HB = H \cup HC,$ and so on.

Here $H \cap HB = \emptyset = H \cap HC.$

Similarly, you should verify that any two distinct right cosets of H in Q_8 are disjoint.

Along the same lines as above, you should show that H and CH (or BH) are the only two distinct left cosets of H in Q_8.

***

Try solving the following exercises now.

If $H \le G$, Hg need not be equal to $gH \; \forall \; g \in G$.

E1) Obtain all the left and right cosets of $H = <(1\ 2)>$ in S_3. Show that $Hx \ne xH$ for some $x \in S_3$.

E2) Prove that if G is an abelian group and $H \le G$, then every left coset of H is a right coset of H in G, and *vice-versa*.

E3) Show that $K = \{I, -I\}$ is a subgroup of Q_8. Obtain all its left and right cosets in Q_8.

E4) i) Is every coset of a subgroup of a group G also a subgroup of G? Give reasons for your answer.

ii) Prove that if G is a group and $H \le G$, then $xH \le G$ iff $x \in H$.

E5) Let G be a group and $H \le G$. Show that for $a, b, c \in G$, $Ha = Hb$ iff $Hac = Hbc$.

In the examples above, you may have noted that each group can be written as the union of disjoint cosets of the subgroup concerned. This is true for any subgroup of any group. To see this, we define an equivalence relation on the elements of G. (This is what we had hinted at in Remark 3!)

Theorem 2: Let H be a subgroup of a group G. The relation ~, defined by $'x \sim y$ iff $xy^{-1} \in H'$ on the elements of G, is an equivalence relation. The equivalence classes are precisely the right cosets of H in G.

Proof: We need to prove that ~ is reflexive, symmetric and transitive.
Firstly, for any $x \in G$, $xx^{-1} = e \in H$. $\therefore x \sim x$, that is, ~ is reflexive.
Secondly, if $x \sim y$ for any $x, y \in G$, then $xy^{-1} \in H$.
$\therefore (xy^{-1})^{-1} = yx^{-1} \in H$. Thus, $y \sim x$. That is, ~ is symmetric.
Finally, if $x, y, z \in G$ such that $x \sim y$ and $y \sim z$, then $xy^{-1} \in H$ and $yz^{-1} \in H$.
$\therefore (xy^{-1})(yz^{-1}) \in H$, i.e., $x(y^{-1}y)z^{-1} = xz^{-1} \in H$. $\therefore x \sim z$, that is, ~ is transitive.
Thus, ~ is an equivalence relation.

The equivalence class of $x \in G$ is
$[x] = \{y \in G \mid y \sim x\} = \{y \in G \mid yx^{-1} \in H\} = \{y \in G \mid Hx = Hy\}$, by Theorem 1.

Now, we will show that $[x] = Hx$. So, let $y \in [x]$. Then $Hy = Hx$.
Since $y \in Hy$, $y \in Hx$. This is true for any $y \in [x]$.
Therefore, $[x] \subseteq Hx$. …(5)
Now, consider any element hx of Hx. Then $x(hx)^{-1} = xx^{-1}h^{-1} = h^{-1} \in H$.
Therefore, $hx \sim x$. That is, $hx \in [x]$. This is true for any $hx \in Hx$.

Therefore, $Hx \subseteq [x]$. …(6)

Thus, (5) and (6) tell us that $[x] = Hx$.

Hence, each equivalence class is a right coset of H in G. ■

Using Theorem 2 above, and Theorem 9, Unit 1, we have the following result.

Corollary 1: Let G be a group and $H \le G$. If Hx and Hy are two right cosets of a subgroup H in G, then $Hx = Hy$ or $Hx \cap Hy = \emptyset$. Further, any subgroup H of a group G partitions G into disjoint right cosets.

Proof: The relation in Theorem 2 is an equivalence relation, with the equivalence classes being $Hx \ \forall\ x \in G$. Using Theorem 9, Unit 1, we see that this equivalence relation partitions G into disjoint cells. Note that any two cells are either equal or disjoint. Hence the result. ■

On exactly the same lines as above, you can prove that

i) **any two left cosets of H in G are identical or disjoint**, and

ii) **G is the disjoint union of the distinct left cosets of H in G**.

So, for instance, in Example 4 you saw that
$S_3 = <(1\ 2\ 3)> \cup\ (1\ 2) <(1\ 2\ 3)>$.
Also, in Example 5, you saw that $Q_8 = <A> \cup\ B <A>$.

Consider another example.

Example 6: Verify Corollary 1 for the group $G = \mathbb{Z}_{15}$ and $H = <\overline{3}>$.

Solution: Here $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$.

Now $H + \overline{1} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}, \overline{13}\}$. Similarly, find $H + \overline{2}, H + \overline{3}, \dots$.

Note that $H + \overline{x} = H + \overline{y}$ iff $\overline{x} - \overline{y} \in H$, i.e., iff $\overline{x - y} \in H$.

Also, by the division algorithm, for any $n \in \mathbb{Z}$, $n = 3q + r$, for some r, $0 \le r < 3$.

Hence $H + \overline{n} = H + \overline{3q} + \overline{r} = H + \overline{r}$, since $\overline{3q} \in H$.

Thus, the only right cosets of H in G are $H, H + \overline{1}, H + \overline{2}$.

Verify that these three sets are disjoint and that $G = H \cup (H + \overline{1}) \cup (H + \overline{2})$.

***

You should solve the following exercises now.

E6) Let H be a subgroup of a group G. Show that there is a one-to-one correspondence between the elements of H and the elements of each right or left coset of H.
(**Hint:** Show that the mapping $f : H \to Hx : f(h) = hx$ is a well-defined bijection.)

E7) Write $\mathbb{Z}$ as a union of the disjoint cosets of $5\mathbb{Z}$.

E8) Write $\mathbb{Z}_8$ as a union of the disjoint cosets of $<\overline{4}>$.

E9) For a group G and $H \le G$, $Hg_1 = Hg_2$ implies $g_1 = g_2$. True, or false? Why?

E10) Let G be a group and $a \in G$ be of order $15.$ Find all the left cosets of $< a^5 >$ in $< a >$.

E11) Let $H = S^1$ (see Example 5 of Unit 3). Give a geometric description of the cosets of H in $\mathbb{C}^*$.

Using E6, you can see that if H is a **finite** subgroup of a group $G,$ then **the number of elements in every coset of H is the same as the number of elements in H**.

There is another interesting fact about cosets. Consider Example 4. You know that H has two distinct right cosets in $S_3,$ and the same number of distinct left cosets in $S_3.$ In fact, for any finite group G and $H \le G,$ the number of left cosets of H in G is the same as the number of right cosets of H in $G.$ Let us see why.

Theorem 3: Let G be a group and H be a subgroup of $G.$ The function $f,$ defined by $f : \{Hx \mid x \in G\} \to \{yH \mid y \in G\} : f(Hx) = x^{-1}H,$ is a bijection. Thus, the number of distinct right cosets of H in G equals the number of distinct left cosets of H in $G.$

Proof: Firstly, we must check that f is well-defined.

For $x,\ y \in G,\ Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow (xy^{-1})^{-1} = yx^{-1} \in H,$ since $H \le G.$

$$\Leftrightarrow (y^{-1})^{-1}x^{-1} \in H, \text{ since } (y^{-1})^{-1} = y.$$

$$\Leftrightarrow x^{-1}H = y^{-1}H \text{ (from Remark 2).}$$

Thus, f is well-defined. In fact, since we have used the two-way implication throughout the argument above, we have simultaneously shown that f is injective. (How?) You should now check that f is a bijection.

Hence, there is a one-to-one correspondence between the set of right cosets of H in G and the set of left cosets of H in $G.$ ■

If, in Theorem 3, H has infinitely many left cosets in $G,$ then H has infinitely many right cosets in $G.$ If H has a finite number of left cosets in $G,$ say $n,$ then H has n right cosets in $G.$ This leads us to the following definition.

Definition: Let H be a subgroup of a group $G.$ The number of distinct left cosets (or of distinct right cosets) of H in G is called the **index** of H in $G,$ and is denoted by $|\mathbf{G : H}|$.

So, Example 3 tells us that $|\mathbb{Z} : n\mathbb{Z}| = n.$ From Example 4, you find that $|S_3 : H| = 2.$ Similarly, from Example 5 you know that $|Q_8 : < A >| = 2.$

Try solving the following exercises now.

E12) Let $S = \{1, 2, 3\}$ and $T = \{1, 2\}.$ Show that $\wp(T) \le \wp(S).$ Also find $|\wp(S) : \wp(T)|$.

E13) For any finite group $G,$ show that $|G : \{e\}| = o(G).$

E14) Find $|\mathbb{C}^* : S^1|$.

E15) If G is an infinite group, and $H \le G$, must $|G : H|$ be infinite? Why, or why not?

So far we have considered the cosets of both finite and infinite groups. Now we shall focus on finite groups only. We will use Theorem 3 to prove a very important theorem about the number of cosets of a subgroup of a finite group in the next section.

5.3 LAGRANGE’S THEOREM

Consider the examples of finite groups discussed in the previous section. In all of them, you will find that $o(G) = o(H)|G : H|$. You will soon see why this is true in general.

Also, in Unit 4, you have seen that if G is a finite cyclic group, and $H \le G$, then $o(H)|o(G)$. In this section, you shall see that this is true for any finite group. This fact is part of a fundamental theorem about finite groups. Its beginnings appeared in a paper in 1770, written by Lagrange. He proved the result, though, for permutation groups only. The general result, that we will state and prove, is said to have been proved by Evariste Galois in 1830, at the early age of 19! However, it is still named after Lagrange only. Let us see what this pivotal theorem is.

Theorem 4 (Lagrange): Let H be a subgroup of a finite group G. Then $o(G) = o(H)|G : H|$.

In particular, $o(H)$ divides $o(G)$, $|G : H|$ divides $o(G)$, and $|G : H| = \dfrac{o(G)}{o(H)}$.

Proof: In the previous section you have seen that we can write G as a union of finitely many disjoint right cosets of H in G. So, if $Hx_1, Hx_2, \ldots, Hx_r$ are all the distinct right cosets of H in G, we have

$$G = Hx_1 \cup Hx_2 \cup \ldots \cup Hx_r, \qquad \ldots(7)$$

and $|G : H| = r$.

From E6, you know that $|Hx_1| = |Hx_2| = \cdots = |Hx_r| = o(H)$.

Thus, the total number of elements in the union on the right hand side of (7) is $o(H) + o(H) + \cdots + o(H)$ $(r \text{ times}) = o(H) \cdot r$.

Therefore, (7) says that
$$\begin{aligned} o(G) &= o(H) \cdot r \\ &= o(H)|G : H|. \end{aligned}$$

Thus, $o(H)|o(G)$, and $|G : H|\,|\,o(G)$.

Further, $|G : H| = \dfrac{o(G)}{o(H)}$. ■

As you can see, Lagrange’s theorem immediately limits the possibilities of subgroups of any given finite group. For instance, any finite group of order 25 can only have subgroups of orders $1, 5$ or 25. It cannot have a subgroup of order 10, for example, since $10 \nmid 25$.

Consider another example.

Example 7: What are the possible orders of a subgroup of a group of order 30? Further, what would the corresponding number of left cosets be?

Solution: Let G be a group of order $30.$ Any subgroup of G can only be of order $1, 2, 3, 5, 6, 10, 15$ or $30.$

Next, the number of cosets of any subgroup H of G is $|G:H| = \frac{o(G)}{o(H)}.$

So, the index of a subgroup of order $1, 2, 3, 5, 6, 10, 15, 30$ would be

$\frac{30}{1}, \frac{30}{2}, \frac{30}{3}, \frac{30}{5}, \frac{30}{6}, \frac{30}{10}, \frac{30}{15}, \frac{30}{30},$ respectively, i.e., $30, 15, 10, 6, 5, 3, 2, 1,$ respectively.

***

Here is an important comment about Lagrange's theorem.

Remark 4: Note that Lagrange's theorem cannot be generalised to infinite groups since the concept of $o(H)$ dividing $o(G)$ is meaningful only for finite groups.

However, note that an infinite group can have a finite subgroup, and an infinite group can have subgroups of finite index.

For example, consider $(\mathbb{R}^*, \cdot),$ which is an infinite group. $(\{1, -1\}, \cdot)$ is a finite subgroup of $(\mathbb{R}^*, \cdot).$

Also, you have seen that $\mathbb{Z}$ is infinite, but the index of $n\mathbb{Z}$ in $\mathbb{Z}$ is finite, namely, $n.$

Now consider an example that we referred to in Unit 4.

Example 8: Give an example of a non-cyclic group of which every proper subgroup is cyclic.

Solution: Consider $K_4,$ the Klein 4-group given in Example 6, Unit 4. Over there you saw that K_4 is not cyclic. Any proper subgroup of K_4 is of order 1 or $2,$ by Lagrange's theorem. $\{e\}$ is the only subgroup of order $1,$ and it is cyclic.

Similarly, the only subgroups of order 2 are $<a>, <b>, <ab>.$

Thus, K_4 is a required example.

***

Try solving some exercises now.

'Indices' is the plural of 'index'.

E16) Let G be a group, $H \lneqq G$ and $K \lneqq H.$ If $o(K) = 30$ and $o(G) = 300,$ what are the possible orders of H? What would the corresponding indices of H in G be?

E17) If H and K are subgroups of a group G of orders 12 and $35,$ respectively, then find $H \cap K.$

E18) If H and K are proper subgroups of a finite group $G,$ with $o(H) \neq o(K),$ must $H \cap K = \{e\}$? Why, or why not?

E19) Find the possible orders of a non-trivial proper subgroup of
i) $S_4,$ ii) $D_{10},$ iii) $Q_8,$ iv) $\mathbb{M}_{2\times 3}(\mathbb{Z}_n), n \in \mathbb{N}.$

You have, by now, got some idea of the power and beauty of Lagrange's theorem. You may wonder if its converse is also true. Consider the following remark about this.

Remark 5: The **converse of Lagrange's theorem:** if G is a finite group and $m \mid o(G)$, then G has a subgroup of order m.

Is this true? If G is cyclic, you know from Theorem 7, Unit 4, that this is true. But, if G is not cyclic, the converse of Lagrange's theorem is not true. In Unit 9, you will study about the subgroup

$$A_4 = \{I, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

of S_4. You will see that A_4 has no subgroup of order 6, though $6 \mid 12 = o(A_4)$.

We can prove quite a few nice results by applying Lagrange's theorem. In the next section, we shall look at some of these results.

5.4 SOME APPLICATIONS

As you have seen, Lagrange's theorem is extremely useful for finding the possible subgroups of finite groups. In this section we shall look at some specific applications of this theorem.

In Unit 4, you have seen that if G is a finite cyclic group, the order of each element divides $o(G)$. Now consider all the examples of non-cyclic finite groups that you have worked on in this unit, and in other units. You can see that for each $g \in G$, $o(g)$ divides $o(G)$, in each case. This is true, in general, as you will now see.

Theorem 5: Let G be a finite group, and $g \in G$. Then $o(g) \mid o(G)$.

Hence, $g^{o(G)} = e \ \forall\ g \in G$.

Proof: Since $g \in G$, $< g > \leq G$.

Hence, $o(< g >) \mid o(G)$, by Lagrange's theorem.

Thus, $o(g) \mid o(G)$.

Now, let $g \in G$ and let $o(g) = n$. Then $o(G) = nm$, for some $m \in \mathbb{N}$.

So $g^{o(G)} = g^{nm} = (g^n)^m$
$= e.$ ■

By Theorem 5, we know that, for example, $G = \mathbb{M}_{2\times 3}(\mathbb{Z}_7)$ cannot have an element of order 5^n for any $n \in \mathbb{N}$, since $o(G) = 6^7$.

Next, let us look at a consequence of Theorem 5 for groups of prime order. It turns out that such groups are forced to be cyclic, and hence abelian.

Theorem 6: Let G be a group of prime order. Then G has no proper non-trivial subgroup. Further, G is cyclic.

Proof: Let G be a group of prime order, p. Let $H \leq G, H \neq \{e\}$. Then $o(H) \mid o(G)$, i.e., $o(H) \mid p$.

$\therefore$ oH) $= 1$ or p. But $H \neq \{e\}$.
Hence, $o(H) = p = o(G)$.
Thus, $H = G$.

Next, since $p \neq 1, \exists\, a \in G$ s.t. $a \neq e$.
So, $< a > \leq G$ s.t. $< a > \neq \{e\}$.
Therefore, $< a > = G$, that is, G is cyclic. ■

Let us consider an example of the usefulness of Theorem 6.

Example 9: Check whether or not all the proper subgroups of a group G, of order 35, are cyclic.

Solution: By Lagrange's theorem, any subgroup of G is of order $1, 5$ or 7. Since $\{e\} = < e >$, and 5 and 7 are prime numbers, all the subgroups of G are cyclic, by Theorem 6.

***

Now, what about groups of composite order? Can we generalise what you have seen in Example 9? If so, to what extent? Let's see.

Theorem 7: If G is a finite group such that $o(G)$ is neither 1 nor a prime, then G has a non-trivial proper subgroup.

Proof: If G is not cyclic, then any $a \in G, a \neq e$, generates a proper non-trivial subgroup $< a >$, and we are through.
Now, suppose G is cyclic, say $G = < x >$, where $o(x) = mn(m, n \neq 1)$.
Then, from Unit 4, you know that $o(x^m) = \dfrac{mn}{(mn, m)} = n$.
Also $n < o(G)$.
Thus, $< x^m >$ is a proper non-trivial subgroup of G. ■

Now, you should solve the following exercises.

E20) Give the possible orders of a non-trivial element of a non-cyclic group of order 28.

E21) Obtain two non-trivial proper subgroups of D_8.

E22) State the converse of Theorem 6. Prove, or disprove, it.

E23) Let G be a finite group of order n. Let $H \lneq G, H \neq \{e\}$. Must n be composite? Why, or why not?

E24) Can we generalise from Example 9 that if $o(G)$ is composite, then every proper subgroup of G must be cyclic? Give reasons for your answer.

We will now prove certain important number theoretic results which follow from Lagrange's theorem. To begin with, let us prove a result that gives us examples of subgroups of $\mathbb{Z}_n^*$ for every $n \geq 2$.

Theorem 8: Let $G=\{\bar{r}\in\mathbb{Z}_n \mid (r, n)=1\}$, where $n\geq 2$, and (r, n) is the g.c.d of r and n. Then $(G, \cdot)$ is a group, where $\bar{r}\cdot\bar{s}=\overline{rs}\ \forall\ \bar{r}, \bar{s}\in\mathbb{Z}_n^*$.
Further, $o(G)=\phi(n)$, where ϕ is the Euler phi-function (see Sec.4.3, Unit 4).

Proof: Let us first check that G is closed under multiplication.
For $\bar{r}, \bar{s}\in G, (r, n)=1$ and $(s, n)=1$. So $(rs, n)=1$. Thus, $\overline{rs}\in G$.
Therefore, $\cdot$ is a binary operation on G.

You know, from Unit 1, that multiplication is associative in $\mathbb{Z}_n$. Hence, it is associative in G.

Next, $\bar{1}\in G$, and is the multiplicative identity.

Finally, for any $\bar{r}\in G$,
$(r, n)=1$
$\Rightarrow ar+bn=1$ for some $a, b\in\mathbb{Z}$ (by Theorem 5 of Unit 1).
$\Rightarrow n \mid (ar-1)$
$\Rightarrow ar\equiv 1 (\text{mod}\, n)$
$\Rightarrow \bar{a}\,\bar{r}=\bar{1}$ in $\mathbb{Z}_n$.
$\Rightarrow \bar{a}=\bar{r}^{-1}$.
Further, $\bar{a}\in G$, because if $(a, n)=d$, then $d \mid (ar+bn)$, i.e., $d \mid 1$, so that $d=1$.
Thus, every element in G has a multiplicative inverse.

Therefore, $(G, \cdot)$ is a group.

Since G consists of all those $\bar{r}\in\mathbb{Z}_n$ such that $r<n$ and $(r, n)=1$,
$o(G)=\phi(n)$. ■

In the theorem above, G is the group of the elements of $\mathbb{Z}_n$ that have multiplicative inverses. In Block 3, you will see that we call this the unit group of $\mathbb{Z}_n$, and denote this by $U(\mathbb{Z}_n)$.

Now let us see where Theorem 8 and Lagrange's theorem, put together, take us. Consider the following result due to the mathematicians Leonhard Euler and Pierre Fermat (pronounced *fair-maa*). It is very useful when dealing with large numbers. This theorem is a generalisation of Fermat's little theorem (see E26). It was proved by Leonhard Euler.

Fig. 2: Pierre de Fermat (1601-1665) was a very important French mathematician.

Theorem 9 (Euler-Fermat): Let $a\in\mathbb{N}$ and $n\geq 2$ such that $(a, n)=1$. Then $a^{\phi(n)}\equiv 1(\text{mod}\, n)$.

Proof: Since $\bar{a}\in\mathbb{Z}_n$ and $(a, n)=1, \bar{a}\in G$ (of Theorem 8).
Since $o(G)=\phi(n)$, from Theorem 5 we see that $\bar{a}^{\phi(n)}=\bar{1}$.
Thus, $a^{\phi(n)}\equiv 1(\text{mod}\, n)$. ■

Consider an example of the application of Theorem 9.

Example 10: Find the remainder obtained on dividing 6^{41} by 55. Use the fact that if $(m, n)=1$, then $\phi(mn)=\phi(m)\phi(n)$.

Solution: We can apply Theorem 9 to $a = 6$ and $n = 55$, since $(6, 55) = 1$.
So $6^{\phi(55)} \equiv 1 (\bmod 55)$.
Now, you know that $(5, 11) = 1$. So $\phi(55) = \phi(5)\phi(11)$.
Also, from Unit 4 you know that $\phi(5) = 4$, $\phi(11) = 10$. Hence, $\phi(55) = 40$.
Thus, $6^{40} \equiv 1 (\bmod 55)$. Hence, $6^{41} = 6^{40} \cdot 6 \equiv 6 (\bmod 55)$.
Therefore, on dividing 6^{41} by 55, the remainder is 6.

***

Now you can use Theorem 9 to solve the following exercises.

E25) What is the remainder obtained on dividing 3^{47} by 23?

E26) Let $a \in \mathbb{N}$ and p be a prime. Show that $a^p \equiv a (\bmod p)$. (This result is called **Fermat's little theorem**.)
[**Hint:** Recall the properties of the Euler phi-function from Unit 4.]

Let us now consider another important application of Lagrange's theorem, this time to permutations of a set X, $S(X)$ (see Unit 2). But first we need to introduce you to a couple of related concepts.

Definitions: Let $G \le (S(X), \circ)$. For each $x \in X$,

1) the **stabiliser** of x in G is the set $\text{Stab}_G(x) = \{\sigma \in G \mid \sigma(x) = x\}$, i.e., the set of all permutations of X that fix x.

2) the **orbit of $\mathbf{x}$** under G is the set $\mathbf{Orb_G(x)} = \{\sigma(x) \mid \sigma \in G\}$.

Here are a couple of important comments about these objects.

Remark 6: i) Note that $\text{Stab}_G(x) \subseteq G$ and $\text{Orb}_G(x) \subseteq X$.

ii) We can define an equivalence relation on the elements of X, using G, in which the equivalence class of $x \in X$ is $\text{Orb}_G x$. So, X is a disjoint union of the orbits of x, $x \in X$.

To get you used to these algebraic objects, let us consider an example.

If there is no confusion about G, we often write Stab(x) instead of $\text{Stab}_G(x)$, and $\text{Orb}(x)$ instead of $\text{Orb}_G(x)$.

Example 11: Let $X = \{1, 2, 3\}$, and
$G = S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
Find $\text{Stab}_G(1)$ and $\text{Stab}_G(2)$, as well as $\text{Orb}_G(1)$ and $\text{Orb}_G(2)$.

Solution: $\text{Stab}_G(1) = \{\sigma \in S_3 \mid \sigma(1) = 1\} = \{I, (2\ 3)\}$, and
$\text{Stab}_G(2) = \{\sigma \in S_3 \mid \sigma(2) = 2\} = \{I, (1\ 3)\}$.
$\text{Orb}_G(1) = \{\sigma(1) \mid \sigma \in S_3\} = \{1, 2, 3\} = X$, since $I(1) = 1$, $(1\ 2)$ moves 1 to 2, $(1\ 3)$ moves 1 to 3.
Similarly, $\text{Orb}_G(2) = \{\sigma(2) \mid \sigma \in S_3\} = \{2, 1, 3\} = X$.

Here, note that $o(G) = 6 = |\mathrm{Stab}(1)|\ |\mathrm{Orb}(1)|$, and $o(G) = |\mathrm{Stab}(2)|\ |\mathrm{Orb}(2)|$.

***

The relationship between $o(G)$, $|\mathrm{Stab}_G(x)|$ and $|\mathrm{Orb}_G(x)|$, that you see in the example above, is true for any finite G, as we shall show now. This is a very important application of Lagrange's theorem, as we had mentioned earlier. But first, a lemma.

Lemma 1: Let X be a non-empty set and $G \leq S(X)$. Then $\mathrm{Stab}_G(x) \leq G\ \forall\ x \in X$.

Proof: Since $I(x) = x$, $I \in \mathrm{Stab}_G(x)$. Hence, $\mathrm{Stab}(x) \neq \emptyset$.

Next, if $\alpha, \beta \in \mathrm{Stab}_G(x)$, then $\alpha\beta^{-1}(x) = x$, so $\alpha\beta^{-1} \in \mathrm{Stab}_G(x)$.

Thus, by the subgroup test, $\mathrm{Stab}_G(x) \leq G\ \forall\ x \in X$. ■

Now let us prove the theorem we had mentioned above.

Theorem 10 (Orbit-Stabiliser Theorem): Let X be a non-empty set and G be a finite subgroup of $S(X)$. Then, for any $x \in X$,

$$o(G) = |\mathrm{Orb}_G(x)|\ o(\mathrm{Stab}_G(x)).$$

Proof: Let $x \in X$, and let $H = \mathrm{Stab}_G(x)$. Then $H \leq G$, by Lemma 1.

Define $f : \{\sigma H | \sigma \in G\} \to \mathrm{Orb}_G(x) : f(\sigma H) = \sigma(x)$.

Let us check that f is well-defined and 1-1.

For $\sigma, \phi \in G$, $\sigma H = \phi H \Leftrightarrow \phi^{-1}\sigma \in H \Leftrightarrow \phi^{-1}\sigma(x) = x \Leftrightarrow \sigma(x) = \phi(x)$. Note that at each stage we have used the two-way implication (if and only if). So we have proved two things – one, f is well-defined, and two, f is 1-1.

Next, f is a surjection because for any $\sigma(x) \in \mathrm{Orb}_G(x)$, there is the coset σH in G such that $f(\sigma H) = \sigma(x)$.

Hence, f is a bijection between the set of (left) cosets of $\mathrm{Stab}_G(x)$ in G and $\mathrm{Orb}_G(x)$.

Hence, $|G : \mathrm{Stab}_G(x)| = |\mathrm{Orb}_G(x)|$.

Thus, by Lagrange's theorem, $o(G) = o(\mathrm{Stab}_G(x))|\mathrm{Orb}_G(x)|$. ■

Try solving a related exercise now.

E27) Let $G = V_4 = \{I, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\} \leq S_4$. Verify the orbit-stabiliser theorem for $x = 1, 3$ in $X = \{1, 2, 3, 4\}$.

With this we end the discussion focussed on cosets and on Lagrange's theorem. Let us summarise what you have studied in this unit.

5.5 SUMMARY

In this unit, you have studied about the following points.

1. The definition, and examples, of right and left cosets of a subgroup of a group.

2. Two left (or right) cosets of a subgroup are disjoint or identical.

3. Any subgroup partitions a group into disjoint left (or right) cosets of the subgroup.

4. The proof of Lagrange's theorem, which states that if H is a subgroup of a finite group G, then $o(G) = o(H)|G : H|$.

   But, the converse is not true, that is, if G is a finite group and $m \mid o(G)$, then G need not have a subgroup of order m.

5. The following consequences of Lagrange's theorem:

   i) The order of a subgroup H of a finite group G, and the index of H in G, divide the order of the group.

   ii) The order of any element of a finite group divides the order of the group.

   iii) Every group of prime order is cyclic.

   iv) A group of prime order has no proper non-trivial subgroup.

   v) Every group of composite order has a non-trivial proper subgroup.

   vi) **Euler-Fermat Theorem:** $a^{\phi(n)} \equiv 1 (\bmod n)$, where $a, n \in \mathbb{N}$, $(a, n) = 1$ and $n \geq 2$, and ϕ is the Euler phi-function.

   vii) **Orbit-Stabiliser Theorem:** Let X be a non-empty set and G be a finite subgroup of $S(X)$. Then, for any $x \in X$, $o(G) = |\text{Orb}_G(x)|\, o(\text{Stab}_G(x))$.

5.6 SOLUTIONS / ANSWERS

E1) $H = \{I, (1\ 2)\}$.

Its left cosets are $H, (1\ 2)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H$.

Now, $(1\ 2)H = H$ since $(1\ 2) \in H$.

Also, using Theorem 1, $(1\ 2\ 3)H = (1\ 3)H, (1\ 3\ 2)H = (2\ 3)H$, since $(1\ 3)^{-1}(1\ 2\ 3) \in H$ and $(2\ 3)^{-1}(1\ 3\ 2) \in H$.

Thus, the distinct left cosets of H in S_3 are $H, (1\ 3)H, (2\ 3)H$.

Similarly, verify that the distinct right cosets of H in S_3 are $H, H(1\ 3), H(2\ 3)$.

Now, $(13)H = \{(1\ 3), (1\ 2\ 3)\}$ and $H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$.

$\therefore (1\ 3)H \neq H(1\ 3)$.

You can also see that $(2\ 3)H \neq H(2\ 3)$.

E2) Consider a left coset of H in $(G, +)$,

$x+H=\{x+h \mid h\in H\}$

$=\{h+x \mid h\in H\}$, since $x+h=h+x\ \forall\ h\in H.$

$=H+x$, a right coset of H in G.

Similarly, you can prove that every right coset is a left coset.

E3) Since $ab^{-1}\in K\ \forall\ a, b\in K$, we can apply Theorem 2 of Unit 3 to say that $K\le Q_8$.
Now, $K=KI=K(-I)$. Also $KA=K(-A)=\{A, -A\}$, since $A(-A)^{-1}=-I\in K$.
Similarly, $KB=K(-B)=\{B, -B\}$, and $KC=K(-C)=\{C, -C\}$.
Hence, its right cosets are K, KA, KB, KC. Similarly, you should verify that its left cosets are K, AK, BK, CK.

E4) i) No, read Remark 1.

ii) $xH\le G\Rightarrow e\in xH\Rightarrow e=xh$, for some $h\in H\Rightarrow x=h^{-1}\in H$.
Conversely, by Theorem 1, $xH=H\le G$.

E5) $Ha=Hb\Leftrightarrow ab^{-1}\in H\Leftrightarrow (ac)(bc)^{-1}\in H\Leftrightarrow Hac=Hbc$.

E6) Let Hx be a coset of H in G. Consider the function
$f: H\to Hx: f(h)=hx$.
Check that f is well-defined.
Now, for $h, h'\in H, hx=h'x\Rightarrow h=h'$, by cancellation.
Therefore, f is 1-1.
Also f is surjective. (Why?)
Thus, f is a bijection.
And hence, there is a one-to-one correspondence between the elements of H and those of Hx.

Similarly, the map $g: H\to xH: g(h)=xh$ is a bijection.
Thus, the elements of H and xH are in one-to-one correspondence.

E7) The distinct cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are $5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4$.
Now, given any $m\in\mathbb{Z}, \exists\ q, r\in\mathbb{Z}$ s.t. $m=5q+r, 0\le r<4$.
Since $5q\in 5\mathbb{Z}, m\in(5\mathbb{Z}+r)$, for some $r=0, 1,\ldots,4$.
$\therefore \mathbb{Z}=5\mathbb{Z}\cup(5\mathbb{Z}+1)\cup(5\mathbb{Z}+2)\cup(5\mathbb{Z}+3)\cup(5\mathbb{Z}+4)$.

E8) As in Example 6, you should show that the distinct cosets of $<\bar{4}>$ in $\mathbb{Z}_8$ are $<\bar{4}>, <\bar{4}>+\bar{1}, <\bar{4}>+\bar{2}, <\bar{4}>+\bar{3}$. Also verify that $\mathbb{Z}_8$ is the union of these disjoint subsets.

E9) False. For example, in E8, $<\bar{4}>+\bar{1}=<\bar{4}>+\bar{5}$, but $\bar{1}\ne\bar{5}$ in $\mathbb{Z}_8$.

E10) Since $o(a)=15$, we find that $o(a^5)=3$.
Let $H=<a^5>=\{e, a^5, a^{10}\}$.
Then $aH=\{a, a^6, a^{11}\}$, $a^2H=\{a^2, a^7, a^{12}\}, a^3H=\{a^3, a^8, a^{13}\}$,
$a^4H=\{a^4, a^9, a^{14}\}$.
Since $<a>$ is the union of $H, aH,\ldots,a^4H$, these are all the left cosets of H in $<a>$.

E11) $S^1 = \{z \in \mathbb{C}^* \mid |z| = 1\}$.

Since $\mathbb{C}^*$ is abelian, every left coset is a right coset.
Any coset is S^1w, where $w \in \mathbb{C}^*$.

$S^1w = \{zw \mid z \in S^1\} = \{zw \mid |z| = 1\} = \{\alpha \in \mathbb{C}^* \mid |\alpha| = |w|\}$.

This is because any $\alpha \in \mathbb{C}$ s.t. $|\alpha| = |w|$ can be written as $\alpha = \alpha w^{-1} w$ (since $w \neq 0$), with $|\alpha w^{-1}| = \dfrac{|\alpha|}{|w|} = 1$, so that $\alpha w^{-1} \in S^1$.

Hence, S^1w is geometrically given by the circle in the plane with centre $(0, 0)$ and radius $|w|$. Look at Fig.3. Each of the **infinitely many** concentric circles shown in it represents a distinct coset of S^1 in $\mathbb{C}^*$.

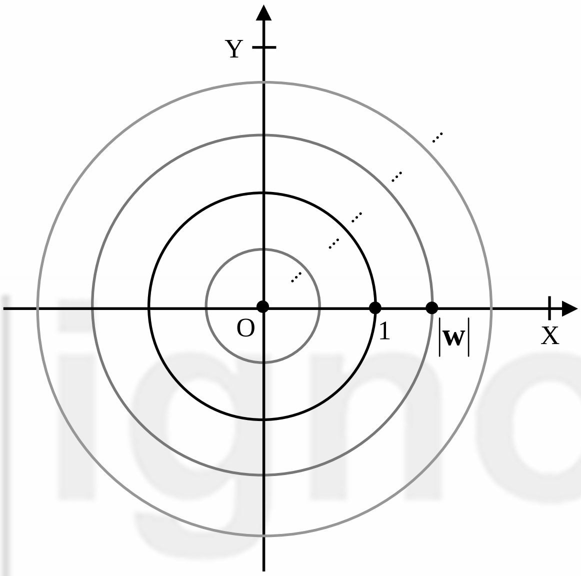

Fig.3: A geometric representation of the infinitely many cosets of S^1 in $\mathbb{C}^*$, each circle representing a coset.

E12) Since any subset of T is a subset of S, $\wp(T) \subseteq \wp(S)$. Also, you have seen in Unit 2 that both are groups w.r.t. the same operation Δ.
Hence, $\wp(T) \leq \wp(S)$.

Now let $H = \wp(T)$, then $H = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

So $H\{3\} = \{\emptyset \Delta \{3\}, \{1\}\Delta\{3\}, \{2\}\Delta\{3\}, \{1, 2\}\Delta\{3\}\}$

$= \{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Now, check that $H \cup H\{3\} = \wp(S)$.

Hence, $|\wp(S) : \wp(T)| = 2$.

E13) The right cosets of $\{e\}$ in G are $\{e\}g = \{g\} \ \forall \ g \in G$.
Hence, the number of distinct right cosets is $o(G)$.

Thus, $|G : \{e\}| = o(G)$.

E14) In E11 you have shown that S^1 has infinitely many cosets in $\mathbb{C}^*$. Hence, $|\mathbb{C}^* : S^1|$ is infinite.

E15) No. For example, $\mathbb{Z}$ is infinite but $|\mathbb{Z} : n\mathbb{Z}| = n$, is finite.

E16) Since $K \lneq H$, $o(K) \mid o(H)$ and $o(K) \neq o(H)$.

Since $H \lneq G$, $o(H) \mid o(G)$ and $o(H) \neq o(G)$.

Also $o(K) = 30$ and $o(G) = 300$.

Thus, $o(H)$ is a factor of 300 which is a multiple of 30, greater than 30 and less than 300. Hence, it can be 60 or 150.

The corresponding index would be $\frac{o(G)}{o(H)}$, i.e., $\frac{300}{60}$ or $\frac{300}{150}$, respectively, that is 5 or 2, respectively.

E17) Since $H \cap K \leq H$ and $H \cap K \leq K$, $o(H \cap K)$ is a factor of 12 and 35. But $(12, 35) = 1$. Hence, $o(H \cap K) = 1$. Hence, $H \cap K = \{e\}$.

E18) No. For instance, take $H = \langle (1\ 2\ 3\ 4) \rangle$ and $K = \langle (1\ 3)(2\ 4) \rangle$ in S_4. Then $H \cap K = K \neq \{e\}$, since $(1\ 3)(2\ 4) = (1\ 2\ 3\ 4)^2$.

E19) i) $o(S_4) = 24$. Hence, the possible orders are $2, 3, 4, 6, 8, 12$.

ii) $o(D_{10}) = 10$. Hence, the possible orders are $2, 5$.

iii) $o(Q_8) = 8$. Hence, the possible orders are $2, 4$.

iv) $o(\mathbb{M}_{2\times 3}(\mathbb{Z}_n)) = 6^n$. Hence, the possible orders are any factor of 6^n, apart from 1 and 6^n.

E20) $o(G) = 28 = 2^2 \times 7$.

Hence, for any $g \in G$ s.t. $g \neq e$, $o(g) = 2, 4, 7, 14$. Note that no $g \in G$ has order 28, since G is not cyclic.

E21) $D_8 = \{I, R, R^2, R^3, r, rR, rR^2, rR^3\}$.

Here $o(R) = 4$, $o(r) = 2$. Hence, $\langle R \rangle$ and $\langle r \rangle$ are two non-trivial proper subgroups of D_8.

E22) The converse is: If G is a finite cyclic group, G is of prime order. This is false since we have infinitely many counterexamples – $\mathbb{Z}_n$, for all composite $n \in \mathbb{N}$.

E23) Yes. Because if n is prime, then, by Theorem 6, H does not exist.

E24) No. For example, consider S_4, and $V_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Then $V_4 \leq S_4$, and V_4 is not cyclic since its non-trivial elements are all of order 2.

E25) You know that in $\mathbb{Z}_{23}$, $(\overline{3})^{\phi(23)} = \overline{1}$.

Also, from Unit 4, you know that $\phi(23) = 22$, since 23 is a prime.

So $\overline{3}^{22} = \overline{1}$. $\therefore \overline{3}^{44} = \overline{1}$.

$\therefore \overline{3}^{47} = \overline{3}^3\ \overline{3}^{44} = \overline{3}^3 = \overline{27}$.

Thus, $3^{47} \equiv 27 \,(\text{mod}\, 23) \equiv 4\,(\text{mod}\, 23)$.

Therefore, on dividing 3^{47} by 23, the remainder obtained is 4.

E26) If $(a, p) = 1$, i.e., $p \nmid a$, then $a^{\phi(p)} \equiv 1(\text{mod}\, p)$.

Since $\phi(p) = p - 1$, $a^{p-1} \equiv 1(\text{mod}\, p)$, i.e., $a^p \equiv a(\text{mod}\, p)$.

If $p \mid a$, then $a \equiv 0(\text{mod}\, p)$, and hence $a^p \equiv 0(\text{mod}\, p)$.

So, in this case too, $a^p \equiv a(\text{mod}\, p)$.

E27) $\text{Stab}(1) = \{I\}$, since each $\sigma \in G$ moves 1, except I.

Similarly, $\text{Stab}(3) = \{I\}$.

Now $\text{Orb}(1) = \{1, 2, 3, 4\} = \text{Orb}(2)$.

Hence, $o(\text{Stab}(1)) \left|\text{Orb}(1)\right| = 1 \times 4 = 4 = o(G)$, and

$o(\text{Stab}(2)) \left|\text{Orb}(2)\right| = 1 \times 4 = 4 = o(G)$.

Thus, Theorem 10 is verified for these cases.

UNIT 6

NORMAL SUBGROUPS

Structure **Page Nos.**

6.1 INTRODUCTION

In the previous unit you studied about cosets of a subgroup. In this unit we shall focus on subgroups H for which each left coset xH is some right coset Hy. Such subgroups were introduced by the great French mathematician, who died very young, Evariste Galois (pronounced *gal-waa*). These subgroups are called 'normal' subgroups.

Fig.1: Galois (1811-1832)

In Sec.6.2, you will study what a normal subgroup is. You will also look at several examples of such subgroups.

Is every subgroup a normal subgroup? How does one decide whether a subgroup is normal or not? These questions will be the focus of Sec.6.3.

If a subgroup of a group is normal, does this confer any extra 'strength' to the subgroup? Are there any useful properties that a normal subgroup has? Answers to these questions will be discussed in Sec.6.4.

As we have noted in previous units, it is important that you study this unit carefully. Only then will you be able to achieve the following learning expectations, around which this unit has been built.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a normal subgroup of a group;
- prove, and apply, the criteria for a subgroup to be normal;

- define, and give examples of, a simple group;
- prove, and apply, basic properties of normal subgroups.

6.2 WHAT IS A NORMAL SUBGROUP?

In Unit 5, you showed that a left coset of a subgroup H, aH, need not be the same as the right coset Ha. But there are certain subgroups of a group for which the right and left cosets represented by the same element are equal, for every element of the group concerned.

For instance, consider $n\mathbb{Z} \le \mathbb{Z}$. For each $m \in \mathbb{Z}$,

$n\mathbb{Z} + m = \{nr + m \mid r \in \mathbb{Z}\} = \{m + nr \mid r \in \mathbb{Z}\}$, since $+$ is commutative

$= m + n\mathbb{Z}.$

Thus, every right coset of $\mathbb{Z}$ is a left coset of $\mathbb{Z}$, with the same representative.

On the other hand, consider the non-abelian group S_3, and the subgroup $H = \{I, (1\ 2)\}$ of S_3. Then $H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$, and $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$.

Thus, $H(1\ 3) \ne (1\ 3)H$.

Through this discussion, we are leading up to the following definition.

Definition: A subgroup N of a group G is called a **normal subgroup**, or an **invariant subgroup**, of G if $Nx = xN\ \forall\ x \in G$, and we denote this by $\mathbf{N \triangleleft G}$.

For example, any group G has two normal subgroups, namely, $\{e\}$ and G itself. Can you see why?

Well, $\{e\}x = \{x\} = x\{e\}$ and $Gx = G = xG$, for any $x \in G$.

$H \ntriangleleft G$ denotes 'H is **not** a normal subgroup of G'.

Similarly, as you noted above, $n\mathbb{Z} \triangleleft \mathbb{Z}\ \forall\ n \in \mathbb{Z}$, while $H = \{I, (1\ 2)\}$ is not a normal subgroup of S_3, i.e., $H \ntriangleleft S_3$.

Let us consider other examples.

Example 1: Show that every subgroup of $\mathbb{Z}_n$ is normal in $\mathbb{Z}_n$, $n \in \mathbb{N}$.

Solution: From Unit 4, you know that if H is a subgroup of $\mathbb{Z}_n$, then $H = \overline{m}\mathbb{Z}_n$, for some $\overline{m} \in \mathbb{Z}_n$.

$= \{\overline{0}, \overline{m}, \overline{2m}, \ldots, \overline{(n-1)m}\}.$

So, for any $\overline{z} \in \mathbb{Z}_n$,

$H + \overline{z} = \{\overline{rm} + \overline{z} \mid \overline{r} \in \mathbb{Z}_n\}$

$= \{\overline{z} + \overline{rm} \mid \overline{r} \in \mathbb{Z}_n\}$, since $+$ is commutative.

$= \overline{z} + H.$

$\therefore H \triangleleft \mathbb{Z}_n.$

***

Example 1 is a special case of the fact that every subgroup of a commutative group is a normal subgroup. We will prove this later (in Corollary 1). Now let us consider some non-abelian groups.

Example 2: Check whether or not $H = \{\pm I, \pm A\}$ is normal in Q_8, the group of quaternions, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

Solution: In Example 5, Unit 5, you saw that H has exactly 2 right cosets in Q_8, H and HB, where $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Similarly, its left cosets are H and BH.

Now, since $B \notin H$, $HB \neq H$. Similarly, $BH \neq H$.

Also $Q_8 = H \cup HB = H \cup BH$ (both being disjoint unions). …(1)

Hence, $HB = Q_8 \setminus H = BH$, that is, $HB = BH$.

Now, by (1), for any $\alpha \in Q_8$, $\alpha \in H$ or $\alpha \in HB$.

Let us, now, apply Theorem 1, Unit 5.

If $\alpha \in H$, then $H\alpha = H = \alpha H$.

If $\alpha \in HB$, then $H\alpha = HB = BH = \alpha H$.

Since $Q_8 = H \cup HB$, we find that $H\alpha = \alpha H \; \forall \; \alpha \in Q_8$.

Hence, $H \lhd Q_8$.

***

Example 3: Check whether or not $H = \{I, (1\ 2)(3\ 4)\}$ is normal in S_4.

Solution: First, note that $H \leq S_4$, since $H = <(1\ \ 2)(3\ \ 4)>$.

Now $H(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 2)(3\ 4) \circ (1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 4\ 3)\}$.

Similarly, $(1\ 2\ 3)H = \{(1\ 2\ 3), (3\ 4\ 1)\}$.

Since $(2\ 4\ 3) \neq (3\ 4\ 1)$ (why?), $H(1\ 2\ 3) \neq (1\ 2\ 3)H$.

Hence, $H \ntriangleleft S_4$.

***

A word of caution here!

Remark 1: When $H \lhd G$, $Hg = gH \; \forall \; g \in G$. **This does not mean** that $hg = gh \; \forall \; h \in H$ and $g \in G$. For instance, in Example 2 above, $HB = BH$, but $AB \neq BA$, as you have seen in Unit 5, and earlier.

$Hg = gH$ means that for $h \in H$, $\exists \; h' \in H$ s.t. $hg = gh'$.

Try solving the following exercises now.

E1) Check whether or not $< r >$ and $< R_{90} >$ are normal in D_8 (see Sec.2.4.3).

E2) Show that $H = <(1\ 2\ 3)> \lhd S_3$ (see Example 4 of Unit 5).

E3) Show that any subgroup of U_{30} is a normal subgroup.

E4) Let G be a cyclic group and $H \leq G$. Check whether $H \lhd G$ or not.

E5) Let $H \leq G$ such that for each $x \in G \; \exists \; y \in G$ s.t. $xH = Hy$. Is $H \lhd G$? Why, or why not?

Before looking at more examples and non-examples of normal subgroups, let us discuss some normality tests.

6.3 CRITERIA FOR NORMAL SUBGROUPS

In the previous section, you saw that to check whether a subgroup H is a normal subgroup of G or not requires an elementwise check of Hx and xH, for each $x \in G$. Is there a better way of checking for normality? To answer this, let's consider the following conditions for a subgroup to be normal.

Theorem 1: Let H be a subgroup of a group G. The following statements are equivalent.

i) H is normal in G.

ii) $g^{-1}Hg \subseteq H \, \forall \, g \in G.$

$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$

iii) $g^{-1}Hg = H \, \forall \, g \in G.$

Proof: We will show that $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$. This will show that the three statements are equivalent, since '$\Rightarrow$' is a transitive relation on the set of all true statements (see E17, Unit 1).

$\mathbf{(i) \Rightarrow (ii):}$ Since (i) is true, $Hg = gH \, \forall \, g \in G.$ We want to prove (ii). For this, consider $g^{-1}Hg$ for $g \in G$. Let $g^{-1}hg \in g^{-1}Hg$.

Since $hg \in Hg = gH, \exists h_1 \in H$ s.t. $hg = gh_1$.

$\therefore g^{-1}hg = g^{-1}gh_1 = h_1 \in H.$

Since $g^{-1}hg$ was an arbitrary element of $g^{-1}Hg$, we conclude that $g^{-1}Hg \subseteq H$, for any $g \in G$.

$\therefore (ii)$ is true.

$\mathbf{(ii) \Rightarrow (iii):}$ Now, we know that (ii) holds, i.e., for $g \in G, g^{-1}Hg \subseteq H.$ To prove (iii), we need to show that $H \subseteq g^{-1}Hg.$

Let $h \in H$. Then

$$h = ehe = (g^{-1}g)h(g^{-1}g)$$
$$= g^{-1}(ghg^{-1})g = g^{-1}\{(g^{-1})^{-1}hg^{-1}\}g.$$

Now put $g^{-1} = x.$ Then $x \in G,$ so that $x^{-1}Hx \subseteq H,$ by (ii).

$\therefore h = g^{-1}(x^{-1}hx)g \in g^{-1}Hg.$

Since h was an arbitrary element of H, we conclude that $H \subseteq g^{-1}Hg.$

Hence, $g^{-1}Hg = H \, \forall \, g \in G.$

$\mathbf{(iii) \Rightarrow (i):}$ For any $g \in G$, we are given that $g^{-1}Hg = H.$ We want to prove that $Hg = gH.$

So, let $hg \in Hg.$

Then $hg = g(g^{-1}hg)$. Also, $g^{-1}hg \in g^{-1}Hg = H.$

$\therefore g^{-1}hg \in H.$

Thus, $hg = g(g^{-1}hg) \in gH.$

$\therefore Hg \subseteq gH.$

Similarly, you can show that $gH \subseteq Hg.$

Thus, $Hg = gH.$

$\therefore H \lhd G,$ that is, (i) is true. ■

Consider the following remark about Theorem 1, similar to Remark 1.

Remark 2: Theorem 1 says that $H \lhd G \Leftrightarrow g^{-1}Hg = H \forall g \in G.$ This **does not mean** that $g^{-1}hg = h \ \forall \ h \in H$ and $g \in G.$

For instance, in Example 2 you have seen that $H \lhd Q_8.$ Therefore, by Theorem 1, $C^{-1}HC = H,$ where $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$ But

$$C^{-1}AC = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = -A \neq A.$$

We now prove a simple result that we mentioned after Example 1. It is actually a corollary to Theorem 1. (You have proved this in E2, Unit 5, also.)

Corollary 1: Every subgroup of a commutative group is normal.

Proof: Let G be an abelian group, and $H \le G.$ For any $g \in G$ and $h \in H,$

$g^{-1}hg = (g^{-1}g)h = h \in H.$

$\therefore g^{-1}Hg \subseteq H \ \forall \ g \in G.$

Thus, $H \lhd G.$ ■

Corollary 1 says that if G is abelian then all its subgroups are normal. Is the converse true? It is not. There are non-commutative groups whose subgroups are all normal. We will give you an example that uses another criterion for normality. So we will give the example after proving this criterion. For now, let us consider an example of the application of Corollary 1.

Example 4: Let G be a cyclic group of order $10.$ How many normal subgroups does G have, and why?

Solution: Let $G = < g >,$ where $o(g) = 10.$ Then, from Unit 4, you know that the subgroups of G are $< e >, < g^2 >, < g^5 >, G.$

Since G is abelian, all these are normal in $G.$

Thus, G has 4 normal subgroups.

***

Now consider an example of applying Theorem 1.

Example 5: Let G_1 and G_2 be two groups. Check whether or not $G_1 \times \{e_2\} \lhd G_1 \times G_2,$ where e_2 is the identity of G_2 (see Sec.2.4.6, Unit 2).

Solution: Note that the direct product $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\},$ and $H = G_1 \times \{e_2\} = \{(g_1, e_2) \mid g_1 \in G_1\}.$

Consider $(g_1, g_2)^{-1}H(g_1, g_2) = (g_1^{-1}, g_2^{-1})H(g_1, g_2).$

Any element of this set is of the form $(g_1^{-1}, g_2^{-1})(g, e_2)(g_1, g_2),$ where $g \in G_1.$

Now $(g_1^{-1}, g_2^{-1})(g, e_2)(g_1, g_2) = (g_1^{-1}gg_1, g_2^{-1}e_2g_2) = (g_1^{-1}gg_1, e_2) \in G_1 \times \{e_2\} = H,$ since $g_1^{-1}gg_1 \in G_1.$

Thus, by Theorem 1(ii), $G_1 \times \{e_2\} \lhd G_1 \times G_2$.

You can, similarly, prove that $\{e_1\} \times G_2 \lhd G_1 \times G_2$, where e_1 is the identity of G_1.

***

Try solving the following exercises now.

E6) Consider the subgroup $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \,|\, \det(A) = 1\}$ of $GL_2(\mathbb{R})$ (see Example 8 of Unit 3). Using the facts, $\det(AB) = \det(A)\det(B)$ and $\det(A^{-1}) = \dfrac{1}{\det(A)}$, prove that $SL_2(\mathbb{R}) \lhd GL_2(\mathbb{R})$.

E7) Check whether or not $H = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle|\, a, b, c \in \mathbb{C} \right\}$ is a normal subgroup of $(GL_2(\mathbb{C}), \cdot)$.

E8) Check whether or nor the centre of a group G is normal in G.

E9) Let G be a group and H be an abelian subgroup of G. Is $H \lhd G$? Why, or why not?

E10) Show that $<(2\ 3)>$ is not normal in S_3.

E11) Consider the group of all diagonal matrices in $GL_2(\mathbb{R}^*)$ (see Sec.2.4.4, Unit 2), with respect to multiplication. How many of its subgroups are normal?

E12) If H is a subgroup of a group G s.t. $g^{-1}Hg = gHg^{-1}\ \forall\ g \in G$, is $H \lhd G$? Why, or why not?

In E2, you proved that $<(1\ 2\ 3)> \lhd S_3$. Did you note that $|S_3 : <(1\ 2\ 3)>| = 2$? Maybe not. But the following criterion relates this to the result in E2.

Theorem 2: Every subgroup of a group G of index 2 is normal in G.

Proof: The argument we will give here is essentially the one we gave in Example 2 to show that $HB = BH$.

Let $N \le G$ such that $|G : N| = 2$. Let the two right cosets of N be N and Nx, and the two left cosets be N and yN.

Now, $G = N \cup yN$, a disjoint union. Hence, $yN = G \setminus N$.

Similarly, $G = N \cup Nx$. Hence, $Nx = G \setminus N = yN$.

So, by E5, $Nx = xN$. Hence, $N \lhd G$. ■

Theorem 2 gives us another criterion for normality of a subgroup. We will use this criterion very often, but particularly in Unit 9 to show that, for any $n \ge 2$, S_n has a subgroup of index 2, which is therefore, a normal subgroup. For now, consider the following example that will disprove the converse of Corollary 1.

Example 6: Show that the converse of Corollary 1 is not true.

Solution: Remember, from Unit 2 of the course 'Real Analysis', that to disprove a statement, one counterexample is enough. So, consider the quaternion group Q_8, which we discussed in Example 2.

Any subgroup of Q_8 has to be of order $1, 2, 4$ or 8, by Lagrange's theorem.

The only subgroups of orders 1 and 8 are $\{I\}$ and Q_8, respectively.

You know that they are normal in Q_8.

Using Theorem 2, you can see that any subgroup of order 4 is normal in Q_8.

Further, from Unit 5 you know that any subgroup of order 2 is cyclic, and it must be generated by an element of order 2. The only such element in Q_8 is $-I$. Thus, the only subgroup of Q_8 of order 2 is $H = \{I, -I\}$.

By actual multiplication, you can see that

$g^{-1}Hg \subseteq H \ \forall \ g \in Q_8. \ \therefore H \lhd Q_8.$

Therefore, all the subgroups of Q_8 are normal.

But, you know that Q_8 is non-abelian (for instance, $AB = -BA \neq BA$).

***

Try solving some exercises now.

E13) Consider the dihedral group D_{2n}. Show that the set of rotations in D_{2n} is a normal subgroup.

E14) State the converse of Theorem 2. Further, prove or disprove it.

E15) Let $S = \{1, 2, \ldots, n\}$ and $T = \{1, 2, \ldots, n-1\}$, for $n \geq 2, n \in \mathbb{N}$. Show that $\wp(T) \lhd \wp(S)$.

E16) Let $G \leq S(X)$, for some finite set X. Let $\text{Orb}_G(x) = \{1, x\}$, where $x \in X$. Show that $\text{Stab}_G(x) \lhd G$.

So far you have seen examples of groups with non-trivial proper normal subgroups. However, not every group has such a subgroup; in fact, there are a large number of such groups. Let us define them.

Definition: A non-trivial group G is called a **simple group** if its only normal subgroups are G and $\{e\}$.

Let us consider an example.

Example 7: Let G be a group of prime order. Show that G is simple.

Solution: From Theorem 6, Unit 5, you know that G has no non-trivial proper subgroup. Hence, G has no such normal subgroup. Hence, G is simple.

***

From Example 7, you can see that there are a huge number of simple groups – all those of prime order. Now, you may wonder if every simple group is of prime order. In Unit 9, you will see a counterexample to this – an example of a simple non-abelian group of order 60. However, for abelian groups we have the following theorem.

Theorem 3: Any finite abelian simple non-trivial group must be cyclic, and of prime order.

Proof: Let G be a finite abelian simple group, with $o(G) = n > 1$.
Let $x \in G, x \neq e$. Then $< x > \leq G$.
Since G is abelian, by Corollary 1, $< x > \lhd G$.
Since $x \neq e, < x > \neq \{e\}$.
Hence, $G = < x >$, since G is simple.
Thus, G is cyclic of order n.
Let p be a prime factor of n. Then G has a subgroup H of order p, as you have seen in Unit 4.
Since G is abelian, $H \lhd G$. But G is simple. Thus, $H = G$.
Hence, $o(G) = o(H) = p$, a prime. ■

Try solving the following exercises now.

E17) For which $n \in \mathbb{N}$ is U_n simple? Why?

E18) Give an example, with justification, of two groups of the same order of which one is abelian and one non-abelian. Can either of these groups be simple? Why, or why not?

E19) Does there exist an infinite abelian simple group? Why, or why not?

E20) Is the direct product of two simple groups simple? Give reasons for your answer.

E21) Let G be a group and $n \in \mathbb{N}$. Let $H = \{g \in G \mid o(g) = n\}$. If $H \leq G$, show that $H \lhd G$. Further, give an example of a group G, where $H \not\leq G$.

E22) Let H be a proper normal subgroup of a group G s.t. $o(H) = 2$. Show that $H \leq Z(G)$.

With this we end this section on normality tests. Let us now consider some properties of normal subgroups.

6.4 PROPERTIES OF NORMAL SUBGROUPS

In Unit 3, you studied several properties of subgroups. In this section we shall see if normal subgroups satisfy similar properties.

One of the properties you discovered in Sec.3.3 was that '$\leq$' is a transitive relation. Does the same hold if '$\leq$' is replaced by '$\lhd$'? If the group is abelian, of course $\lhd$ will be transitive. (Why?) What happens if the group G is non-abelian? If $H \lhd N$ and $N \lhd G$, we know that

i) $n^{-1}hn \in H \ \forall \ n \in N$ and $h \in H$,

ii) $g^{-1}ng \in N \ \forall \ g \in G$ and $n \in N$.

From these two facts we cannot conclude that $g^{-1}hg \in H \ \forall \ g \in G$ and $h \in H.$ Thus, it is **not** necessary that $H \lhd G.$ You will study an example that shows '$\lhd$' is not transitive, in Unit 9. However, we do have the following result.

Theorem 4: Let G be a group and $H \le G, K \le H.$ If $K \lhd G,$ then $K \lhd H.$

Proof: Since $K \lhd G, g^{-1}Kg = K \ \forall \ g \in G.$ Thus, $g^{-1}Kg = K \ \forall \ g \in H.$
Hence, $K \lhd H.$ ■

By Theorem 4, you know that, for example, $SL_2(\mathbb{R}) \lhd H$ for any subgroup H of $GL_2(\mathbb{R})$ that contains $SL_2(\mathbb{R}).$

Theorem 4 will come into play in Unit 7, while discussing subgroups of quotient groups.

Try solving a related exercise now.

E23) Let G be a group and $H \lhd G.$ Let $K \le H.$ Is $K \lhd G?$ Why, or why not?

Now let us see how normal subgroups behave w.r.t. the set operations of intersection, union and product.

Theorem 5: Let H and K be normal subgroups of a group $G.$ Then $H \cap K \lhd G.$

Proof: From Unit 3, you know that $H \cap K \le G.$ To show that $H \cap K \lhd G,$ we have to show that $g^{-1}xg \in H \cap K \ \forall x \in H \cap K$ and $g \in G.$
Now, let $x \in H \cap K$ and $g \in G.$ Then $x \in H$ and $H \lhd G.$ $\therefore g^{-1}xg \in H.$
Similarly, $g^{-1}xg \in K.$ $\therefore g^{-1}xg \in H \cap K.$
Thus, $H \cap K \lhd G.$ ■

Note that the whole argument of Theorem 5 can be used to prove that **the intersection of any family of normal subgroups of G is a normal subgroup of G**.

Next, let us consider the union of two normal subgroups. From Unit 3, you know that if $H \le G, K \le G$ then $H \cup K$ need not be a subgroup of $G.$ Hence, $H \lhd G, K \lhd G$ **does not imply** that $H \cup K \lhd G,$ except in some particular cases. Which cases are these? In the following exercises, we ask you to answer this, and prove other important properties of normal subgroups.

E24) Let G be a group and $H \lhd G, K \lhd G,$ with $H \cup K \le G.$ Under what conditions on H and K is $H \cup K \lhd G?$

E25) If G is a group, $H \le G, K \lhd G,$ will $H \cap K \lhd H?$ Why, or why not?

E26) Let G_1 and G_2 be two groups, and $H \lhd G_1, K \lhd G_2.$ Is $H \times K \lhd G_1 \times G_2?$ Why, or why not?

Let us now look at the product of subgroups. Recall, from Unit 3, that if $H, K \le G,$ then $HK \le G$ iff $HK = KH.$

Now consider a group you are familiar with, D_{2n}. From Unit 4, you know that D_8 is generated by r and R_{90}, where r is a reflection in the plane. In E1 you have seen that $< R_{90} > \lhd D_8$ but $< r > \ntriangleleft D_8$. Let us now see what happens in D_{2n}, $n \ge 3$.

Example 8: Take D_{2n}, $n \ge 3$, the group you studied in Sec.2.4, Unit 2.
Let $H = < r >$ and $K = < R >$, where $R = R_\theta$, $\theta = {}^{360}\!/\!{}_{n}$.
Show that $K \lhd D_{2n}$, $H \ntriangleleft D_{2n}$ and $D_{2n} = HK$.

Solution: Let us write $r = x$ and $R = y$. Then, from Unit 4 you know that the elements of D_{2n} are of the form $x^i y^j$, where $i = 0, 1$ and
$j = 0, 1, \ldots, n-1$, $o(x) = 2$, $o(y) = n \ge 3$, and $xy = y^{-1}x = y^{n-1}x$.
$\therefore D_{2n} = \{e, x, y, y^2, \ldots, y^{n-1}, xy, xy^2, \ldots, xy^{n-1}\} = K \cup xK$, and $x \notin K$.
$\therefore |D_{2n} : K| = 2$.
Thus, by Theorem 2, $K \lhd D_{2n}$. (You have already shown this in E13.)
Note that we can't apply Corollary 1, since D_{2n} is non-abelian (as $xy = y^{-1}x$ and $y \ne y^{-1}$).
Now let us see if $H \lhd D_{2n}$.
Consider $y^{-1}xy$. Now $y^{-1}xy = xy^2$, because $y^{-1}x = xy$.
If $xy^2 \in H$, then $xy^2 = e$ or $xy^2 = x$. (Remember $o(x) = 2$, so that $x^{-1} = x$.)
If $xy^2 = e$, then $y^2 = x^{-1} = x \Rightarrow y^3 = xy = y^{-1}x \Rightarrow y^4 = x$.
Continuing in this way, a pattern emerges – for odd m, we find $y^m = y^{-1}x$, and for even m, $y^m = x$.
In either case $y^m \ne e$, since $x \ne e$ and $x \ne y$.
So $y^n \ne e$, which is a contradiction. Hence, $xy^2 \ne e$.

If $xy^2 = x$, then $y^2 = e$, a contradiction since $o(y) \ge 3$.

$\therefore y^{-1}xy = xy^2 \notin H$, and hence, $H \ntriangleleft G$.

Finally, note that $H \cap K = \{e\}$, so that $o(H \cap K) = 1$.
So, from Unit 3, we get, $o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = 2n$.
Also $o(D_{2n}) = 2n$ and $HK \subseteq D_{2n}$.
Hence, $D_{2n} = HK$.

***

What you have seen in Example 8 is that $HK = G$, so HK is a subgroup of G. Thus, $HK = KH$. Is this true whenever one of H or K is normal in G? You will find the answer while doing the following exercises about the product of subgroups.

E27) i) Prove that if $H \lhd G$ and $K \le G$, then $HK \le G$.
(**Hint:** Use Theorem 7 of Unit 3.)

ii) Prove that if $H \lhd G$, $K \lhd G$, then $HK \lhd G$. (Note that this is false if '$\lhd$' is replaced by '$\le$'.)

iii) Is the converse of (ii) above true? Give reasons for your answer.

E28) i) If H and K are normal abelian subgroups of a group, and if $H \cap K = \{e\}$, show that HK is abelian.

ii) If the condition on $H \cap K$ is removed in (i) above, will HK still be abelian? Why, or why not?

From E27(ii), you know that if H and K are normal subgroups of a group G, then HK is a normal subgroup of G. What happens when HK is the whole of G? We get a special, and very important, situation similar to the external direct product that you studied in Sec.2.4.6. To understand this situation, consider the following definition.

Definition: Let H and K be **normal** subgroups of a group G. Then G is called the **internal direct product** of H and K if
$G = HK$ and $H \cap K = \{e\}$.
We denote this fact by $\mathbf{G = H \times K}$.

Let us consider some examples.

Example 9: Consider the Klein 4-group, $K_4 = \{e, a, b, ab\}$, where $a^2 = e$, $b^2 = e$ and $ab = ba$. Show that K_4 is the internal direct product of $< a >$ and $< b >$.

Solution: Let $H = < a >$ and $K = < b >$. Then $H \cap K = \{e\}$.
Also, you can see that $K_4 = HK$.
$\therefore K_4 = H \times K$.

***

Example 10: Check whether or not $\mathbb{Z}_{10}$ is the internal direct product of its subgroups $\overline{5}\mathbb{Z}_{10}$ and $\overline{2}\mathbb{Z}_{10}$.

Solution: Let $H = \{\overline{0}, \overline{5}\}$ and $K = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$. Then

i) $\mathbb{Z}_{10} = H + K$, since any element of $\mathbb{Z}_{10}$ is the sum of an element of H and an element of K, and

ii) $H \cap K = \{\overline{0}\}$.

Thus, $\mathbb{Z}_{10} = H \times K$.

***

Both the examples above were of abelian groups. However, consider the next example, which is a generic example.

Example 11: Show that, for any two groups G_1 and G_2, $G_1 \times G_2$ is the internal direct product $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

Solution: Let $H = G_1 \times \{e_2\}$ and $K = \{e_1\} \times G_2$. You have already seen that H and K are normal in $G_1 \times G_2$.

We need to show that any element of $G_1 \times G_2$ is of the form hk, where $h \in H$ and $k \in K$.

Now, any element of $G_1 \times G_2$ is $(x, y) = (x, e_2)\,(e_1, y)$, with $(x, e_2) \in H$, $(e_1, y) \in K$.

$\therefore G_1 \times G_2 = HK$.

Now, let $(x, y) \in H \cap K$.

Since $(x, y) \in H$, $y = e_2$. Since $(x, y) \in K$, $x = e_1$.

$\therefore (x, y) = (e_1, e_2)$. $\therefore H \cap K = \{(e_1, e_2)\}$.

$\therefore G_1 \times G_2 = (G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$.

***

We would like to make a remark about terminology here.

Remark 3: Let H and K be normal subgroups of a group G. Then the internal direct product of H and K is essentially the same as the external direct product of the groups H and K. Therefore, when we talk of an internal direct product of subgroups, we often drop the word 'internal', and just say 'direct product of subgroups'.

The definition of the internal direct product of two subgroups can be extended to that of several subgroups, as you will find if you study more advanced mathematics. In fact, this concept is the basis of the algebraic structure of any finitely generated abelian group.

Now, you may ask: can every group be written as an internal direct product of two or more of its proper normal subgroups? To answer this, consider the following theorem. It gives conditions under which a group is an internal direct product of its subgroups.

Theorem 6: Let a group G be the internal direct product of its normal subgroups H and K. Then

i) each $x \in G$ can be **uniquely** expressed as $x = hk$, where $h \in H$, $k \in K$, and

ii) $hk = kh \ \forall \ h \in H, k \in K$.

Proof: We know that $G = HK$ with $H \cap K = \{e\}$.

i) Let $x \in G$. Then $x = hk$, for some $h \in H$, $k \in K$.

Now suppose $x = h_1k_1$ also, where $h_1 \in H$ and $k_1 \in K$.

Then $hk = h_1k_1$. …(2)

$\therefore h_1^{-1}h = k_1k^{-1}$.

Now $h_1^{-1}h \in H$.

Also, since $h_1^{-1}h = k_1k^{-1} \in K$, $h_1^{-1}h \in K$. $\therefore h_1^{-1}h \in H \cap K = \{e\}$.

$\therefore h_1^{-1}h = e$, which implies that $h = h_1$.

And then, by cancellation in (2), $k = k_1$.

Thus, the representation of x as the product of an element of H and an element of K is unique.

ii) The best way to show that two elements x and y commute is to show that $x^{-1}y^{-1}xy$ is identity. So, let $h \in H$ and $k \in K$, and consider $h^{-1}k^{-1}hk$.

Since $K \lhd G$, $h^{-1}k^{-1}h \in K$.

$\therefore h^{-1}k^{-1}hk \in K.$

By similar reasoning, $h^{-1}k^{-1}hk \in H$.

$\therefore h^{-1}k^{-1}hk \in H \cap K = \{e\}.$

$\therefore h^{-1}k^{-1}hk = e,$ that is, $hk = kh.$ ■

Now, a word of caution!

Remark 4: If you consider S_3, you will find that $S_3 = HK$, where $H = <(1\ 2)>, K = <(1\ 2\ 3)>$, and $H \cap K = \{I\}$. So, you may think $S_3 = H \times K$. But $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$.

So, what is not okay? $H \not\lhd S_3$.

The point is that you must make sure **every condition** of the definition is satisfied before concluding that $G = H \times K$.

Consider another observation about Theorem 6.

Remark 5: Note that Theorem 6(ii) is a very helpful tool to decide that $G \neq H \times K$. Also, note that (ii) says that elements of H commute with elements of K. It **does not** say that H is abelian, or K is abelian. For instance, in Example 11, if G_1 and G_2 are non-abelian, then so are H and K.

Let us consider an example now, to answer the question raised before Theorem 6.

Example 12: Check whether or not $\mathbb{Z}$ is a direct product of its subgroups.

Solution: Suppose $\mathbb{Z} = H \times K$, where H, K are subgroups of $\mathbb{Z}$. From Unit 3, you know that $H = <m>$ and $K = <n>$, for some $m, n \in \mathbb{Z}$.

Then $mn \in H \cap K$. Hence, $H \cap K \neq \{0\}$, unless $m = 0$ or $n = 0$.

Now, if $m = 0$, then $1 \in \mathbb{Z}$ cannot be written as hk, with $h = 0$ and $k \in K$. Similarly, if $n = 0$, we conclude that Theorem 6(i) does not hold here. Thus, we reach a contradiction.

Hence, $\mathbb{Z}$ cannot be written as a direct product of its subgroups.

***

Try solving the following exercises now.

E29) Prove a partial converse of Theorem 6, namely, if H and K are normal subgroups of G which satisfy (i) of Theorem 6, then $G = H \times K$.

E30) If G is a finite group, $H \lhd G, K \lhd G$ such that $G = H \times K$, show that $o(G) = o(H) \cdot o(K)$.

E31) Check if, in Example 2, $Q_8 = <A> \times <B>$ or not.

E32) Show that $\mathbb{R}^*$ is the internal direct product of $\mathbb{R}^+$ and $\{1, -1\}$, where $\mathbb{R}^+$ is the set of positive real numbers.

Now, as you have seen, a non-abelian group has many subgroups that are not normal. Is there some way to decide how "near" to being normal, in some sense, a subgroup is? You know that if $H \ntriangleleft G$, then $g^{-1}Hg$ is not H for at least one $g \in G$. So, if we know for how many $g \in G$, $g^{-1}Hg = H$, does this give us some meaningful measure? In this context, consider the following definition.

Definition: Let G be a group and H be a subgroup of G. The set $N(H) = \{g \in G \mid g^{-1}Hg = H\}$ is called the **normaliser of $\mathbf{H}$** in G.

Note that $\mathbf{H \triangleleft G}$ iff $\mathbf{N(H) = G}$.
Also note that $H \subseteq N(H)$, since $H \le G$.

Consider an example.

Example 13: Show that if $H = <(1\ \ 2)> \le S_3$, then $N(H) = H$.

Solution: $H = \{I, (1\ 2)\}$. You know that $H \ntriangleleft S_3$.
Here $N(H) = \{\sigma \in S_3 \mid \sigma^{-1}H\sigma = H\}$.
Firstly, $H \subseteq N(H)$.
Also, since $(1\ 3)(1\ 2)(1\ 3) = (2\ \ 3) \notin H$, $(1\ 3) \notin N(H)$.
Similarly, verify that $\sigma \notin N(H)\ \forall\ \sigma \notin H$.
Hence, $N(H) = H$.

***

So, you can see that $|G \setminus N(H)|$ gives us a measure of how far H is from being normal in G. The set $N(H)$ is actually a group, as you will now see.

Theorem 7: Let G be a group and $H \le G$. Then $H \le N(H) \le G$.

Proof: Firstly, $H \subseteq N(H)$. Thus, $H \le N(H)$.
So $e \in N(H)$.
Also, if $g \in N(H)$, then $g^{-1}Hg = H \Rightarrow (g^{-1})^{-1}Hg^{-1} = H \Rightarrow g^{-1} \in N(H)$.
Finally, if $g_1, g_2 \in N(H)$, then you should show that $g_1g_2 \in N(H)$.
Thus, $N(H) \le G$. ■

Now, the question is: Is $N(H) \triangleleft G\ \forall\ H \le G$? Does Example 13 answer this?
It does. Since $H = N(H)$ there, and $H \ntriangleleft S_3$, we see that $N(H) \ntriangleleft S_3$.
Hence, **$\mathbf{N(H)}$ need not be normal in $\mathbf{G}$**.

Try doing the following related exercises now.

E33) Prove that $H \triangleleft G$ iff $N(H) = G$.

E34) If $H \le G$, check whether or not $H \triangleleft N(H)$.

E35) If G is a group and $g \in G$, find $N(<g>)$ and $N(Z(G))$.

E36) If G is a non-trivial group and $H \leq G$, can $N(H) = \{e\}$? Why?

E37) Find $N(<r>)$, where r is a reflection in D_8.

With this we come to the end of this discussion on normal subgroups. In the next unit, we shall focus on a related concept. This concept is actually the reason for which Galois defined, and developed, the idea of normal subgroups.

Let us now summarise what we have discussed in this unit.

6.5 SUMMARY

In this unit, you have studied about the following points.

1. The definition, and examples, of a normal subgroup of a group.

2. $H \triangleleft G$ iff $g^{-1}Hg = H \ \forall \ g \in G$.

3. Every subgroup of an abelian group is a normal subgroup.

4. $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$ are normal subgroups of the direct product $G_1 \times G_2$.

5. Every subgroup of index 2 is normal, but the converse is not true.

6. The definition, and examples, of a simple group.

7. Every group of prime order is simple.

8. Every finite abelian simple non-trivial group is cyclic, of prime order.

9. If $H \triangleleft G$, then $H \triangleleft K$, where $K \leq G$ s.t. $H \subseteq K$.

10. If $H \triangleleft G$, $K \triangleleft G$, then $H \cap K \triangleleft G$.

11. If $H \triangleleft G$ and $K \leq G$, then $HK \leq G$. Further, if $K \triangleleft G$ also, then $HK \triangleleft G$.

12. The definition, and examples of the internal direct product of normal subgroups.

13. Let a group G be the internal direct product of its normal subgroups H and K. Then

    i) each $x \in G$ can be **uniquely** expressed as $x = hk$, where $h \in H$, $k \in K$, and

    ii) $hk = kh \ \forall \ h \in H$, $k \in K$.

14. The definition, examples and basic properties of the normaliser of a subgroup of a group.

6.6 SOLUTIONS / ANSWERS

E1) From Unit 4, you know that $\{r, R_{90}\}$ generates D_8, where $o(r) = 2,\ o(R_{90}) = 4$ and $rR_{90} = R_{90}^{-1}r.$

Let $H = \langle r \rangle = \{I, r\}$ and $K = \langle R_{90} \rangle = \{I, R_{90}, R_{180}, R_{270}\}.$

Then $HR_{90} = \{R_{90}, rR_{90}\}$ and $R_{90}H = \{R_{90}, R_{90}r\}.$

Since $R_{90}r \neq R_{90}$ and $R_{90}r \neq rR_{90}$, $HR_{90} \neq R_{90}H.$

Thus, $H \not\triangleleft D_8.$

Now, $KR = K = RK\ \forall\ R \in K.$

Also, you should use the Cayley table of D_8 in Unit 2 to show that $Kr = rK.$

Hence, $Kx = xK\ \forall\ x \in D_8.$

Thus, $K \triangleleft D_8.$

E2) $S_3 = \{I, (1\ 2), (1\ 3), (2,\ 3), (1\ 2\ 3), (1\ \ 3\ \ 2)\},$

$H = \{I, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}.$

Now, $\forall\ \sigma \in H, \sigma H = H = H\sigma.$

You should check that

$H(1\ 2) = (1\ \ 2)H,\ H(1\ 3) = (1\ 3)H,\ H(2\ 3) = (2\ 3)H.$

$\therefore H \triangleleft S_3.$

E3) Let $H \leq U_{30}$. From Unit 4, you know that $H = \langle \zeta^i \rangle$ for some i s.t. $o(\zeta^i)\big|30,$ where ζ is a primitive $30th$ root of unity.

Then, for any $\zeta^j \in U_{30},$

$H\zeta^j = \{\zeta^{im} \cdot \zeta^j \big| m \in \mathbb{Z}\} = \{\zeta^j \cdot \zeta^{im} \big| m \in \mathbb{Z}\} = \zeta^j H.$

Hence, $H \triangleleft U_{30}.$

E4) Let $G = \langle g \rangle$. Then, from Unit 4, you know that $H = \langle g^m \rangle$ for some $m \in \mathbb{Z}.$ Hence, as in E3, you can show that $H \triangleleft G.$

E5) Yes. Since $x \in xH,\ x \in Hy.$ So $Hx \cap Hy \neq \emptyset.$

Then, from Corollary 1, Unit 5, $Hx = Hy.$

Hence, $xH = Hx$ for each $x \in G.$ Hence, $H \triangleleft G.$

E6) For any $A \in GL_2(\mathbb{R})$ and $B \in SL_2(\mathbb{R}),$

$$\begin{aligned} \det(A^{-1}BA) &= \det(A^{-1})\ \det(B)\det(A) \\ &= \frac{1}{\det(A)}\det(A), \text{ since } \det(B) = 1. \\ &= 1. \end{aligned}$$

$\therefore A^{-1}BA \in SL_2(\mathbb{R}).$

$\therefore SL_2(\mathbb{R}) \triangleleft GL_2(\mathbb{R}),$ by Theorem 1(ii).

E7) It is not. For example, $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \in GL_2(\mathbb{C})$ and $\begin{bmatrix} 1 & 2 \\ 0 & i \end{bmatrix} \in H.$

But $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 2 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \notin H,$ which you should verify.

Hence $H \ntriangleleft GL_2(\mathbb{C})$.

E8) Let $g \in G$ and $x \in Z(G)$. Then

$g^{-1}xg = g^{-1}gx,$ since $x \in Z(G)$.

$= x \in Z(G).$

$\therefore g^{-1}Z(G)g \subseteq Z(G)\ \forall\ g \in G.$

$\therefore Z(G) \triangleleft G.$

E9) No. For example, $H = <(1\,2)>$ is an abelian subgroup of S_3.

But, as you have seen in Sec.6.2, $H \ntriangleleft G$.

E10) Since $(1\,2\,3)^{-1}(2\,3)(1\,2\,3) = (1\,2) \notin <(2\,3)>, <(2\,3)> \ntriangleleft S_3$.

E11) All, since this group is abelian (which you should verify).

E12) No. For example, take $H = <r>$ in D_8.

You have seen that $<r> \ntriangleleft D_8,$ in E1.

However, you should check that $g^{-1}Hg = gHg^{-1}\ \forall\ g \in D_8$.

E13) $D_{2n} = <r, R>,$ where $H = \{R^i \mid i = 0, 1, \ldots, n-1\}$ is the set of rotations.

Now $o(H) = n,$ since $H = <R>$. Also, $o(D_{2n}) = 2n$.

Hence, $|D_{2n} : H| = 2.$ Thus, by Theorem 2, $H \triangleleft D_{2n}$.

E14) **Converse:** If G is a group and $H \triangleleft G,$ then $|G : H| = 2$.

Consider $3\mathbb{Z}$ in $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $3\mathbb{Z} \triangleleft \mathbb{Z}$.

However, $|\mathbb{Z} : 3\mathbb{Z}| = 3,$ as you know from Unit 5.

Thus, the converse of Theorem 2 is false.

E15) You have seen earlier that $\wp(T) \leq \wp(S)$.

Now $o(\wp(T)) = 2^{n-1}$ and $o(\wp(S)) = 2^n$.

Hence $|\wp(S) : \wp(T)| = {2^n}/{2^{n-1}} = 2.$

Thus, $\wp(T) \triangleleft \wp(S)$.

E16) By Theorem 10, Unit 5, you know that $o(G) = o(\mathrm{Stab}_G(x))\,|\mathrm{Orb}_G(x)|$.

So, $o(G) = 2o(\mathrm{Stab}_G(x))$.

Hence, $|G : \mathrm{Stab}_G(x)| = 2$.

Thus, by Theorem 2, $\mathrm{Stab}_G(x) \triangleleft G$.

E17) For any prime $p,$ $|U_p| = p,$ a prime. Hence, by Example 7, U_p is simple.

Further, since U_n is cyclic, from Unit 4 you know that it will be simple only if $n = p$.

E18) For instance, $\mathbb{Z}_6$ and S_3 are both of order $6.$ Neither is simple.

In general, if G_1 and G_2 are groups of order $n,$ where G_1 is abelian and G_2 is not, then n cannot be prime. This is because every group of prime order is cyclic, and hence, abelian. Hence, by Theorem 3, G_1 cannot be simple. However, G_2 could be simple – as you will see in Unit 9.

E19) Since such a group is abelian, it will have proper cyclic subgroups, which will be normal. Hence, it won't be simple.

E20) Let G_1 and G_2 be simple groups. Then $G_1 \times \{e_2\} \triangleleft G_1 \times G_2,$ as you have seen in Example 5. Also $G_1 \times \{e_2\}$ is not trivial, since G_1 is not trivial.
Hence, $G_1 \times G_2$ is not simple.

E21) We are given that $H \leq G.$
Since $o(g^{-1}hg) = o(h) \; \forall \; g \in G, \, h \in H, \, g^{-1}hg \in H.$
Hence, $H \triangleleft G.$
If G is finite and $n \nmid o(G),$ then $H = \emptyset.$ Hence, $H \not\leq G,$ trivially.
If $n = 1,$ then $H = \{e\} \leq G.$
So, to give an example, we need to think of some $n \geq 2.$ But now, see what happens. Since $e \in G$ is of order $1,$ $e \notin H$ for any $n \geq 2.$ Hence, $H \not\leq G$ for any $n \geq 2.$

E22) Since $o(H) = 2, \, H = <h> = \{e, h\},$ where $h^2 = e.$
Since $H \triangleleft G, \, g^{-1}hg \in H \; \forall \; g \in G$ and $h \in H.$
So, for any $g \in G, \, g^{-1}hg = e$ or $g^{-1}hg = h.$
If $g^{-1}hg = e,$ then $h = e,$ a contradiction to the fact that $o(h) = 2.$
Thus, $g^{-1}hg = h,$ i.e., $hg = gh \; \forall \; g \in G.$ So $H \subseteq Z(G).$
Hence, $H \leq Z(G).$

E23) $K \leq H$ and $H \leq G.$ Thus, from Unit 3, you know that $K \leq G.$ However, K need not be normal in $G.$
For example, consider $K = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| \, a \in \mathbb{R} \right\}.$ Then you should check that $K \leq SL_2(\mathbb{R}).$ Also, you know that $SL_2(\mathbb{R}) \triangleleft GL_2(\mathbb{R}).$
Now, take $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \in GL_2(\mathbb{R})$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in K.$
Then $A^{-1}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}A \notin K,$ which you should check.
Hence, $K \not\triangleleft G.$

E24) Firstly, $H \cup K \leq G$ if and only if $H \leq K$ or $K \leq H,$ as you know from Unit 3.
So $H \cup K \leq G \Rightarrow H \cup K = H$ or $H \cup K = K.$
Thus, given that H and K are normal in $G,$ $H \cup K \triangleleft G$ iff $H \cup K \leq G,$ i.e., iff $H \leq K$ or $K \leq H.$

E25) Yes. To see why, take $x \in H \cap K$ and $h \in H.$

Now $x \in H \cap K \Rightarrow x \in H$ and $x \in K$.
So $h^{-1}xh \in H,$ since $x, h \in H.$
Also, $K \lhd G \Rightarrow h^{-1}xh \in K.$
Hence, $h^{-1}xh \in H \cap K.$
Thus, $H \cap K \lhd H.$

E26) Yes. Firstly, in Unit 3 you have seen that $H \times K \leq G_1 \times G_2$.
Next, let $(h, k) \in H \times K$ and $(g_1, g_2) \in G_1 \times G_2$. Then
$(g_1, g_2)^{-1}(h, k)(g_1, g_2) = (g_1^{-1}hg_1, g_2^{-1}kg_2) \in H \times K,$ since $H \lhd G_1$ and $K \lhd G_2$.
Hence, $H \times K \lhd G_1 \times G_2$.

E27) i) Let $hk \in HK$. Since $H \lhd G, k^{-1}hk \in H,$ say $k^{-1}hk = h'$.
Then $hk = kh' \in KH.$ Thus, $HK \subseteq KH.$
Similarly, show that $KH \subseteq HK.$
Thus, $HK = KH.$
Hence, from Theorem 7, Unit 3, you know that $HK \leq G.$

ii) Since $H \lhd G$ and $K \lhd G, HK \leq G,$ by (i) above.
Now, for any $g \in G$ and $hk \in HK,$
$g^{-1}hkg = (g^{-1}hg)(g^{-1}kg) \in HK,$ since $H \lhd G, K \lhd G.$
Thus, $HK \lhd G.$

iii) No, as you have seen in Example 8.

E28) i) Consider hk and h_1k_1 in HK.
Then consider $hkh_1k_1(hk)^{-1}(h_1k_1)^{-1}$. If we show that this is in $H \cap K,$ then $(hk)(h_1k_1) = (h_1k_1)(hk),$ i.e., HK will be abelian.
Now, $hkh_1k_1k^{-1}h^{-1}k_1^{-1}h_1^{-1}$
$= hkh_1k^{-1}k_1h^{-1}k_1^{-1}h_1^{-1},$ since K is abelian.
Since $h, kh_1k^{-1}, k_1h^{-1}k_1^{-1}, h_1^{-1} \in H, h(kh_1k^{-1})(k_1h^{-1}k_1^{-1})h_1^{-1} \in H.$
So $hkh_1k_1k^{-1}h^{-1}k_1^{-1}h_1^{-1} \in H.$
Also, $hkh_1k_1k^{-1}h^{-1}k_1^{-1}h_1^{-1}$
$= hk(h^{-1}h)h_1k_1k^{-1}(h_1^{-1}h_1)h^{-1}k_1^{-1}h_1^{-1}$
$= (hkh^{-1})hh_1k_1k^{-1}(hh_1)^{-1}h_1k_1^{-1}h_1^{-1},$ since H is abelian.
$\in K.$
Hence the result.

ii) No. For instance, consider the quaternion group Q_8, and $H = \langle A \rangle, K = \langle B \rangle$. Then $H \cap K = \{\pm I\}.$
Also, $HK = Q_8,$ which is not abelian.
Note that both H and K are normal abelian subgroups of Q_8.

E29) We know that each $x \in G$ can be expressed as $hk,$ where $h \in H$ and $k \in K.$
$\therefore G = HK.$
We need to show that $H \cap K = \{e\}.$

Let $x \in H \cap K.$

Then $x \in H$ and $x \in K.$

$\therefore xe \in HK$ and $ex \in HK.$

So, x has two representations, xe and $ex,$ as a product of an element of H and an element of $K.$ But we have assumed that each element must have **only one** such representation. So the two representations, xe and $ex,$ must coincide, that is, $x = e.$

$\therefore H \cap K = \{e\}.$

$\therefore G = H \times K.$

E30) Since G is finite, so are H and $K.$

Now $G = HK,$ with $H \cap K = \{e\}.$

So $o(G) = o(HK) = o(H) \cdot o(K),$ from Unit 3.

E31) Since $< A > \cap < B > = \{\pm I\}, Q_8 \neq < A > \times < B >.$

E32) First, verify that $\mathbb{R}^+$ and $\{1, -1\}$ are subgroups of $\mathbb{R}^*.$

Since $\mathbb{R}^*$ is abelian, they are normal subgroups.

Next, for any $r \in \mathbb{R}^*, r > 0$ or $r < 0.$

Hence, $r = \pm \left|r\right| \in < -1 > \mathbb{R}^+.$

Also, $< -1 > \cap \mathbb{R}^+ = \{1\}.$

Thus, $\mathbb{R}^* = < -1 > \times \mathbb{R}^+.$

E33) $H \triangleleft G \Leftrightarrow g^{-1}Hg = H \; \forall \; g \in G$

$\Leftrightarrow g \in N(H) \; \forall \; g \in G$

$\Leftrightarrow N(H) = G.$

E34) $N(H) = \{g \in G \mid g^{-1}Hg = H\}.$

Hence, $\forall \; g \in N(H), g^{-1}Hg = H.$ Hence, $H \triangleleft N(H).$

E35) $N(< g >) = \{x \in G \mid x^{-1}gx = g^i$ for some $i \in \mathbb{Z}\}.$

$N(Z(G)) = \{g \in G \mid g^{-1}Z(G)g = Z(G)\}.$

Since $Z(G) \triangleleft G, N(Z(G)) = G.$

E36) No. If $H = \{e\},$ then $N(H) = G \neq \{e\}.$

If $H \neq \{e\},$ then $H \leq N(H).$ Thus, $N(H) \neq \{e\}.$

E37) $< r > = \{I, r\}.$

Since $R^4 = I$ and $R^{-i}rR^i = rR^{2i}, R^{-2}rR^2 = rR^4 = r.$

So $R^2 \in N(< r >).$

Since $(rR^i)^{-1}r(rR^i) = R^{-i}rR^i = rR^{2i}, rR^2 \in N(< r >)$ also.

Also, for $i = 1, 3, R^i$ and rR^i are not in $N(< r >)$ since $rR^{2i} \notin < r >.$

So $N(< r >) = \{I, r, R^2, rR^2\}.$

UNIT 7

QUOTIENT GROUPS

Structure Page Nos.

7.1 INTRODUCTION

In this block, so far, you have studied different aspects of left and right cosets of subgroups. However, we have not discussed any binary operation on the set of cosets of a subgroup. In this unit, we will define one such operation, and see if the set is a group under this operation.

In Sec.7.2, you will see how the binary operation on a group G can be used to define a binary operation on the set of cosets of a normal subgroup of G. However, this definition doesn't work if the subgroup concerned is not normal, as you will see. Further, you will see why the set of cosets of a normal subgroup is a group with respect to this operation. We call this group a quotient group. Interestingly, normal subgroups were actually defined by Galois in a manner that the cosets would form a group.

In the next section, Sec.7.3, you will study several properties of quotient groups. These properties will help you realise the potential strength of the concept of a quotient group.

The purpose of having a unit focussed completely on quotient groups is to give you a chance to spend more time on digesting this concept. This is because many people find the idea of a quotient group not easy to grasp in the first go. Please study this unit carefully, to help you achieve the learning expectations given below.

Objectives

After studying this unit, you should be able to:

- define, and give examples of, a quotient group;

- explain why the formation of a quotient group, G/N, requires $N \triangleleft G$;
- prove, and apply, some basic properties of quotient groups.

7.2 WHEN THE COSETS FORM A GROUP

Let us begin with considering S_3 and $H = \{I, (1\ 2)\}$. The set of right cosets of H in S_3 is $A = \{H, H(1\ 3), H(2\ 3)\}$. Now, it seems natural to define an operation $*$ on A, using the composition on S_3, i.e., for $H\sigma, H\rho$ in A, define $H\sigma * H\rho = H(\sigma \circ \rho) \in A$. Is this operation well-defined? Let's see.

The way $*$ is defined, it is closed on A.
However, note that $H(1\ 3) = H(1\ 3\ 2)$ since $(1\ 3)(1\ 3\ 2)^{-1} \in H$. Similarly, $H(2\ 3) = H(1\ 2\ 3)$.
So, if $*$ were well-defined, $H(1\ 3) * H(2\ 3)$ should be $H(1\ 3\ 2) * H(1\ 2\ 3)$.
But $H(1\ 3) * H(2\ 3) = H((1\ 3) \circ (2\ 3)) = H(2\ 1\ 3) = H((1\ 2) \circ (1\ 3)) = H(1\ 3)$, since $(1\ 2) \in H$; and
$H(1\ 3\ 2) * H(1\ 2\ 3) = H((1\ 3\ 2) \circ (1\ 2\ 3)) = HI = H$.
Also $H(1\ 3) \neq H$, since $(1\ 3) \notin H$.
Hence, $*$ is not well-defined.

Now consider $K = <(1\ 2\ 3)> = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ in S_3.
Consider the operation $*$ on the set of cosets of K in S_3, given by
$K\sigma * K\rho = K(\sigma \circ \rho)\ \forall\ \sigma, \rho \in S_3$.
By definition, $*$ is closed on the set of cosets of K.
Let us see if $K\sigma_1 = K\sigma_2$ and $K\rho_1 = K\rho_2$, then is $K(\sigma_1 \circ \rho_1) = K(\sigma_2 \circ \rho_2)$ or not, for $\sigma_1, \sigma_2, \rho_1, \rho_2 \in S_3$.
Here, if $\sigma_1 \in K$ or $\rho_1 \in K$, there is nothing to check really. (Why?)
Now, if $\sigma_1 = (1\ 2)$ and $\sigma_2 = (2\ 3)$, and $\rho_1 = (1\ 3)$, $\rho_2 = (1\ 2)$, then
$\sigma_1 \circ \rho_1 \in K$, $\sigma_2 \circ \rho_2 \in K$.
So $K(\sigma_1 \circ \rho_1) = K = K(\sigma_2 \circ \rho_2)$. You will find this happening for every $\sigma_1, \sigma_2, \rho_1, \rho_2$ not in K.
Thus, in this case $*$ is well-defined.
The difference between H and K, in this context, is that $H \ntriangleleft S_3$ while $K \triangleleft S_3$.

So, it appears that if $K \triangleleft G$, then we can define a binary operation on the set of cosets of K in G with respect to which this set could possibly be a group. Let's see if this is actually so.

Let H be a normal subgroup of a group G. Then $gH = Hg$ for every $g \in G$.
Consider the set of all cosets of H in G. **We denote this set by G/H.**
(Note that since $H \triangleleft G$, we need not write 'left coset' or 'right coset', simply 'coset' is enough.)
Now, let us define $* : G/H \times G/H \to G/H : Hx * Hy = Hxy$, where xy is the product in G.
Then $*$ is closed on G/H. Let us check if $*$ is well-defined.
Let $Hx = Hx_1$ and $Hy = Hy_1$, for $x, x_1, y, y_1 \in G$. Then $xx_1^{-1} \in H$, $yy_1^{-1} \in H$.

$$\therefore (xy)(x_1y_1)^{-1} = (xy)(y_1^{-1}x_1^{-1}) = x(yy_1^{-1})x_1^{-1}$$

$$= x(yy_1^{-1})x^{-1}(xx_1^{-1}) \in H, \text{ since } xx_1^{-1}, yy_1^{-1} \in H \text{ and } H \lhd G.$$

So, $(xy)(x_1y_1)^{-1} \in H.$

$\therefore Hxy = Hx_1y_1,$ i.e., $*$ is well-defined.

So, you have seen that if $H \lhd G,$ then $*$ is a well-defined binary operation on $G/H.$ You have also seen an example to show if $H \not\lhd G,$ then $*$ is not well-defined. Thus, to ensure that $*$ is well-defined, H must be normal in $G.$

Fig.1: Hölder (1859-1937)

Before going further, consider this remark on notation.

Remark 1: We shall usually denote the operation on G/H by multiplication, unless we specify another operation.

We will now show that $(G/H, \cdot)$ is a group. This theorem is due to the German mathematician Otto Hölder, who proved it in 1889.

Theorem 1: Let H be a normal subgroup of a group $G.$ Then G/H is a group under multiplication, defined by $Hx \cdot Hy = Hxy,$ for $x, y \in G.$ The coset $H = He$ is the identity of G/H and the inverse of Hx is the coset $Hx^{-1}.$

Note that the elements of G/H are subsets of $G.$

Proof: Firstly, G/H is a non-empty set, since $H \in G/H.$

Next, by definition, multiplication is closed in $G/H.$
This multiplication is also associative, since

$$\begin{aligned}((Hx)(Hy))(Hz) &= (Hxy)(Hz)\\ &= H(xy)z\\ &= Hx(yz), \text{ as the product in } G \text{ is associative.}\\ &= (Hx)(Hyz)\\ &= (Hx)((Hy)(Hz)) \text{ for } x, y, z \in G.\end{aligned}$$

Now, if e is the identity of $G,$ then $Hx \cdot He = Hxe = Hx,$ for every $x \in G.$
Also, $He = H$ since $e \in H.$ Thus, $Hx \cdot H = Hx \ \forall \ x \in G.$

Finally, for any $x \in G, (Hx)(Hx^{-1}) = Hxx^{-1} = He = H.$

Hence, $(G/H, \cdot)$ satisfies $G1', G2', G3'$ of Unit 2. Thus, it is a group with identity $H.$ Further, the inverse of Hx is $Hx^{-1} \ \forall \ x \in G.$ ■

So, we have proved that G/H, the set of all cosets of a normal subgroup H in $G,$ is a group with respect to multiplication defined by $Hx \cdot Hy = Hxy.$ This leads us to the following definition.

Definition: Let G be a group and let $H \lhd G.$ The group $(G/H, \cdot)$ is called the **quotient group** (or **factor group**) of G by $H.$

For example, you have seen that S_3/K is a quotient group, where $K = <(1\ 2\ 3)>.$ Note that the number of elements in S_3/K is $2,$ the elements being K and $K(1\ 2).$ Thus, $o(S_3/K) = |S_3 : K|.$ In this context, consider the following observation.

Remark 2: The cardinality of G/H is the number of distinct cosets of H in G. As you know from Unit 5, this number is $|G:H|$, the index of H in G. Thus, if G/H is finite, then $o(G/H) = |G:H|$.

Hence, if G is a finite group and $H \lhd G$, then by Lagrange's theorem

$$\mathbf{o(G/H) = \frac{o(G)}{o(H)}}.$$

Now, let us consider a couple of observations related to the operation on G/H.

Remark 3: i) Note that if $H \lhd G$, $xH = Hx\ \forall\ x \in G$. So

$$(xH)\cdot(yH) = Hx \cdot Hy = Hxy = xyH \text{ in } G/H.$$

ii) If $(G, +)$ is an abelian group and $H \le G$, then you know that $H \lhd G$. In this case, the operation on G/H is defined by

$$(H + x) + (H + y) = H + (x + y).$$

Let us now look at a few examples of quotient groups.

Example 1: Obtain the group G/H, where $G = S_3$ and $H = S_3$.

Solution: Firstly, note that $S_3 \lhd S_3$. Hence, S_3/S_3 is a group. The only coset of S_3 in S_3 is S_3. Hence, the only element in this factor group is S_3, the identity element. Hence, S_3/S_3 is the trivial group.

***

What you have seen in Example 1 is true for any group. Consider the following important remark.

Remark 4: Given any group G, **G/G is the trivial group**. This is true regardless of whether G is finite or infinite, abelian or non-abelian, cyclic or non-cyclic.

Now consider an example of an infinite cyclic group, whose quotient group is a finite cyclic group.

Example 2: Show that the group $\mathbb{Z}/n\mathbb{Z}$ is of order n.

Solution: You know that $\mathbb{Z} = <1>$, an infinite cyclic group.

In Unit 5, you have seen that all the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are of the form $a + n\mathbb{Z} = \{a + kn | k \in \mathbb{Z}\}$, where $a = 0, 1, \ldots, n-1$. Thus,

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, where $\overline{i}$ denotes the coset $i + n\mathbb{Z}$.

Now, the operation in $\mathbb{Z}/n\mathbb{Z}$ is given by $\overline{a} + \overline{b} = \overline{a+b}$. Hence, for any $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{m} = \overline{1} + \overline{1} + \cdots + \overline{1}(m \text{ times}) = m \cdot \overline{1}$.

Thus, $\mathbb{Z}/n\mathbb{Z} = <\overline{1}>$, where $o(\overline{1}) = n$ since $n \cdot \overline{1} = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ and $m.\overline{1} \ne \overline{0}$ for $0 < m < n$.

So, $o(\mathbb{Z}/n\mathbb{Z}) = n$.

***

In the example above, note that the elements of $\mathbb{Z}/n\mathbb{Z}$ are precisely the congruence classes modulo n, that is, the elements of $\mathbb{Z}_n$.

Next, let us consider an example of a non-cyclic abelian group, and see if its quotient group is always non-cyclic.

Example 3: Consider the group Q_8, and its subgroup $H = \{\pm I, \pm A\}$ (of Example 2, Unit 6). Obtain the elements of Q_8/H, and the order of each element. Also obtain the Cayley table of Q_8/K, where $K = \{\pm I\}$.

Solution: In Unit 6, you have seen that $H \lhd Q_8$. In Unit 4, you have seen that Q_8 is not cyclic.

Now $o(Q_8/H) = \dfrac{o(Q_8)}{o(H)} = \dfrac{8}{4} = 2$, by Remark 2.

Hence, from Unit 4 you know that Q_8/H is cyclic, and is generated by an element of order 2.

In Example 2, Unit 6, you have also seen that $Q_8/H = \{H, HB\}$, where

$B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Here $o(H) = 1$, since H is the identity of Q_8/H.

Also $o(HB) = 2$, since $HB \cdot HB = HB^2$, and $B^2 = -I \in H$.

Thus, $Q_8/H = \langle HB \rangle$.

So, though Q_8 is non-cyclic, Q_8/H is cyclic.

Next, Q_8/K is of order 4. You should check that its distinct non-trivial elements are KA, KB, KAB, each of order 2. So, the Cayley table is as below.

$\cdot$	K	KA	KB	KAB
K	K	KA	KB	KAB
KA	KA	K	KAB	KB
KB	KB	KAB	K	KA
KAB	KAB	KB	KA	K

From the table, you can see that this is the same as the Klein 4-group (see Example 3, Unit 2).

***

Before going to the next example, consider an important remark emerging out of Example 3.

Remark 5: In Example 3, you have seen that $o(HB) = 2$. This is the order of HB as an element of the group G/H. Of course, HB is also the subset $\{\pm B, \pm AB\}$ of Q_8, which has cardinality 4. **Do not confuse this cardinality with the order of $\mathbf{HB}$, as an element of $\mathbf{Q_8/H}$.**

Let us now consider some examples where G/H is infinite.

Example 4: Show that G/H is an infinite group, where $G = GL_2(\mathbb{R})$ and $H = SL_2(\mathbb{R})$. How many elements of finite order does G/H have, and what are the possible finite orders?

Solution: You know that $SL_2(\mathbb{R}) \triangleleft GL_2(\mathbb{R})$ (see E6, Unit 6).

Any element of G/H is of the form $A \cdot SL_2(\mathbb{R})$, where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$.

Also, note that, for $A, B \in GL_2(\mathbb{R})$, $A \cdot SL_2(\mathbb{R}) = B \cdot SL_2(\mathbb{R})$ iff $B^{-1}A \in SL_2(\mathbb{R})$, i.e., iff $\det(B^{-1}A) = 1$, i.e., iff $\det A = \det B \neq 0$.

Further, for each $n \in \mathbb{Z}$, $\det\left(\begin{bmatrix} n & 0 \\ 0 & 1 \end{bmatrix}\right) = n$. Hence, there are at least as many distinct elements in G/H as there are non-zero integers. Thus, G/H is an infinite group.

Next, for $A \notin SL_2(\mathbb{R})$,

$A \cdot SL_2(\mathbb{R})$ is of finite order m

$\Leftrightarrow A^m \cdot SL_2(\mathbb{R}) = SL_2(\mathbb{R})$

$\Leftrightarrow A^m \in SL_2(\mathbb{R})$

$\Leftrightarrow (\det A)^m = 1$

$\Leftrightarrow \det A = -1$, since $A \notin SL_2(\mathbb{R})$ and $\det A \in \mathbb{R}$.

You can check that there are infinitely many matrices in $GL_2(\mathbb{R})$ with determinant (-1). For example, $\begin{bmatrix} 1 & b \\ 1 & b-1 \end{bmatrix}$ is one such type, for each $b \in \mathbb{R}$.

Further, note that

$\det A = -1 \Rightarrow \det A^2 = 1 \Rightarrow A^2 \in SL_2(\mathbb{R}) \Rightarrow o(A \cdot SL_2(\mathbb{R})) = 2.$

Thus, if $A \cdot SL_2(\mathbb{R})$ is of finite order, the order must be 1 or 2.

***

Example 5: Consider $G = \{\alpha \in \mathbb{C} \mid \alpha^m = 1 \text{ for some } m \in \mathbb{Z}\}$. Show that G is a subgroup of $\mathbb{C}^*$. Also show that $U_{10} \triangleleft G$, and find $|G : U_{10}|$.

Solution: Firstly, $G \neq \emptyset$. (Why?)

Secondly, the multiplicative identity, $1 \in G$. (Why?)

Thirdly, if $\alpha \in G$, then $\alpha^m = 1$ for some $m \in \mathbb{Z}$. So $(\alpha^{-1})^m = 1$. Thus, $\alpha^{-1} \in G$.

Finally, if $\alpha, \beta \in G$, then $\alpha^m = 1 = \beta^n$ for some $m, n \in \mathbb{Z}$.

So $(\alpha\beta)^{mn} = \alpha^{mn}\beta^{mn} = 1$. Hence, $\alpha\beta \in G$.

Thus, $G \leq \mathbb{C}^*$.

Now, $U_{10} = \{\alpha \in \mathbb{C}^* \mid \alpha^{10} = 1\} \leq \mathbb{C}^*$ and $U_{10} \subseteq G$. Thus, $U_{10} \leq G$.

Since G is abelian, $U_{10} \triangleleft G$.

Now, for each prime p s.t. $p \nmid 10$, let ζ be a primitive $p\text{th}$ root of unity. Then $\zeta U_{10} \neq U_{10}$, as $\zeta^{10} \neq 1$.

Also $\zeta_1 U_{10} = \zeta_2 U_{10}$ iff $(\zeta_1\zeta_2^{-1})^{10} = 1$, i.e., iff $\zeta_1^{10} = \zeta_2^{10}$.

So, if ζ_1 is a primitive $p_1\text{th}$ root of unity and ζ_2 is a primitive $p_2\text{th}$ root of unity, for two distinct primes p_1, p_2 not dividing 10, then $\zeta_1 U_{10} \neq \zeta_2 U_{10}$. (Here note that $o(\zeta_i^{10}) = p_i$, for $i = 1, 2$.)

Thus, $|G : U_{10}|$ is at least as large as the number of primes in $\mathbb{N}$, except for 2 and 5. Hence, it is infinite.

***

Now consider another 'finite example'.

Example 6: Obtain the orders of all the factor groups of U_{15}. Also find the distinct elements of any one non-trivial factor group.

Solution: From Unit 4, you know that the subgroups of U_{15} are $H_1 = < e >, H_2 = < \zeta >, H_3 = < \zeta^3 >,\ H_4 = < \zeta^5 >$, where ζ is a primitive 15th root of unity.

The orders of these groups are as follows:

$o(H_1) = 1, o(H_2) = 15, o(H_3) = 5, o(H_4) = 3.$

Thus, the orders of the corresponding factor groups are $o(G/H_i) = \dfrac{o(G)}{o(H_i)}$, i.e.,

$\dfrac{15}{1}, \dfrac{15}{15}, \dfrac{15}{5}, \dfrac{15}{3}$, respectively, i.e., $15, 1, 3, 5$, respectively.

Consider G/H_3 now.

Note that $o(G/H_3)$ is prime. Hence, G/H_3 is cyclic. In fact,

$G/H_3 = < \zeta H_3 > = \{H_3, \zeta H_3, \zeta^2 H_3\}.$

***

Consider the following comment related to the example above.

Remark 6: We can generalise what you have seen in Example 6 (and Example 2).

If $G = < g >$ and $H = < g^n >$, then $o(G/H) = n$, and

$\mathbf{G/H = \{H, gH, \ldots, g^{n-1}H\} = < gH >}$.

Now, another example.

Example 7: Consider D_8, and $H = < R_{90} >$. You have shown, in Unit 6, that $H \lhd D_8$. Find the elements of D_8/H.

Solution: First, $o(D_8/H) = \dfrac{8}{4} = 2$. Also, $r \notin H$, where r is a reflection in a diagonal of the square.

So $D_8/H = \{H, Hr\}$.

***

Try doing some exercises now.

E1) Let $V_4 = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \le S_4$. Show that $H = \{I, (1\ 2)(3\ 4)\} \lhd V_4$, and find $o(V_4/H)$. Also obtain two distinct elements of V_4/H, with justification.

E2) Let $S = \{a, b, c\}$ and $T = \{a, b\}$. You have shown, in Unit 6, that $\wp(T) \lhd \wp(S)$. Find the elements of $\wp(S)/\wp(T)$.

E3) Find the order of $(\bar{3} + <\bar{8}>)$ in $\mathbb{Z}_{20}/\bar{8}\mathbb{Z}_{20}$, and of $(\bar{3} + <\bar{9}>)$ in $\mathbb{Z}_{20}/\bar{9}\mathbb{Z}_{20}$.

E4) Construct the Cayley table for $5\mathbb{Z}/15\mathbb{Z}$.

E5) Give an example, with justification, of a finite group G with $H \lhd G$ and x, y in G s.t. $Hx = Hy$ in G/H but $o(x) \neq o(y)$.

E6) For any group G, determine the factor groups corresponding to G and to $\{e\}$.

E7) Let G be a group and $H \leq G$ such that $(G/H, \cdot)$ is a group, where '.' is defined as in Theorem 1. Will H be normal in G? Why, or why not?

E8) Let G be a finite group, $H \lhd G$ and $a \in G$ s.t. $o(Ha) = 3$ and $o(H) = 10$. Find all possible orders a can have.

E9) If G is a finite group and $H \lhd G$, prove that $o(Hg)$ in G/H must divide $o(g)\ \forall \in G$.

E10) Show that $\mathbb{R}/\mathbb{Z}$ has elements of every order. Does every element of $\mathbb{R}/\mathbb{Z}$ have finite order? Why?

E11) Is $\mathbb{C}/\mathbb{Q}$ a group? Why, or why not?
Further, if $\mathbb{C}/\mathbb{Q}$ is a group, give two distinct non-trivial elements of $\mathbb{C}/\mathbb{Q}$, with justification. If it isn't a group, find a non-trivial proper normal subgroup of $\mathbb{C}$.

E12) i) Let $\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$. You have seen, in Unit 2, that $\mathcal{F}$ is a group with respect to pointwise addition. Let $C = \{f : \mathbb{R} \to \mathbb{R} \mid f(r) = c\ \forall\ r \in \mathbb{R},$ where $c \in \mathbb{R}\}$ be the set of constant functions. Show that $C \lhd \mathcal{F}$. What do the elements of $\mathcal{F}/C$ look like? Is $\mathcal{F}/C$ finite or infinite? Is $\mathcal{F}/C$ abelian or non-abelian?

ii) Let $\text{Cont} = \{f \in \mathcal{F} \mid f$ is continuous on $\mathbb{R}\}$. Show that $\mathcal{F}/\text{Cont}$ is a well-defined group. Does it have an element of order 2? Why, or why not?

By now you would have developed some familiarity with quotient groups. Let us move on to look at some algebraic properties of these algebraic objects.

7.3 PROPERTIES OF QUOTIENT GROUPS

In this section we will consider questions like: do G and G/H have the same algebraic properties? For instance, if G is abelian, will its factor groups be abelian? And, conversely, if $H \lhd G$ such that G/H is abelian, will G be abelian?

Let us begin with a theorem.

Theorem 2: If G is an abelian group, then every factor group of G is abelian.

Proof: Let $H \lhd G$ and $xH, yH \in G/H$.

Then $(xH)(yH) = xyH = yxH,$ since G is abelian

$= (yH)(xH).$

Hence, G/H is abelian. ■

By Theorem 2, you know that $\mathbb{Z}/n\mathbb{Z}$ is abelian (which you already know, of course!). You now also know that $\mathbb{M}_{m\times n}(\mathbb{C})/H$ is abelian, for every subgroup H of $(\mathbb{M}_{m\times n}(\mathbb{C}), +)$.

Now, what about the converse of Theorem 2? If G/H is abelian **for some** $H \lhd G,$ must G be abelian? If G/H is abelian **for every** non-trivial normal subgroup of $G,$ must G be abelian? Think about these questions while solving the following exercises.

E13) Give an example to show that even if G/H is abelian $\forall\ H \lhd G,$ $H \neq \{e\}, G$ need not be abelian.

E14) If G is a cyclic group, must G/H be cyclic $\forall\ H \lhd G$? Further, is the converse true, i.e., if G/H is cyclic for some $H \lhd G,$ must G be cyclic? Give reasons for your answers.

E15) i) If G is a finite group, must G/H be finite $\forall\ H \lhd G$?

ii) If G is a group, $H \lhd G$ and G/H is finite, must G be finite? Give reasons for your answers.

Let us go a little further in our discussion on when G/H is abelian.

You may be surprised to know that given a group $G,$ we can always define a normal subgroup $H,$ such that G/H is abelian. Let us define this subgroup.

The commutator subgroup was introduced by the British mathematician G. A. Miller, in 1898.

Definition: Let G be a group and $x, y \in G.$

i) The element $x^{-1}y^{-1}xy$ is called the **commutator** of x and $y,$ and is denoted by **[x, y]**.

ii) The subgroup of G generated by the set of all commutators in G is called the **commutator subgroup** of $G.$ It is denoted by **[G, G]** or $\mathbf{G'}$.

For example, if G is a commutative group, then

$x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e\ \forall\ x, y \in G.\ \therefore [G, G] = \{e\}.$

In particular, if G is cyclic, then $G' = \{e\}.$

Consider the following remark about $G'.$

Remark 7: Note that the set $C=\{x^{-1}y^{-1}xy \mid x,\ y\in G\}$ **generates** $[G, G]$.

Thus, from Unit 4, you know that any element of $[G, G]$ is of the form $\prod_{i=1}^{m} a_i^{n_i}$, where $a_i = x_i^{-1}y_i^{-1}x_iy_i$ for some $x_i,\ y_i \in G$ and $n_i\in\mathbb{Z},\ m\in\mathbb{N}$.
What you must note here is that **C itself may not be a group**. So $[G, G]$ may not be C, but $[G, G] = < C >$.

Let us consider some non-trivial examples of a commutator subgroup.

Example 8: Find the commutator subgroup of S_3.

Solution: Note that, for any 2-cycle $(i\ j)$ in S_3, $(i\ j)(i\ j)=I$. So, $(i\ j)^{-1}=(i\ j)$.
Also $(1\ 2\ 3)^{-1}=(1\ 3\ 2)$.
Since $o(S_3)=6$, there are ${}^6C_2=15$ commutators in S_3, not necessarily distinct. For instance, $I^{-1}\sigma^{-1}I\sigma = I$ is a commutator. So is $(1\ 2)(1\ 3)(1\ 2)(1\ 3)=(1\ 2\ 3)$.
Another one is $(1\ 2)(1\ 2\ 3)^{-1}(1\ 2)(1\ 2\ 3)=(1\ 2)(1\ 3\ 2)(1\ 2)(1\ 2\ 3)=(1\ 3\ 2)$.
You can check that the set of commutators is $\{I, (1\ 2\ 3), (1\ 3\ 2)\}$.
Thus, $[S_3, S_3]$ is generated by $(1\ 2\ 3)$ and $(1\ 3\ 2)=(1\ 2\ 3)^2$.
Thus, $[S_3, S_3] = <(1\ 2\ 3)>$, and you know that this is normal in S_3.
Note that $S_3/[S_3, S_3]$ is of order 2, and hence is abelian.

***

Example 9: Find $[G, G]$, where $G=D_8$.

Solution: $D_8=\{I, r, R, R^2, R^3, rR, rR^2, rR^3\}$, where $R^4=I=r^2$ and $rR=R^{-1}r$.
For each $x,\ y\in D_8$, you should check that $x^{-1}y^{-1}xy=I$ or R^2.
Thus, $[G, G] = <\{I, R^2\}> = <R^2>$.
Note that $G/[G, G] = \{\bar{I}, \bar{r}, \bar{R}, \overline{rR}\}$ is the Klein 4-group, $<\bar{r}>\times<\bar{R}>$.

***

In the examples above it turns out that the set of commutators is a subgroup. However, this need not be so. You will come across such examples if, and when, you study advanced algebra.

Now, let us state the reasons for the importance of the commutator subgroup.

Theorem 3: Let G be a group. Then $[G, G]$ is a normal subgroup of G. Further, $G/[G, G]$ is commutative.

Proof: $[G, G]$ is a subgroup, by definition.
Now, for any commutator $x^{-1}y^{-1}xy$ and for any $g\in G$,
$g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg)\in[G, G]$.
Also, any element of $[G, G]$ is of the form $a=\prod_i a_i^{n_i}$, where $a_i = x_i^{-1}y_i^{-1}x_iy_i$ for some $x_i,\ y_i\in G$ and $n_i\in\mathbb{Z}$.

Hence, $g^{-1}ag = \prod_i (g^{-1}a_i g)^{n_i} \in [G, G],$ since $g^{-1}a_i g \in [G, G] \,\forall\, i.$

$\therefore [G, G] \triangleleft G.$

For proving the second part of the theorem, let us denote $[G, G]$ by $H,$ for convenience.

Now, G/H will be abelian iff $Hx \cdot Hy = Hy \cdot Hx \,\forall\, x, y \in G.$ Also,

$$\begin{aligned} Hx \cdot Hy = Hy \cdot Hx &\Leftrightarrow Hxy = Hyx \\ &\Leftrightarrow (xy)(yx)^{-1} \in H \\ &\Leftrightarrow xy\,x^{-1}y^{-1} \in H. \end{aligned}$$

Since $xy\,x^{-1}y^{-1} \in H \,\forall\, x, y \in G, Hx \cdot Hy = Hy \cdot Hx \,\forall\, x, y \in G,$

that is, G/H is abelian. ■

$[G, G]$ tells us how far, in a sense, G is from being commutative. The larger $[G, G]$ is, the further G is from being abelian.

Now, not only is $G\big/[G, G]$ abelian, you will see that $[G, G]$ is the *smallest* normal subgroup H of G that has the property that G/H is abelian.

Theorem 4: Let G be a group. If $N \triangleleft G$ such that G/N is abelian, then $[G, G] \le N.$

Proof: Since G/N is abelian, $Nx \cdot Ny = Ny \cdot Nx \,\forall\, x, y \in G.$ Thus,

$Nxy = Nyx \,\forall\, x, y \in G,$ so that $(xy)(yx)^{-1} \in N \,\forall\, x, y \in G.$

Thus, $xyx^{-1}y^{-1} \in N \,\forall\, x, y \in G.$

Hence, $[G, G] \subseteq N,$ and hence, $[G, G] \le N.$ ■

Let us see how Theorem 4 can be of help in finding the commutator subgroup of a group. We will use it for finding a shorter route than you used in Example 9, to reach the same goal.

Example 10: Find $H = [G, G],$ where $G = D_8.$

Solution: You know that $D_8 = < r, R \,|\, r^2 = I, R^4 = I, rR = R^{-1}r >.$

Now, certainly $I \in H.$ Also, $rRr^{-1}R^{-1} = R^2 \in [G, G].$

So, $< R^2 > \le [G, G].$

Since $Z(D_8) = < R^2 > = \{I, R^2\}, < R^2 >$ is normal in $G.$

Also $\bar{r}\,\bar{R} = \overline{rR} = \overline{R^{-1}r} = \overline{R^3 r} = \overline{Rr} = \bar{R}\,\bar{r}$ in $G/< R^2 >,$

so that $G/< R^2 >$ is abelian.

Hence, by Theorem 4, $[G, G] = < R^2 >.$

***

Why don't you try some exercises now?

E16) Find the commutator subgroup of $D_{10}.$

E17) Find the commutator subgroup of $G/[G, G],$ for any group $G.$

E18) Find the commutator subgroup, and the centre, of a simple

i) abelian group,

ii) non-abelian group.

E19) Find G', where $G = Q_8$.

Let us now discuss some interesting properties of the quotient group $G/Z(G)$. You know that if G is abelian, then $Z(G) = G$. So $G/Z(G)$ is the trivial group, and hence, it is abelian.

Now look at Q_8. You know that $Z(Q_8) = \{\pm I\}$. So $Q_8/Z(Q_8)$ is abelian (see Example 3). But Q_8 is non-abelian.

So if $G/Z(G)$ is abelian, we can't say if G is abelian or not. However, if $G/Z(G)$ is cyclic, it turns out that G has to be abelian, according to the following theorem.

Theorem 5: If G is a group s.t. $G/Z(G)$ is cyclic, then G is abelian.

Proof: Let $G/Z(G) = < gZ(G) >$, and let $x, y \in G$.

Then $xZ(G) = [gZ(G)]^m = g^m Z(G)$, and $yZ(G) = g^n Z(G)$, for some $m, n \in \mathbb{Z}$.

So $x \in g^m Z(G), y \in g^n Z(G)$.

Therefore, $x = g^m z_1$, $y = g^n z_2$ for some $z_1, z_2 \in Z(G)$.

Then $xy = (g^m z_1)(g^n z_2) = g^m (g^n z_1) z_2$, since $z_1 \in Z(G)$.

$$= g^{m+n} z_1 z_2 = g^{m+n} z_2 z_1 = (g^n z_2)(g^m z_1), \text{ as } z_2 \in Z(G).$$

$$= yx.$$

Hence, G is abelian. ■

Note that one way in which we can apply Theorem 5 is that if G is not abelian, then $G/Z(G)$ cannot be cyclic. Thus, for example, we know that $S_3/Z(S_3)$ is not cyclic.

Similarly, we know that $D_{2n}/Z(D_{2n})$ is not cyclic, since D_{2n} is not abelian.

Let us consider another example of the application of Theorem 5.

Example 11: Let G be a non-abelian group of order pq, where p and q are distinct primes. Then $Z(G) = \{e\}$.

Solution: Since G is non-abelian, $G \neq Z(G)$.

By Lagrange's theorem $o(Z(G)) = 1$, p or q.

If $o(Z(G))$ is p or q, a prime, then $o(G/Z(G))$ is q or p, respectively, a prime. So $G/Z(G)$ must be cyclic, which is not the case since G is not abelian.

Hence, $o(Z(G)) = 1$, that is, $Z(G) = \{e\}$.

***

From Example 11, you know, for example, that $Z(D_{2p}) = \{e\}$, where p is an odd prime.

Try solving some related exercises now.

E20) If G is a group s.t. $G/Z(G)$ is not cyclic, must G be non-abelian? Why, or why not?

E21) i) Let G be a non-abelian group of order p^3, where p is a prime. If $Z(G) \neq \{e\}$, then find $o(Z(G))$.

ii) Use (i) above to find $Z(G)$, for $G = D_8$. Hence, find the relation between $Z(D_8)$ and D_8'.

Consider a general remark here, about solution strategies.

Remark 8: E21 gives another example of many different strategies being available for finding $Z(G)$. We should use whatever is most suitable for the given conditions.

Let us now consider what the subgroups of factor groups look like. Are they at all related to the subgroups of the original group? Let's see.

Theorem 6: Let G be a group and $H \lhd G$.

i) For any subgroup K of G, $H \lhd HK$ and ${}^{HK}\!/_{H} \le {}^{G}\!/_{H}$.

ii) Conversely, any subgroup of G/H is of the form T/H, for some subgroup T of G containing H.

Proof: i) From Unit 6, you know that since $H \lhd G$, $HK \le G$ and $H \lhd HK$.

Now, let $Hx, Hy \in HK/H$, where $x, y \in HK$. Then

$(Hx)(Hy)^{-1} = Hxy^{-1} \in HK/H$, since $xy^{-1} \in HK$.

Hence, by the subgroup test, ${}^{HK}\!/_{H} \le {}^{G}\!/_{H}$.

ii) Let $S \le G/H$, and $T = \{g \in G \,|\, gH \in S\}$.

Then $e \in T$, since $H \in S$, as S is a subgroup.

Also, for $x, y \in T$, we have $xH, yH \in S$, so that $(xH)(yH)^{-1} \in S$, i.e., $(xy^{-1})H \in S$, that is, $xy^{-1} \in T$.

Hence, $T \le G$.

Next, for any $h \in H$, $hH = H \in S$. Hence $h \in T$.

Thus, $H \subseteq T$.

Since $H \lhd G$, $H \lhd T$. Thus, T/H is well-defined.

Finally, note that $gH \in S$ iff $gH \in T/H$. Thus, $S = T/H$. ■

Now that you know what the subgroups of a quotient group look like, can you guess what its normal subgroups look like? Does your answer match the following statement?

Theorem 7: If G is a group and $H \lhd G$, then any normal subgroup of G/H is of the form T/H, where $T \lhd G$ and $H \subseteq T$.

We leave the proof of this to you (see E22). ■

Now it is time to solve some exercises.

E22) Prove Theorem 7.

E23) Let G be a group. Let N be a maximal normal subgroup of $G,$ i.e., $N \lhd G, N \neq G,$ and if $H \lhd G$ s.t. $H \neq G,$ then $N \not\subset H.$
Show that G/N is a simple group.
Conversely, if N is a proper normal subgroup of G s.t. G/N is simple, then show that N is a maximal normal subgroup of $G.$

E24) Let G be a group generated by a set $S,$ and let $H \lhd G.$ Find a set of generators of $G/H.$

E25) Find all the normal subgroups, and maximal normal subgroups, of $\mathbb{Z}/n\mathbb{Z}, n \geq 2.$

E26) If G is a group and $H \lhd G,$ which of the following statements is true? Give reasons for your answers.

i) If H and G/H are abelian, so is $G.$

ii) If H and G/H are cyclic, so is $G.$

iii) If G is non-abelian, so is $G/H.$

iv) If G is a finite group and G/H contains an element of order $n,$ then G contains an element of order $n.$

E27) Construct the Cayley table of $Q_8/Z(Q_8).$ Hence decide if $Q_8/Z(Q_8)$ and $\mathbb{Z}_4$ have the same algebraic structure or not.

In E26 you have seen that though a normal subgroup H of a group $G,$ and $G/H,$ both share a certain algebraic property, it does not follow that G has the same algebraic property. However, now we shall prove a very important theorem which shows how we can sometimes use the properties that H and G/H have, to obtain a certain property of $G.$

Consider any finite abelian group, say $\mathbb{Z}_{10}.$ This is of order 10 and the primes dividing it are 2 and $5.$ Also, $\overline{5} \in \mathbb{Z}_{10}$ is of order 2 and $\overline{2} \in \mathbb{Z}_{10}$ is of order $5.$ Thus, $\mathbb{Z}_{10}$ has elements of order 2 and of order $5.$
So, the question is, does any finite abelian group have the property you have seen above for $\mathbb{Z}_{10}?$ That is, if G is a finite abelian group and $p \mid o(G), p$ a prime, will G have an element of order $p?$ It turns out that this is true. This amazing result is due to the famous French mathematician, Cauchy. To prove it, let us first prove a lemma (that is, a result required for proving the main theorem). For proving this lemma, we are going to use results you have studied in Unit 4.

Lemma 1: If G is a finite group of order $n(>1),$ then G has an element of order p for some prime s.t. $p \mid n.$

Proof: If n is a prime, then you know that G is cyclic, say $G = < x >,$ where $o(x) = n.$

So, let us assume that n is not a prime, and let $g \in G, g \neq e.$

Then you know that $o(g) = m,$ for some $m(\neq 1)$ such that $m \mid n.$

If m is a prime, then g is the element we are looking for.

If m is not a prime, let $p \mid m,$ where p is a prime. Then $m = pr,$ for some $r \in \mathbb{N}.$

So $o(g^r) = p$ and $g^r \in G.$ ■

Let us use this lemma to prove the result mentioned earlier, namely, **Cauchy's theorem for finite abelian groups**.

In fact, Cauchy's theorem is true for any finite group, whether it is abelian or not. However, we shall only prove it for abelian groups.

Theorem 8: Let G be a finite abelian group of order $n \geq 2.$ For each prime p dividing n, G has an element of order $p.$

Proof: We will prove the statement by using the strong form of the principle of mathematical induction (see Theorem $3',$ Unit 1).

Now, if $n = 2,$ then you know from Unit 4 that G is cyclic. Hence, $G = < x >,$ with $o(x) = 2,$ and 2 is the only prime factor of $2.$ So, the theorem is true for $n = 2.$

Now, assume that the theorem is true for any abelian group of order $m < n,$ where $n > 2,$ i.e., if A is an abelian group of order $m < n,$ and a prime $q \mid m,$ then A has an element of order $q.$

Now consider $G,$ a finite abelian group of order $n,$ and let $p \mid n,$ where p is a prime. By Lemma 1, G has an element x of order $q,$ for some prime $q \mid n.$

If $p = q,$ then x is the element we are looking for.

If $p \neq q,$ consider $\overline{G} = G/< x >.$ Note that $< x > \lhd G,$ since G is abelian.

Now $o(\overline{G}) = \dfrac{o(G)}{o(< x >)} = \dfrac{n}{q} < n$ and $p \mid (n/q)$ since $(p, q) = 1$ and $p \mid n.$

Thus, by induction, $\overline{G}$ has an element $g < x >$ of order $p,$

i.e., $g^p \in < x >.$ …(1)

Note that $g \neq e,$ since $o(g < x >) = p \neq 1.$

Now, either $g^p = e,$ or $g^p \neq e.$

If $g^p = e,$ then $g \in G$ of order $p,$ and we are through.

If $g^p \neq e,$ let $o(g^p) = r.$

Since $g^p \in < x >$ and $o(< x >) = q, r \mid q.$

But q is a prime. Hence, $r = q,$ i.e., $o(g^p) = q.$

$\therefore g^{pq} = e.$ $\therefore o(g) \mid pq.$ $\therefore o(g)$ is $1, p, q$ or $pq.$

Since $g \neq e, o(g) \neq 1.$

If $o(g) = p,$ we are through.

If $o(g) = q,$ then $(g < x >)^q = g^q < x > = < x >.$ Therefore, $o(g < x >) \mid q.$

But, from (1), $o(g < x >) = p,$ a prime distinct from $q.$ So we reach a contradiction. Hence, $o(g) \neq q.$

$\therefore o(g) = pq.$

Hence, from Unit 4 you know that,

$$o(g^q) = \frac{pq}{(pq, q)} = p.$$

$\therefore g^q \in G$ is of order $p.$

Thus, in all the cases, G has an element of order $p,$ i.e., the theorem is true for $n.$

Hence, by the strong form of the principle of induction, it is true for any finite abelian group. ■

In the proof above, you would have noted that we have used a property of $< x >,$ and a property of $G/< x >,$ to prove a property of $G.$ So, quotient groups can be used very gainfully in such ways also.

As an immediate corollary to Theorem 8, consider the following result.

Corollary 1: Any abelian group of order pq is cyclic, where p and q are distinct primes.

Proof: Let G be an abelian group of order $pq.$ By Cauchy's theorem $\exists\, x, y \in G$ s.t. $o(x) = p, o(y) = q.$

Now $(xy)^{pq} = (x^p)^q (y^q)^p,$ since G is abelian

$= e.$

$\therefore o(xy) \mid pq.$ Hence, $o(xy) = 1, p, q$ or $pq.$

If $o(xy) = 1,$ then $x = y^{-1}.$ $\therefore o(x) = o(y^{-1}) = o(y),$ which is a contradiction.

$\therefore o(xy) \neq 1.$

Suppose $o(xy) = p.$ Then $(xy)^p = e \Rightarrow y^p = e \Rightarrow q \mid p,$ a contradiction.

Hence, $o(xy) \neq p.$

Similarly, $o(xy) \neq q.$

Hence, $o(xy) = pq = o(G).$

$\therefore G = < xy >.$ ■

Using Theorem 8, you know that any abelian group of even order has an element of order $2.$ Similarly, you know that an abelian group of order 110 has an element of order $11,$ because of Cauchy's theorem.

Again, because of Corollary 1, you know that any abelian group of order $6,$ or $15,$ or 21 must be cyclic. These results are, therefore, extremely useful tools for studying finite groups.

Now, it's time for you to solve some related exercises.

E28) Verify Cauchy's theorem for $\wp(\{a_1, a_2, a_3\})$ and $\mathbb{Z}_4 \times \mathbb{Z}_6.$

E29) Verify Cauchy's theorem for $D_{10}/H,$ where $H = [D_{10}, D_{10}].$

E30) Prove that if G is a finite abelian group of order $n \geq 2,$ then G has a subgroup of order p for each prime p dividing $n.$

Let us stop our focussed discussion on factor groups for the time being. You will, of course, be using these algebraic objects in the next unit. You will also use similar 'quotient objects' in Blocks 3 and 4 of this course, and in the course 'Linear Algebra'.

Let us now summarise what we have discussed in this unit.

7.4 SUMMARY

In this unit, you have studied the following points.

1. The definition, and examples, of a quotient group (also called a factor group).

2. For any group G and $H \triangleleft G,$ the cardinality of G/H is $|G:H|$. In particular, if G is a finite group, then $o(G/H) = \frac{o(G)}{o(H)}.$

3. If G is an abelian group, then so is $G/H \;\forall\; H \triangleleft G.$ But the converse is not true.

4. If G is a cyclic group, then so is $G/H \;\forall\; H \triangleleft G.$ But the converse is not true.

5. For any group $G,$ the commutator subgroup $[G, G] \triangleleft G,$ and $G \big/ [G, G]$ is abelian.

6. If G is a group s.t. $G/Z(G)$ is cyclic, then G is abelian.

7. If G is a group, $H \triangleleft G, K \le G,$ then $H \triangleleft HK$ and $HK \big/ H \le G \big/ H.$ Conversely, any subgroup of G/H is of the form T/H for some subgroup T of G containing $H.$

8. Any normal subgroup of the quotient group G/H is of the form $N/H,$ where N is a normal subgroup of G containing $H.$

9. The proof, and applications, of Cauchy's theorem for finite abelian groups, the statement of which is:
   If G is a finite abelian group and p is a prime dividing $o(G),$ then G has an element of order $p.$

7.5 SOLUTIONS / ANSWERS

E1) By actual multiplication you can see that each element of V_4 is of order $2.$ Hence, $H = <(1\ 2)(3\ 4)> \le V_4.$

Since $|V_4 : H| = \frac{o(V_4)}{o(H)} = 2,$ by Theorem 2 of Unit 6, $H \triangleleft V_4.$

Two distinct cosets of H in V_4 are H and $(1\,3)(2\ 4)H.$

They are distinct since $(1\,3)(2\ 4) \notin H.$

E2) Since $\{c\} \notin \wp(T), \{c\}\wp(T) \neq \wp(T).$

Also $\left|\wp(S):\wp(T)\right| = \frac{o(\wp(S)}{o(\wp(T))} = \frac{2^3}{2^2} = 2.$

Thus, $\wp(T)$ and $\{c\}\wp(T)$ are the elements of the quotient group.

E3) Note that $o\left(\mathbb{Z}_{20}/\overline{8}\mathbb{Z}_{20}\right) = \frac{o(\mathbb{Z}_{20})}{o(\overline{8})} = \frac{20}{5} = 4.$

So $o(\overline{3} + < \overline{8} >) = 1,\ 2$ or $4.$

Since $\overline{3} \notin < \overline{8} >,$ and $2 \cdot \overline{3} = \overline{6} \notin < \overline{8} >,\ o(\overline{3}) = 4.$

So $\mathbb{Z}_{20} \big/ 8\mathbb{Z}_{20} = < \overline{3} + < \overline{8} >> .$

Now consider $o\left(\mathbb{Z}_{20}/\overline{9}\mathbb{Z}_{20}\right) = \frac{o(\mathbb{Z}_{20})}{o(\overline{9})} = \frac{20}{20} = 1,$ since $(9,\ 20) = 1.$ (This says that $\mathbb{Z}_{20} = < \overline{9} > .$)

Hence, $o(\overline{3} + \overline{9}\mathbb{Z}_{20}) = 1.$ In fact, $\overline{3} + \overline{9}\mathbb{Z}_{20} = \overline{9}\mathbb{Z}_{20},$ since $\overline{3} \in \overline{9}\mathbb{Z}_{20}.$

E4) $5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}, 15\mathbb{Z} = \{15n \mid n \in \mathbb{Z}\} \leq 5\mathbb{Z}.$

So $15\mathbb{Z} \lhd 5\mathbb{Z}.$

Now, by the division algorithm, for $n \in \mathbb{Z},$

$5n = 15q + r$ for some $q,\ r \in \mathbb{Z},\ 0 \leq r < 15.$

Since $5 \mid 5n$ and $5 \mid 15q,$ we find $5 \mid r,$ say $r = 5r',$ where $0 \leq r' < 3.$

So $\overline{5n} = \overline{5r'},$ where $r' = 0, 1$ or $2,$ going modulo 15.

Hence, $5\mathbb{Z} = 15\mathbb{Z} \cup (5 + 15\mathbb{Z}) \cup (10 + 15\mathbb{Z}).$

So $\left|5\mathbb{Z} : 15\mathbb{Z}\right| = 3.$

Thus, the Cayley table is as below:

$+$	$\overline{0}$	$\overline{5}$	$\overline{10}$
$\overline{0}$	$\overline{0}$	$\overline{5}$	$\overline{10}$
$\overline{5}$	$\overline{5}$	$\overline{10}$	$\overline{0}$
$\overline{10}$	$\overline{10}$	$\overline{0}$	$\overline{5}$

E5) Consider $G = S_3,\ H = < (1\ 2\ 3) >,\ x = (1\ 2\ 3),\ y = I.$

Then $Hx = Hy = H,$ since $x,\ y \in H.$ But $o(x) = 3,\ o(y) = 1.$

E6) Regarding $G/G,$ see Remark 4.

$G/\{e\} = \{g\{e\} \mid g \in G\} = \{\{g\} \mid g \in G\}.$ Each element of this factor group is a singleton.

Also $\{g_1\} = \{g_2\}$ iff $g_1 = g_2.$

Hence, $\left|G : \{e\}\right|$ is the cardinality of $G.$

E7) If H is a subgroup of $G,$ then the product of cosets of H is defined only when $H \lhd G.$

This is because if $Hx \cdot Hy = Hxy\ \forall\ x,\ y \in G,$ then, in particular,

$(Hx^{-1})(Hx) = Hx^{-1}x = He = H\ \forall\ x \in G.$

Therefore, for any $h \in H,\ x^{-1}hx = ex^{-1}hx \in (Hx^{-1}) \cdot (Hx) = H.$

That is, $x^{-1}Hx \subseteq H$ for any $x \in G$.
$\therefore H \lhd G$.

E8) Since $o(Ha) = 3$, $a^3 \in H$ but $a \notin H$, $a^2 \notin H$.

Since $o(H) = 10$, $(a^3)^{10} = 1$, i.e., $a^{30} = 1$. So $o(a) \mid 30$.

Thus, $o(a)$ can be $1, 2, 3, 5, 6, 10, 15$ or 30.

However, $o(a) \neq 1$, since $a \neq e$ as $a \notin H$.

Again, $o(a) \neq 2$, since $a^2 = e$ would mean $a^2 \in H$; but $a^2 \notin H$.

Similarly, if $o(a) = 5$, then $a^5 = e$. So $(Ha)^5 = H$, i.e., $Ha^2 = H$, as $Ha^3 = H$. So $a^2 \in H$, again a contradiction. So $o(a) \neq 5$.

In this way you should check that $o(a) \neq 10$.

Hence, $o(a) = 3, 6, 15$ or 30.

E9) Let $o(g) = r$ and $o(Hg) = m$.

Since $g^r = e$, $(Hg)^r = H$. Thus, $m \mid r$.

E10) For each $n \in \mathbb{N}$, $\frac{1}{n} \in \mathbb{R}$ s.t. $\frac{1}{n} + \mathbb{Z}$ has order n.

Hence, $\mathbb{R}/\mathbb{Z}$ has elements of order $n \; \forall \; n \in \mathbb{N}$.

However, every element of $\mathbb{R}/\mathbb{Z}$ is not of finite order.

For instance, consider $\sqrt{2} + \mathbb{Z}$. There is no $n \in \mathbb{N}$ s.t. $n\sqrt{2} \in \mathbb{Z}$.

E11) Verify that $\mathbb{Q} \leq \mathbb{C}$. Hence, $\mathbb{Q} \lhd \mathbb{C}$. Hence, $\mathbb{C}/\mathbb{Q}$ is a group.

Consider $\sqrt{2} + \mathbb{Q}$ and $i + \mathbb{Q}$. Since $\sqrt{2} - i \notin \mathbb{Q}$, these elements are distinct. Since $\sqrt{2} \notin \mathbb{Q}$ and $i \notin \mathbb{Q}$, these are non-trivial elements of the factor group.

E12) i) Verify that if $f, g \in C$, then $f - g \in C$. So $C \leq \mathcal{F}$.

Since $\mathcal{F}$ is abelian, $C \lhd \mathcal{F}$.

$\mathcal{F}/C = \{f + C \mid f \in \mathcal{F}\}$.

For $f_1, f_2 \in \mathcal{F}$, $f_1 + C = f_2 + C$ iff $f_1 - f_2$ is a constant function.

Now, for each $n \in \mathbb{N}$, define $f_n \in \mathcal{F}$ by $f_n(r) = nr^2 \; \forall \; r \in \mathbb{R}$.

Then $f_n + C \neq f_m + \mathbb{C}$ for $n \neq m$.

Hence, there are at least as many cosets of C in $\mathcal{F}$ as the number of elements in $\mathbb{N}$, which is infinite. Hence, $\mathcal{F}/C$ is infinite.

Next, you should check that $\mathcal{F}/C$ is abelian.

ii) Since $f, g \in \mathrm{Cont} \Rightarrow f - g \in \mathrm{Cont}$, $\mathrm{Cont} \lhd \mathcal{F}$.

Hence, $\mathcal{F}/\mathrm{Cont}$ is well-defined.

Now, for any $f \in \mathcal{F}$ s.t. f is not continuous, $f + f = 2f$ cannot be continuous, as you know from the course, Calculus.
Hence, Cont has no element of order 2.

E13) Consider $G = Q_8$, the quaternion group.

You know that $H \lhd G \; \forall \; H \leq G$. Also $o(Q_8/H)$ is 2 or 4.

If $o(Q_8/H)$ is 2, then Q_8/H is cyclic.

Also, Q_8/H is of order 4 only for $H=\{\pm I\}.$ And then, from Example 3, you know that Q_8/H is abelian.

Hence, Q_8/H is abelian $\forall\ H \lhd G,\ H \neq \{e\}.$

But Q_8 is not abelian.

E14) Let $G=<x>$ and G/H be a quotient group of $G.$ Any element of G/H is of the form $Hx^n=(Hx)^n,$ since any element of G is of the form $x^n.$

$\therefore G/H=<Hx>.$ Thus, G/H must be cyclic.

From E13, you know that $Q_8/<A>$ is cyclic, but Q_8 is not cyclic. So the converse is not true.

E15) i) Let $G=\{g_1, g_2,\ldots,g_n\}.$ Then $G/H=\{Hg_i | i=1,\ldots n\}.$ Hence, G/H is finite.

ii) No. For example $\mathbb{Z}/n\mathbb{Z},$ is finite, but $\mathbb{Z}$ is not.

E16) $D_{10}=<r, R | r^2=I, R^5=I, rR=R^{-1}r>.$

You know that $<R> \lhd D_{10}$ and $D_{10}/<R>$ is abelian.

Hence, by Theorem 4, $D'_{10} \leq <R>.$

Also $[r, R^3]=R.$ Hence, $R \in D'_{10}.$

Thus, $D'_{10}=<R>.$

E17) Let us write $[G, G]=H.$ By Theorems 2 and 3, $[G/H]'=\{H\}.$

E18) i) If G is abelian, then $Z(G)=G$ and $G'=\{e\},$ regardless of whether G is simple or not.

ii) If G is non-abelian, $Z(G)\neq G$ and $G'\neq\{e\}.$ Since G is simple and $Z(G)\lhd G, G'\lhd G,$ we must have $Z(G)=\{e\}$ and $G'=G.$

E19) Since every subgroup of Q_8 is normal in Q_8 and Q_8/H is abelian $\forall\ H \leq Q_8, H\neq\{e\}, Q'_8$ has to be the smallest of these, by Theorem 4. Hence, $Q'_8=\{\pm I\}.$

E20) Yes. If G is abelian, then $Z(G)=G,$ and hence, $G/Z(G)$ is trivially cyclic.

E21) i) $o(Z(G))=p$ or $p^2,$ by Lagrange's theorem, since $G\neq Z(G).$ If $o(Z(G))=p^2,$ then $o\big(G/Z(G)\big)=p.$ Hence, $G/Z(G)$ is cyclic, so that G is abelian, a contradiction. Thus, $o(Z(G))\neq p^2.$ Hence, $o(Z(G))=p.$

ii) By (i), $o(Z(G))=2.$ We know that $I\in Z(G)$ and $r\notin Z(G)$ (since $rR\neq Rr$). The only other element of order 2 in G is $R^2.$ Hence, $Z(G)=\{I, R^2\}=<R^2>.$

Thus, from Example 10, $Z(G) = G'$ in this case.

E22) Let $N \lhd G/H$. Then $N = T/H$ for some $T \le G, H \subseteq T,$ by Theorem 6.
Now, for any $t \in T, Ht \in N$.
So, for $g \in G, (Hg)^{-1}(Ht)(Hg) \in N,$ i.e., $H(g^{-1}tg) \in T/H,$ i.e., $g^{-1}tg \in T.$
Hence, $T \lhd G.$
Thus, $N = T/H,$ where $T \lhd G, H \subseteq T.$

E23) Suppose $S \lhd G/N.$ Then $S = T/N$ for some $T \lhd G, N \subseteq T.$
Since N is maximal, $T = G$ or $T = N.$ Hence, $S = \{\bar{e}\}$ or $S = G/N,$ that is, G/N is simple.

Conversely, if G/N is simple and $S \lhd G,$ s.t. $N \subseteq S,$ then by Theorem 7, $S/N \lhd G/N.$ Hence, $S/N = \{\bar{e}\}$ or $S/N = G/N.$
Thus, $S = N$ or $S = G,$ that is, N is a maximal normal subgroup of $G.$

E24) $G = <S> = \left\{ \prod_{i=1}^{r} s_i^{n_i} \middle| s_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{N} \right\}.$

So $G/H = \left\{ \prod_{i=1}^{r} (Hs_i)^{n_i} \middle| s_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{N} \right\}.$

Thus, $G/H = <\{Hs | s \in S\}>.$

E25) Since $\mathbb{Z}/n\mathbb{Z}$ is abelian, every subgroup is a normal subgroup. By Theorem 7, any normal subgroup is of the form $m\mathbb{Z}/n\mathbb{Z},$ where $n\mathbb{Z} \subseteq m\mathbb{Z},$ i.e., $m | n.$

By E23, a maximal normal subgroup will be of the form $p\mathbb{Z}/n\mathbb{Z},$ where $p | n, p$ a prime.

E26) i) False. For example $D_8/<R>$ is abelian, and $<R>,$ being cyclic, is abelian, but D_8 is not abelian.

ii) False. The same example as in (i) is a counterexample. (Why?)

iii) False. Again, D_8 is a counterexample. (Why?)

iv) True. Let $Hx \in G/H$ s.t. $o(Hx) = n.$ Then, by E9, $n | o(x).$ Let $o(x) = mn, m \in \mathbb{N}.$
Then, from Unit 4, you know that $o(x^m) = n,$ and $x^m \in G.$

E27) $Q_8 = \{\pm I, \pm A, \pm B, \pm C\},$ where $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$

$C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = AB$ and $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$

Since $AB \neq BA$, $AC \neq CA$, $Z(Q_8) = \{\pm I\}$.

So $Q_8/Z(Q_8) = \{\bar{I}, \bar{A}, \bar{B}, \overline{AB}\}$.

The Cayley table is as given in Example 3.

Thus, $Q_8/Z(Q_8)$ has no element of order 4. Hence, it is not cyclic. On the other hand, $\mathbb{Z}_4 = <\bar{1}>$ is cyclic.

Thus, $Q_8/Z(Q_8)$ and $\mathbb{Z}_4$ have different algebraic structures.

E28) Let $X = \{a_1, a_2, a_3\}$. Then $o(\wp(X)) = 8$. The only prime dividing 8 is 2. Now, for any $Y \subseteq X$, $Y \neq \emptyset$, $Y \Delta Y = \emptyset$. Thus, $o(Y) = 2$. Hence, every non-zero element of $\wp(X)$ is of order 2.

$o(\mathbb{Z}_4 \times \mathbb{Z}_6) = o(\mathbb{Z}_4) \cdot o(\mathbb{Z}_6) = 24$. The primes concerned are 2 and 3. Then $(\bar{2}, \bar{0})$ and $(\bar{0}, \bar{2})$ are of orders 2 and 3, respectively, because

$$\begin{aligned} 2(\bar{2}, \bar{0}) &= 2(2+4\mathbb{Z}, 0+6\mathbb{Z}) \\ &= (4+4\mathbb{Z}, 0+6\mathbb{Z}) \\ &= (0+4\mathbb{Z}, 0+6\mathbb{Z}) \\ &= (\bar{0}, \bar{0}) \end{aligned}$$

(Note that the first element in $(\bar{0}, \bar{0})$ is the zero of $\mathbb{Z}_4$, and the second is the zero of $\mathbb{Z}_6$.)

Similarly, $3(\bar{0}, \bar{2}) = 3(0+4\mathbb{Z}, 2+6\mathbb{Z}) = (0+4\mathbb{Z}, 6+6\mathbb{Z}) = (\bar{0}, \bar{0})$.

E29) You have seen, in E16, that $D'_{10} = <R>$. Hence, D_{10}/D'_{10} is of order 2, and is generated by an element of order 2, $\bar{r}$. Thus, Cauchy's theorem is verified.

E30) By Cauchy's theorem, $\exists\, x \in G$ s.t. $o(x) = p$.
Then $H = <x>$ is a subgroup of G of order p.

UNIT 8

GROUP HOMOMORPHISMS

Structure　　Page Nos.

8.1 INTRODUCTION

So far, in this course, we have not discussed functions from one group to another. As you have seen in the course, Calculus, there can be many different functions from a set G_1 to a set G_2. In this unit, we will study functions from a group $(G_1, *_1)$ to a group $(G_2, *_2)$ which preserve certain algebraic properties of G_1.

In Sec.8.2, we will discuss various properties of those functions between groups which preserve the algebraic operation of their domain groups. These functions are called group homomorphisms, a term introduced by the mathematician Klein in 1893. While studying them, you will often need to refer to what you have studied in Units 6 and 7. So it may be useful to quickly review those units before studying this unit.

In Sec.8.3, we will introduce you to a very important mathematical idea, an isomorphism. You will see that an isomorphism is a bijective homomorphism. The importance of isomorphisms lies in the fact that two groups are isomorphic if and only if they have exactly the same algebraic properties.

In Sec.8.4, we will prove a very basic theorem of group theory, namely, the Fundamental Theorem of Homomorphism. You will also study some of its important consequences in this section. This theorem was formulated, in its most general form, by the 'Mother of Algebra', Emmy Noether, in 1827. However, for groups specifically, it seems to have first been published some years later, in a textbook on abstract algebra by the mathematician, Van der Waerden.

Finally, in Sec.8.5, we will discuss automorphisms, which are isomorphisms of a group onto itself. We shall look at a certain subgroup of automorphisms, in particular. As you will see, this subgroup allows us to have an insight into the structure of the quotient group of G by its centre, for any group G.

The concepts of 'homomorphism' and 'isomorphism' are crucial for understanding group theory. You will study analogous concepts in Block 3, as well as in the course, Linear Algebra. So it is important for you to be clear about these concepts. This requires you to work towards achieving the following learning expectations, around which this unit is built.

Objectives

After studying this unit, you should be able to

- check whether a function between groups is a homomorphism or not;
- obtain the kernel and image of any homomorphism;
- check whether a function between groups is an isomorphism or not;
- state, prove and apply the Fundamental Theorem of Homomorphism for groups;
- state, prove and apply the second and third isomorphism theorems for groups;
- prove, and apply, some important properties of the set of automorphisms of a group.

8.2 HOMOMORPHISMS

Let us start our discussion of functions from one group to another with an example. Consider the Cayley tables of $\mathbb{Z}_4 = <\overline{1}>$ and of $U_4 = <i>, i = \sqrt{-1}.$

Table 1: Cayley table of $\mathbb{Z}_4$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Table 2: Cayley table of U_4

$\bullet$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Now, consider $f: \mathbb{Z}_4 \to U_4 : f(\overline{m}) = i^m$. Look at the following table, Table $1'$, where every entry $\overline{a}+\overline{b}$ of Table 1 is replaced by $f(\overline{a}+\overline{b})$. (Note that Table $1'$ is **not** an operation table. In it we are just showing $f(\overline{x})$ for the corresponding $\overline{x}$ in Table 1.)

Table $1'$: Each entry $\mathbf{x}$ of Table 1 replaced by $\mathbf{f(x)}$

	$f(\overline{0})$	$f(\overline{1})$	$f(\overline{2})$	$f(\overline{3})$
$f(\overline{0})$	$f(\overline{0})$	$f(\overline{1})$	$f(\overline{2})$	$f(\overline{3})$
$f(\overline{1})$	$f(\overline{1})$	$f(\overline{2})$	$f(\overline{3})$	$f(\overline{0})$
$f(\overline{2})$	$f(\overline{2})$	$f(\overline{3})$	$f(\overline{0})$	$f(\overline{1})$
$f(\overline{3})$	$f(\overline{3})$	$f(\overline{0})$	$f(\overline{1})$	$f(\overline{2})$

Next, consider Table $2'$, the Cayley table for $\{f(\bar{0}), f(\bar{1}), f(\bar{2}), f(\bar{3})\}$ with respect to multiplication.

Table $2'$: Operation table for $(\{f(\bar{0}), f(\bar{1}), f(\bar{2}), f(\bar{3})\}, \cdot)$

$\cdot$	$f(\bar{0})$	$f(\bar{1})$	$f(\bar{2})$	$f(\bar{3})$
$f(\bar{0})$	$f(\bar{0})\cdot f(\bar{0})$	$f(\bar{0})\cdot f(\bar{1})$	$f(\bar{0})\cdot f(\bar{2})$	$f(\bar{0})\cdot f(\bar{3})$
$f(\bar{1})$	$f(\bar{1})\cdot f(\bar{0})$	$f(\bar{1})\cdot f(\bar{1})$	$f(\bar{1})\cdot f(\bar{2})$	$f(\bar{1})\cdot f(\bar{3})$
$f(\bar{2})$	$f(\bar{2})\cdot f(\bar{0})$	$f(\bar{2})\cdot f(\bar{1})$	$f(\bar{2})\cdot f(\bar{2})$	$f(\bar{2})\cdot f(\bar{3})$
$f(\bar{3})$	$f(\bar{3})\cdot f(\bar{0})$	$f(\bar{3})\cdot f(\bar{1})$	$f(\bar{3})\cdot f(\bar{2})$	$f(\bar{3})\cdot f(\bar{3})$

If you put the value of $f(\bar{m})$ in Table $2'$, for $m = 0, 1, 2, 3,$ you find that it is the same as Table 2. Also, on comparing the entries of Tables $1'$ and $2'$, you can see that $f(\bar{a}+\bar{b}) = f(\bar{a})\cdot f(\bar{b})\ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_4$.

Hence, we conclude that $f(\bar{a}+\bar{b}) = f(\bar{a})\cdot f(\bar{b})\ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_4$.

Now consider the Cayley table of $K_4 = \{e, a, b, ab\}$, the Klein 4-group.

Table 3: Cayley table of K_4

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Consider $g : \mathbb{Z}_4 \to K_4 : g(\bar{0}) = e, g(\bar{1}) = a, g(\bar{2}) = b, g(\bar{3}) = ab,$ and go through the same process as for f above. You would note that, for example,
$g(\bar{1}+\bar{1}) = g(\bar{2}) = b.$

Now $\bar{1}+\bar{1}$ is at the intersection of the 2nd row and the 2nd column of Table 1, but the element in the corresponding position in Table 3 is e, not b. So,
$g(\bar{1}+\bar{1}) \neq g(\bar{1})\cdot g(\bar{1}).$

These examples lead us to the following definitions.

Definitions: i) We say that a function f from a group $(G_1, *_1)$ to a group $(G_2, *_2)$ **preserves the operation** if $f(x *_1 y) = f(x) *_2 f(y)\ \forall\ x, y \in G_1$. Such a function is called a **group homomorphism** (or simply, a **homomorphism**).

ii) A homomorphism from a group G to itself is called an **endomorphism.**

iii) A group homomorphism that is injective is called a **monomorphism**.

iv) A group homomorphism that is surjective is called an **epimorphism**.

The word 'homomorphism' is derived from the two Greek words 'homos', meaning 'like' or 'similar', and 'morphe', meaning 'form' or 'structure'.

For example, $f : \mathbb{Z}_4 \to U_4$ (given above) is a group homomorphism, while $g : \mathbb{Z}_4 \to K_4$ is not.

Further, from Tables $1, 1'$ and $2,$ you should verify that f is 1-1 and onto. Hence, f is a monomorphism as well as an epimorphism.

Let us consider another example.

Example 1: Consider the groups $(\mathbb{Z}, +)$ and $(\{1, -1\}, \cdot)$. Let us define

$$f:\mathbb{Z}\to\{1, -1\}: f(n)=\begin{cases}1, & \text{if } n \text{ is even}\\ -1, & \text{if } n \text{ is odd,}\end{cases} \quad \text{and}$$

$$g:\mathbb{Z}\to\{1, -1\}: g(n)=\begin{cases}1, & n\geq 0\\ -1, & n<0.\end{cases}$$

Show that f is a group homomorphism, but g is not. Is f a monomorphism? Is f an epimorphism? Give reasons for your answers.

Solution: If a and b are both even, or both odd, then $a+b$ is even.
So, in these cases $f(a+b)=1=f(a)\cdot f(b).$
If a is odd and b is even, then $a+b$ is odd. So $f(a+b)=-1=f(a)\cdot f(b).$
Similarly, if a is even and b is odd, $f(a+b)=f(a)\cdot f(b).$
Thus, f preserves the operation in all cases.
Hence, $f(a+b)=f(a)\cdot f(b)\ \forall\ a, b\in\mathbb{Z}.$

Now, $f(2)=f(4)=1,$ and $2\neq 4.$ So f is not 1-1, i.e., f is not a monomorphism.
Since $f(0)=1$ and $f(1)=-1,$ f is surjective. Hence, f is an epimorphism.

Next, if $a=2, b=-2,$ then $g(a+b)=g(0)=1.$ But $g(a)\cdot g(b)=(1)(-1)=-1.$
So $g(a+b)\neq g(a)g(b)$ in this case.
Thus, g is not a group homomorphism.

***

Consider the following general remark that is related to the example above.

Remark 1: To show that a function h from a group G_1 to a group G_2 is **not** a homomorphism, it suffices to show one pair of elments $a, b\in G$ s.t. $h(ab)\neq h(a)h(b).$

Before discussing more examples, let us define two key sets related to a given homomorphism.

Definition: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups and $f:G_1\to G_2$ be a homomorphism. Then

i) the **image of $\mathbf{f}$** (also called **the homomorphic image of $\mathbf{G_1}$**) is defined to be the set $\mathbf{Im\,f}=\{f(x)\mid x\in G_1\}.$

ii) the **kernel of $\mathbf{f}$** is defined to be the set $\mathbf{Ker\ f}=\{x\in G_1\mid f(x)=e_2\},$ where e_2 is the identity of $G_2.$

Note that $\operatorname{Im} f\subseteq G_2,$ and $\operatorname{Ker} f = f^{-1}(\{e_2\})\subseteq G_1.$

As you will see later, the image and kernel of a homomorphism help us understand the homomorphism's behaviour.

Now let us consider some more examples of homomorphisms.

Example 2: Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot).$ Show that the map $\exp:(\mathbb{R}, +)\to(\mathbb{R}^*, \cdot):\exp(r)=e^r$ is a group homomorphism. Also find $\operatorname{Im}\exp$ and $\operatorname{Ker}\exp.$

Solution: First, let us check that $\exp$ is well-defined. If $r_1 = r_2$ in $\mathbb{R}$, then $e^{r_1} = e^{r_2}$ in $\mathbb{R}^*$, i.e., $\exp(r_1) = \exp(r_2)$. Hence, $\exp$ is well-defined.

Now, for any $r_1, r_2 \in \mathbb{R}$, you know that $e^{r_1+r_2} = e^{r_1} \cdot e^{r_2}$.

$\therefore \exp(r_1 + r_2) = \exp(r_1) \cdot \exp(r_2)$.

Hence, $\exp$ is a homomorphism from the additive group of real numbers to the multiplicative group of non-zero real numbers.

Now, $\text{Im } \exp = \{\exp(r) \mid r \in \mathbb{R}\} = \{e^r \mid r \in \mathbb{R}\} = \mathbb{R}^+$, the group of positive real numbers.

Also, $\text{Ker } \exp = \{r \in \mathbb{R} \mid e^r = 1\}$, since 1 is the identity in $(\mathbb{R}^*, \cdot)$.

$= \{0\}$.

Note that $\exp$ takes the identity 0 of $\mathbb{R}$ to the identity 1 of $\mathbb{R}^*$. The function $\exp$ also carries the additive inverse $(-r)$ of r to the multiplicative inverse e^{-r} of $\exp(r)$.

***

Example 3: Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$. Define $f : (\mathbb{C}, +) \to (\mathbb{R}, +)$ by $f(x + iy) = x$, the real part of $x + iy$. Show that f is a homomorphism. What are $\text{Im } f$ and $\text{Ker } f$?

Solution: First, is f well-defined? You should check that it is.

Next, take any two elements $a + ib$ and $c + id$ in $\mathbb{C}$. Then,

$f((a + ib) + (c + id)) = f((a + c) + i(b + d)) = a + c = f(a + ib) + f(c + id)$.

Therefore, f is a group homomorphism.

$\text{Im } f = \{f(x + iy) \mid x, y \in \mathbb{R}\} = \{x \mid x \in \mathbb{R}\} = \mathbb{R}$.

So, f is a surjective function.

$\text{Ker } f = \{x + iy \in \mathbb{C} \mid f(x + iy) = 0\} = \{x + iy \in \mathbb{C} \mid x = 0\}$

$= \{iy \mid y \in \mathbb{R}\}$

$= i\mathbb{R}$, the set of purely imaginary numbers and 0.

Note that f carries the additive identity of $\mathbb{C}$ to the additive identity of $\mathbb{R}$ and $(-z)$ to $-f(z)$, for any $z \in \mathbb{C}$.

***

Example 4: Check whether or not the following functions are group homomorphisms from G_1 to G_2. For any function that is so, further decide whether or not it is a monomorphism and/or an epimorphism.

i) $f : \mathbb{Z} \to \mathbb{M}_3(\mathbb{R}) : f(m) = \begin{bmatrix} m & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & m \end{bmatrix}$,

ii) $f : D_8 \to \mathbb{Z}_8 : f(r) = \overline{1},\ f(R_{90}) = \overline{2},\ f(I) = \overline{0}$, where $D_8 = < r, R_{90} >$,

iii) $f : \mathbb{C}^* \to \mathbb{R}^* : f(z) = |z|$.

Solution: For each of the functions given above, you must first check that it is well-defined.

i) Here $f(r+s)=\begin{bmatrix} r+s & 0 & 0 \\ 0 & r+s & 0 \\ 0 & 0 & r+s \end{bmatrix}=\begin{bmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{bmatrix}+\begin{bmatrix} s & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{bmatrix}$

$$=f(r)+f(s)\ \forall\ r,s\in\mathbb{Z}.$$

Hence, f is a homomorphism.

Now, take $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\in\mathbb{M}_3(\mathbb{R})$. Then $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\neq\begin{bmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{bmatrix}$ for any $r\in\mathbb{R}$, since the elements in the $(1,\ 2)\text{th}$ place are different.

Thus, $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\neq f(r)$ for any $r\in\mathbb{R}$.

$\therefore \operatorname{Im} f\neq\mathbb{M}_3(\mathbb{R})$.

Hence, f is not surjective.

Next, if $f(r)=f(s)$ for some $r,\ s\in\mathbb{R}$, $\begin{bmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{bmatrix}=\begin{bmatrix} s & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{bmatrix}$.

Hence, $r=s$.

Thus, f is 1-1, and hence, a monomorphism.

ii) Any element of D_8 is of the form $r^iR_{90}^j$, where $rR_{90}=R_{90}^{-1}r,\ r^2=I,\ R_{90}^4=I.$

Suppose f is a homomorphism. Then $f(r^2)=f(r)+f(r)$ in $\mathbb{Z}_{8.}$

But $r^2=I$, so that $f(r^2)=\overline{0}$.

On the other hand, $f(r)+f(r)=\overline{1}+\overline{1}=\overline{2}$. Since $\overline{0}\neq\overline{2}$, we reach a contradiction. Therefore, f is not a homomorphism.

iii) Note that $f(z_1z_2)=|z_1z_2|=|z_1|\,|z_2|$, as you know from Calculus.

$$=f(z_1)f(z_2).$$

Thus, f is a homomorphism.

Now, consider $-1\in\mathbb{R}^*$. There is no $z\in\mathbb{C}^*$ s.t. $f(z)=|z|=-1$, since $|z|>0$.

Hence, f is not surjective.

You should check that f is not a monomorphism either.

***

Example 5: Show that $f:\mathbb{M}_{2\times3}(\mathbb{C})\to\mathbb{M}_3(\mathbb{C}):f(A)=\begin{bmatrix} A \\ \mathbf{0} \end{bmatrix}$, where $\mathbf{0}$ is the row vector $(0,\ 0,\ 0)$, is a well-defined monomorphism. Also find $\operatorname{Ker} f$.

Solution: First, let us understand f through a particular case. Let $A=\begin{bmatrix} 2 & \pi & 3i \\ -1 & i & 9-i\sqrt{2} \end{bmatrix}\in\mathbb{M}_{2\times3}(\mathbb{C})$.

Then $f(A)=\begin{bmatrix} 2 & \pi & 3i \\ -1 & i & 9-i\sqrt{2} \\ 0 & 0 & 0 \end{bmatrix}=\begin{bmatrix} A \\ \mathbf{0} \end{bmatrix}\in \mathbb{M}_3(\mathbb{C}).$

If f is clear to you now, you should verify that if $A = B$ in $\mathbb{M}_{2\times3}(\mathbb{C})$, then $\begin{bmatrix} A \\ \mathbf{0} \end{bmatrix}=\begin{bmatrix} B \\ \mathbf{0} \end{bmatrix}$ in $\mathbb{M}_3(\mathbb{C})$, i.e., $f(A) = f(B)$. Hence, f is well-defined.

Next, $f(A+B)=\begin{bmatrix} A+B \\ \mathbf{0} \end{bmatrix}=\begin{bmatrix} A \\ \mathbf{0} \end{bmatrix}+\begin{bmatrix} B \\ \mathbf{0} \end{bmatrix}$, since $\mathbf{0}+\mathbf{0}=\mathbf{0}$.

$$= f(A) + f(B).$$

Now suppose $f(A) = f(B)$, where $A = [a_{ij}], B = [b_{ij}]$. Then $\begin{bmatrix} A \\ \mathbf{0} \end{bmatrix}=\begin{bmatrix} B \\ \mathbf{0} \end{bmatrix}$.

Hence, $a_{ij} = b_{ij}\ \forall\ i = 1, 2,\ j = 1, 2, 3.$ So $A = B$.

Thus, f is 1-1, and hence, a monomorphism.

Finally, $\text{Ker } f = \{A \in \mathbb{M}_{2\times3}(\mathbb{C}) \,\Big|\, \begin{bmatrix} A \\ \mathbf{0} \end{bmatrix} = \mathbf{0_3}\}$, where $\mathbf{0_3}$ is the zero in $\mathbb{M}_3(\mathbb{C})$.

$$= \{A \in \mathbb{M}_{2\times3}(\mathbb{C}) \,|\, A = \mathbf{0}_{\mathbf{2\times3}}\},\text{ where } \mathbf{0}_{\mathbf{2\times3}} \text{ is the zero in } \mathbb{M}_{2\times3}(\mathbb{C}).$$

$$= \{\mathbf{0}_{\mathbf{2\times3}}\}.$$

***

Example 5 can be generalised to show that **there is a monomorphism from $\mathbb{M}_{\mathbf{m\times n}}(\mathbb{C})$ into $\mathbb{M}_{\mathbf{r\times p}}(\mathbb{C})\ \forall\ \mathbf{r \geq m, p \geq n}$.** In this sense, we can say that, for example, $\mathbb{M}_n(\mathbb{C}) \leq \mathbb{M}_{n+m}(\mathbb{C})\ \forall\ n, m \geq 0$, by adding m rows and columns of zeroes to each $A \in \mathbb{M}_n(\mathbb{C})$.

We shall refer to this again in Remark 3, following Example 8.

Now you should solve the following exercises. This will help you to see if you have understood what you have studied so far.

E1) Check whether or not $I: G \to G: I(g) = g$ is an endomorphism, for any group G. Is it a monomorphism?

E2) Show that $f: (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +): f(x) = \ln x$, the natural logarithm of x, is a group homomorphism. Find $\text{Ker } f$ and $\text{Im } f$ also.

E3) Is $f: (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot): f(A) = \det(A)$ a homomorphism? If yes, obtain $\text{Ker } f$ and $\text{Im } f$. Otherwise, explain why f is not a homomorphism.

E4) Which of the following statements are true? Give reasons for your answers.

i) $f: \mathbb{Z} \to \mathbb{Z}: f(z) = 5z$ is a monomorphism.

ii) $f: \mathbb{R}^* \to \mathbb{R}^*: f(z) = 5z$ is a monomorphism.

iii) $f: \mathbb{R} \to \mathbb{R}: f(x) = x^2$ is a homomorphism.

iv) $f: \mathbb{R}^* \to \mathbb{R}^*: f(x) = x^2$ is a homomorphism.

v) If G is a group and $H \leq G,$ then there can be no homomorphism from G to $H.$

In the context of E4 above, consider the following comment.

Remark 2: Look at f in E4(i) and (ii). It is defined in the same way. But, in (i) it is a homomorphism, and not in (ii). What makes this difference? It is the operations of the domain group and the codomain group. If the operation concerned changes, f may not preserve it. So, always be careful about noting the operations in the domain group and codomain group you are working with when you are defining a homomorphism.

If you look at the examples above, you would note that the homomorphism carries the identity to the identity and the inverse to the inverse. In fact, this property is true for any group homomorphism, as you will now see.

Theorem 1: Let $f:(G_1, *_1) \to (G_2, *_2)$ be a group homomorphism. Then

i) $f(e_1) = e_2,$ where e_1 is the identity of G_1 and e_2 is the identity of $G_2.$

ii) $f(x^{-1}) = [f(x)]^{-1},$ for all x in $G_1.$

Proof: We know that $f(x *_1 y) = f(x) *_2 f(y) \ \forall \ x, \ y \in G_1.$

i) Let $x \in G_1.$ Now, $e_1 *_1 x = x.$ Hence,
$f(x) = f(e_1 *_1 x) = f(e_1) *_2 f(x).$
Also $f(x) = e_2 *_2 f(x)$ in $G_2.$
Thus, $f(e_1) *_2 f(x) = e_2 *_2 f(x).$
So, by the right cancellation law in $G_2, f(e_1) = e_2.$

ii) For any $x \in G_1, f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2,$ from (i).
Hence, $f(x^{-1}) = [f(x)]^{-1} \ \forall \ x \in G_1.$ ■

You have just seen that if $f: G_1 \to G_2$ is a homomorphism, then f maps the identity of G_1 to the identity of $G_2,$ and the inverse of $g \in G_1$ to the inverse of $f(g) \in G_2.$ Do you expect the converse to be true? That is, if $f: G_1 \to G_2$ is a function such that $f(e_1) = e_2$ and $[f(x)]^{-1} = f(x^{-1}) \forall x \in G_1,$ then will f be a homomorphism? Let's see.

Example 6: Show that the converse of Theorem 1 is false.

Solution: Consider $f: \mathbb{Z} \to \mathbb{Z}: f(0) = 0$ and $f(n) = \begin{cases} n+1 \forall n > 0, \\ n-1 \forall n < 0. \end{cases}$

Since $f(1+1) \neq f(1) + f(1), f$ is not a homomorphism.

But $f(e_1) = e_2$ since $e_1 = e_2 = 0.$ So (i) of Theorem 1 holds for $f.$

Also, if $n > 0, f(-n) = -n-1 = -(n+1) = -f(n).$

Similarly, you should check that if $n < 0,$ then $f(-n) = -f(n).$

So (ii) of Theorem 1 is satisfied also by $f.$

Thus, f is a counterexample of the converse of Theorem 1. Hence, the converse is false.

***

Let us look at a few more examples of homomorphisms now. We can get one important class of homomorphisms from quotient groups.

Example 7: Let $H \lhd G$. Consider the mapping $p : G \to G/H : p(x) = Hx$. Show that p is an epimorphism. What is $\operatorname{Ker} p$?

p, in Example 7, is called the **natural**, or **canonical**, **group homomorphism**. The reason this is called 'natural' will become clear to you in Sec.8.4.

Solution: First, note that p is a well-defined mapping since $x = y \Rightarrow Hx = Hy \Rightarrow p(x) = p(y)$.
Now, for $x, y \in G$, $p(xy) = Hxy = Hx \cdot Hy = p(x)p(y)$.
Therefore, p is a homomorphism.
Here, $\operatorname{Im} p = \{p(x) \mid x \in G\} = \{Hx \mid x \in G\} = G/H$.
Therefore, p is surjective.
Hence, p is an epimorphism.

$\operatorname{Ker} p = \{x \in G \mid p(x) = H\}$ (Remember, H is the identity of G/H.)

$= \{x \in G \mid Hx = H\}$

$= \{x \in G \mid x \in H\}$, by Theorem 1 of Unit 5.

$= G \cap H$
$= H.$

***

In Example 7 you can see that $\operatorname{Ker} p \lhd G$. You should also verify that Theorem 1 is true here.

Another class of examples of homomorphisms concerns the inclusion map.

Example 8: Let H be a subgroup of a group G. Show that the map $i : H \to G : i(h) = h$ is a monomorphism. Also find $\operatorname{Ker} i$ and $\operatorname{Im} i$.

i, in Example 8, is called the **inclusion map**. We sometimes denote the map $i : H \to G$ by $H \overset{i}{\hookrightarrow} G$.

Solution: Since $i(h_1h_2) = h_1h_2 = i(h_1)i(h_2) \ \forall \ h_1, h_2 \in H$, i is a group homomorphism.

Also, if $i(h_1) = i(h_2)$ for some $h_1, h_2 \in H$, then $h_1 = h_2$. Hence, i is 1-1.

Now, $\operatorname{Ker}\, i = \{h \in H \mid h = e\} = \{e\}$, and

$\operatorname{Im}\, i = \{i(h) \mid h \in H\} = \{h \mid h \in H\} = H.$

***

Consider the following remark in the context of Example 8.

Remark 3: When $H = G$ in Example 8, we get the identity function I, which you have shown to be a monomorphism in E1.

Now consider another class of examples related to functions.

Example 9: Let $\mathcal{F}$ be the group of all functions from $\mathbb{R}$ to $\mathbb{R}$ w.r.t. pointwise addition. Let $r \in \mathbb{R}$. Define $\phi_r : \mathcal{F} \to \mathbb{R} : \phi_r(f) = f(r)$. Show that ϕ_r is a homomorphism. Also find $\operatorname{Im} \phi_r$ and $\operatorname{Ker} \phi_r$.

ϕ_r, in Example 9, is called the **evaluation homomorphism** at the point r.

Solution: First, let us check that ϕ_r is well-defined. If $f = g$ in $\mathcal{F}$, then $f(r) = g(r)$ in $\mathbb{R}$, so that $\phi_r(f) = \phi_r(g)$. Hence, ϕ_r is well-defined.

Next, since $\phi_r(f+g)=(f+g)(r)=f(r)+g(r)=\phi_r(f)+\phi_r(g)$, ϕ_r is a homomorphism.

Now, for any $c\in\mathbb{R}$, define $f:\mathbb{R}\to\mathbb{R}:f(x)=c$.

Then $f\in\mathcal{F}$ s.t. $\phi_r(f)=f(r)=c$. So $c\in\operatorname{Im}\phi_r$. Hence, $\operatorname{Im}\phi_r=\mathbb{R}$.

$\operatorname{Ker}\phi_r=\{f\in\mathcal{F}\mid\phi_r(f)=0\}=\{f\in\mathcal{F}\mid f(r)=0\}$.

***

Try solving the following exercises now.

E5) Consider the natural homomorphism p from S_3 to S_3/A_3, where $A_3=<(1\ 2\ 3)>$. Does $(1\ 2)\in\operatorname{Ker}p$? Does $(1\ 2)\in\operatorname{Im}p$?

E6) Let $S^1=\{z\in\mathbb{C}\mid |z|=1\}$, the unit circle.

Define $f:(\mathbb{R},+)\to(S^1,\cdot):f(x)=e^{2ix}$. Is f a homomorphism? If so, find $\operatorname{Ker}f$. If not, change the definition of f so that f becomes a homomorphism.

E7) Let G be a group and $H\lhd G$. Show that there exists a group G_1 and a homomorphism $f:G\to G_1$ such that $\operatorname{Ker}f=H$.
(**Hint:** Does Example 7 help?)

E8) Consider $\phi:S_3\to<(1\ 2)>:\phi(\sigma)=\sigma(1\ 2)\sigma^{-1}$. Is ϕ a homomorphism? If it is, then find $\operatorname{Ker}\phi$. If ϕ is not a homomorphism, find a subgroup K of S_3 and a homomorphism $\psi:S_3\to K$.

Now let us consider the composition of two homomorphisms. Let us first look at an example related to $\mathbb{Z}$.

Example 10: Consider the homomorphisms $f:\mathbb{Z}\to\mathbb{Z}:f(z)=5z$ and $p:\mathbb{Z}\to\mathbb{Z}/15\mathbb{Z}:p(z)=\bar{z}$. Is $p\circ f$ a well-defined homomorphism? Why, or why not?

Solution: If $z_1=z_2$ in $\mathbb{Z}$, then $5z_1=5z_2$, and $5z_1+15\mathbb{Z}=5z_2+15\mathbb{Z}$.

So $p\circ f(z_1)=p\circ f(z_2)$. Thus, $p\circ f$ is well-defined.

Also, $p\circ f(z_1+z_2)=5(z_1+z_2)+15\mathbb{Z}=(5z_1+15\mathbb{Z})+(5z_2+15\mathbb{Z})$

$$=p\circ f(z_1)+p\circ f(z_2).$$

Thus, $p\circ f$ is a homomorphism.

***

What you have seen in Example 10 is not specific to $\mathbb{Z}$. It is true in general. Let us see why.

Theorem 2: If $f:G_1\to G_2$ and $g:G_2\to G_3$ are two group homomorphisms, then $g\circ f:G_1\to G_3$ is also a group homomorphism.

Proof: First, note that $g\circ f$ is well-defined since $\operatorname{Im}f\subseteq$ Domain g.

Now, let $x,\ y\in G_1$. Then

$g \circ f(xy) = g(f(xy))$

$= g(f(x)f(y))$, since f is a homomorphism.

$= g(f(x))g(f(y))$, since g is a homomorphism.

$= g \circ f(x) \cdot g \circ f(y)$.

Thus, $g \circ f$ is a homomorphism. ■

Try a related exercise now.

E9) Show that the composition of $f : \mathbb{C} \to \mathbb{R} : f(x+iy) = y$ and $g : \mathbb{R} \to \mathbb{C} : g(r) = ir$ is a homomorphism. What are $\text{Ker}(g \circ f)$ and $\text{Im}(g \circ f)$? Is $\text{Ker}(g \circ f) \subseteq \text{Ker } g$? Is $\text{Ker}(g \circ f) \subseteq \text{Ker } f$? Give reasons for your answers.

So far you have seen that the kernel and image of a homomorphism are subsets of groups. In the examples you have studied so far you may have noticed that these subsets are actually subgroups. We will now prove that the kernel of a homomorphism is a normal subgroup, and the image is a subgroup.

Theorem 3: Let $f : G_1 \to G_2$ be a group homomorphism. Then

i) $\text{Ker } f$ is a normal subgroup of G_1, and

ii) $\text{Im } f$ is a subgroup of G_2.

Proof: i) $\text{Ker } f = \{x \in G_1 \mid f(x) = e_2\}$.

Since $f(e_1) = e_2$, $e_1 \in \text{Ker } f$. $\therefore \text{Ker } f \neq \emptyset$.

Now, if $x, y \in \text{Ker } f$, then $f(x) = e_2$ and $f(y) = e_2$.

$\therefore f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = e_2$.

$\therefore xy^{-1} \in \text{Ker } f$.

Therefore, by the subgroup test of Unit 3, $\text{Ker } f \leq G_1$.

Next, for any $y \in G_1$ and $x \in \text{Ker } f$,

$f(y^{-1}xy) = f(y^{-1})f(x)f(y)$

$= [f(y)]^{-1}e_2 f(y)$, since $f(x) = e_2$.

$= e_2$.

$\therefore \text{Ker } f \lhd G_1$.

ii) $\text{Im } f \neq \emptyset$, since $f(e_1) \in \text{Im } f$.

Now, let $x_2, y_2 \in \text{Im } f$. Then $\exists x_1, y_1 \in G_1$ such that $f(x_1) = x_2$ and $f(y_1) = y_2$. Then $y_2^{-1} = f(y_1^{-1})$.

$\therefore x_2 y_2^{-1} = f(x_1)f(y_1^{-1}) = f(x_1 y_1^{-1}) \in \text{Im } f$.

$\therefore \text{Im } f \leq G_2$. ■

In Theorem 3 you have seen that $\text{Im } f \leq G_2$. Consider the following remark in this context.

Remark 4: Consider $i : H \to S_4$, the inclusion map, where $H = \{I, (1\,2)\}$. Here $\text{Im } i = H$.

Now, take $(2\ 4) \in S_4$. Then $(2\ 4)^{-1}(1\ 2)(2\ 4) = (2\ 4)(1\ 2)(2\ 4) = (1\ 4) \notin \operatorname{Im} i$.
Thus, $\operatorname{Im} i \ntriangleleft S_4$.
This example shows that $\operatorname{Im} f$ need not be normal in G_2 (in Theorem 3).
However, if G_2 is abelian, then you know that $\operatorname{Im} f \triangleleft G_2$.

Let us consider some immediate outcomes of Theorem 3.

Example 11: Show that $\{ix \mid x \in \mathbb{R}\}$ is a normal subgroup of $\mathbb{C}$.

Solution: From Theorem 3 and Example 3, we see that $\{ix \mid x \in \mathbb{R}\}$ is a normal subgroup of $\mathbb{C}$.

***

Example 12: Consider $\phi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot) : \phi(x) = \cos x + i \sin x$. Find $\operatorname{Ker} \phi$ and $\operatorname{Im} \phi$. **Hence** show that $< 2\pi > \triangleleft \mathbb{R}$ and $S^1 \triangleleft \mathbb{C}^*$, where S^1 is the unit circle.

Solution: You can show that $\phi(x + y) = \phi(x)\phi(y)$. Thus, ϕ is a group homomorphism.
Now $\phi(x) = 1$ iff $x = 2\pi n$ for some $n \in \mathbb{Z}$.
Thus, $\operatorname{Ker} \phi = \{2\pi n \mid n \in \mathbb{Z}\} = < 2\pi >$.
Hence, by Theorem 3, $< 2\pi > \triangleleft \mathbb{R}$.
In this case, $\operatorname{Im}\phi$ is a subgroup of $\mathbb{C}^*$, which is abelian. So $\operatorname{Im} \phi \triangleleft \mathbb{C}^*$.
Note that $\operatorname{Im} \phi$ is the set of all the complex numbers with absolute value 1, i.e., the set of all the complex numbers on the circle with radius 1 unit and centre $(0, 0)$, i.e., S^1.
So, $S^1 \triangleleft \mathbb{C}^*$.

***

In the context above, consider the following general comment about solutions.

Remark 5: In the example above, note the wording of the question. In the last part it says '**Hence** show that …'. So, you need to prove that $< 2\pi >$ and S^1 are normal subgroups of the respective groups **using** what you have done in the previous stage of the solution.
You could have directly shown that $< 2\pi >$ and S^1 are normal subgroups too, but then you would not have been answering what the question has asked.

Now let us look at the kernel of a homomorphism. You may have noticed that sometimes it is $\{e\}$ (as in Example 2), and sometimes it is a large subgroup (as in Example 3). Does the size of the kernel indicate anything? In fact, as you will now see, the larger the kernel, the further away is the homomorphism from becoming a monomorphism.

Theorem 4: Let $f : G_1 \to G_2$ be a group homomorphism. Then f is injective iff $\operatorname{Ker} f = \{e_1\}$, where e_1 is the identity element of the group G_1.

Proof: First, let us assume that f is injective.
Let $x \in \operatorname{Ker} f$. Then $f(x) = e_2$, i.e., $f(x) = f(e_1)$. But f is 1-1. $\therefore x = e_1$.
Thus, $\operatorname{Ker} f = \{e_1\}$.

Conversely, suppose $\text{Ker } f = \{e_1\}$.

Let $x, y \in G_1$ such that $f(x) = f(y)$. Then

$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = f(y)[f(y)]^{-1} = e_2$.

$\therefore xy^{-1} \in \text{Ker } f = \{e_1\}$. $\therefore xy^{-1} = e_1$. Hence, $x = y$.

This shows that f is injective. ■

Theorem 4 is very useful. For example, by using Theorem 4 and Example 8, we can immediately see that any inclusion $i: H \to G$ is 1-1, since $\text{Ker } i = \{e\}$.

Let us consider some other examples.

Example 13: Consider the situation in Example 7. Under what conditions on H is p 1-1?

Solution: $p: G \to G/H : p(x) = Hx$. You know that $\text{Ker } p = H$.

Thus, p is 1-1 iff $H = \{e\}$.

***

Example 14: Consider the group T of translations of $\mathbb{R}^2$ (see Example 7, Unit 2). Define a map $\phi: (\mathbb{R}^2, +) \to (T, \circ)$ by $\phi(a,b) = f_{a,b}$, where $f_{a,b}(x,y) = (x+a, y+b)$. Show that ϕ is an epimorphism, which is also 1-1.

Solution: In Unit 2, you have seen that $f_{a+b,c+d} = f_{a,b} \circ f_{c,d}$, for $(a,b), (c,d)$ in $\mathbb{R}^2$, i.e., $\phi((a,b)+(c,d)) = \phi((a,b)) \circ \phi((c,d))$.

Thus, ϕ is a homomorphism of groups.

Now, any element of T is $f_{a,b} = \phi((a,b))$. Therefore, ϕ is surjective.

Let us now see why ϕ is also injective. Note that $f_{0,0}$ is the identity of T.

Let $(a,b) \in \text{Ker } \phi$. Then

$\phi((a,b)) = f_{0,0}$

$\Rightarrow f_{a,b} = f_{0,0}$

$\Rightarrow f_{a,b}(0,0) = f_{0,0}(0,0)$,

$\Rightarrow (a,b) = (0,0)$

$\therefore \text{Ker } \phi = \{(0,0)\}$, i.e., ϕ is 1-1, by Theorem 4.

So we have proved that ϕ is a homomorphism, which is bijective.

***

Try solving the following exercises now.

E10) For any $n > 1$, consider $\mathbb{Z}_n$ and U_n, the group of nth roots of unity. Let ζ denote a primitive nth root of unity. Then $U_n = <\zeta>$. Show that $f: \mathbb{Z}_n \to U_n : f(\bar{r}) = \zeta^r$ is a group homomorphism. Find $\text{Ker } f$ and $\text{Im } f$. Hence decide if f is injective and/or surjective.

E11) Let G be a group, and H and K be normal subgroups of G. Consider $f : G \to (G/H) \times (G/K) : f(g) = (Hg, Kg)$. Show that f is a homomorphism. Also find $\text{Ker } f$ and $\text{Im } f$.

Further, under what conditions on H and K will f be a monomorphism? Is f surjective?

And now let us look at a very useful property of an epimorphism.

Theorem 5: If $f : G_1 \to G_2$ is an epimorphism and S is a set that generates G_1, then $f(S)$ generates G_2.

Proof: From Unit 4, you know that if S generates G_1, then $G_1 = <S> = \{x_1^{r_1} x_2^{r_2} \ldots x_m^{r_m} \mid m \in \mathbb{N}, x_i \in S, r_i \in \mathbb{Z}$ for all $i\}$.

We need to show that $G_2 = < f(S) >$.

Now, since $S \subseteq G_1$, $f(S) \subseteq G_2$.

Hence, $< f(S) > \leq G_2$.

To show that $G_2 \leq < f(S) >$, let $x \in G_2$. Since f is surjective, $\exists\ y \in G_1$ such that $f(y) = x$.

Since $y \in G_1$, $y = x_1^{r_1} \ldots x_m^{r_m}$, for some $m \in \mathbb{N}$, $x_i \in S$ and $r_i \in \mathbb{Z}, 1 \leq i \leq m$.

Thus, $x = f(y) = f(x_1^{r_1} \ldots x_m^{r_m})$

$= (f(x_1))^{r_1} \ldots (f(x_m))^{r_m}$, since f is a homomorphism.

$\Rightarrow x \in < f(S) >$, since $f(x_i) \in f(S)$ for every $i = 1, 2, \ldots, m$.

Thus, $G_2 \leq < f(S) >$.

Hence, $G_2 = < f(S) >$. ■

Let us use Theorem 5 to state some important properties of homomorphisms; in fact, these are immediate corollaries of Theorem 5.

Corollary 1: The homomorphic image of a cyclic group is cyclic. ■

In E12, we ask you to prove this, and the next corollary.

Corollary 2: The homomorphic image of a finitely generated group is finitely generated. ■

Let us now consider a particular case in which Theorem 5 is used.

Example 15: Let $f : D_{10} \to G$ be a group epimorphism. What do the elements of G look like?

Solution: You know that D_{10} is generated by r and R, where $r^2 = I, R^5 = I$ and $rR = R^{-1}r$. So $\{f(r), f(R)\}$ generates G. Also, since f is a homomorphism, $[f(r)]^2 = I = [f(R)]^5$ and $f(r)f(R) = [f(R)]^{-1} f(r)$.

Hence, the elements of G are of the form $f(r)^m f(R)^n$, where $m = 0, 1$ and $n = 0, 1, 2, 3, 4$.

***

In the context of Theorem 5, consider the following remark.

Remark 6: Note that if f (in Theorem 5) is not surjective, $f(S)$ need not generate G_2. For example, take the inclusion map $i : <(1\ 2)> \to S_3$. Then $i(<(1\ 2)>) = <(1\ 2)> \neq S_3$.

Now let us consider another basic result that shows how certain algebraic properties of a group are preserved by a group homomorphism.

Theorem 6: Let $f : G_1 \to G_2$ be a group homomorphism, where G_1 is abelian. Then $f(G_1)$ is abelian.

Proof: Let $a, b \in f(G_1)$. Then $\exists\ x,\ y \in G_1$ such that $a = f(x), b = f(y)$. So

$ab = f(x)f(y) = f(xy) = f(yx),$ since G_1 is abelian

$\quad = f(y)f(x)$

$\quad = ba.$

Hence, $f(G_1)$ is abelian. ■

While solving the following exercises, you will prove some important properties of homomorphic images of groups.

E12) Prove Corollary 1 and Corollary 2.
State the converse of Corollary 1. Is it true? Why, or why not?

E13) State the converse of Theorem 6. Is it true? Give reasons for your answer.

E14) Use Theorem 5 to prove that the quotient group of a cyclic group is cyclic.

So far you have seen examples of various kinds of homomorphisms – injective, surjective and bijective. From Theorems 5 and 6, you can already see how a homomorphism preserves certain algebraic properties, like being abelian or being finitely generated. Now you will see how bijective homomorphisms preserve every bit of algebraic information of the groups concerned.

8.3 ISOMORPHISMS

In this section we will discuss an important class of homomorphisms, namely, those that are 1-1 and onto. So, let's go back to Tables 1 and 2, at the beginning of Sec.8.2. Over there you saw that not only is $f : \mathbb{Z}_4 \to U_4$ a homomorphism, but it is 1-1 and onto. You also saw that Table 2 looked exactly like Table 1, with $m \cdot \overline{1}$ replaced by i^m, $m = 0, 1, 2, 3.$ Thus, f was not just preserving the operation, but also telling us that the elements in $\mathbb{Z}_4$ and U_4 behave **exactly the same way w.r.t. their respective operations. And hence**, $(\mathbb{Z}_4, +)$ **and** $(U_4, \cdot)$ **have exactly the same algebraic structure**. The f there is an example of what we now define.

The word 'isomorphism' is derived from the Greek word 'isos', meaning 'equal'.

Definitions: Let G_1 and G_2 be two groups.

i) A group homomorphism $f : G_1 \to G_2$ is called a **group isomorphism** (or simply, an **isomorphism**) if f is 1-1 and onto.

In this case, we say that the **group G_1 is isomorphic to the group G_2**, or that **G_1 and G_2 are isomorphic**. We denote this fact by $G_1 \simeq G_2$, or $G_1 \cong G_2$. (We shall use '$\simeq$' to denote 'is isomorphic to'.)

ii) An isomorphism of a group G onto itself is called an **automorphism** of G.

For example, the identity function, $I_G : G \to G : I_G(x) = x$, is an automorphism of G, and $\mathbb{Z}_4 \simeq U_4$ (as discussed above).

Also, from Example 13 you know that $G \simeq G/\{e\}$, for any group G.

Further, from Example 14 you know that $\mathbb{R}^2 \simeq T$, the group of translations of $\mathbb{R}^2$.

Note that an isomorphism is a monomorphism and an epimorphism.

Let us now look at some more examples of isomorphic groups.

Example 16: Show that $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$ is a subgroup of $\mathbb{M}_2(\mathbb{R})$.

Then show that $f : G \to \mathbb{C} : f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$ is an isomorphism.

Solution: Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$, $G \neq \emptyset$.

Now, if $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$, then $(-A) = \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \in G$.

Also, check that, for any $A, B \in G$, $A - B \in G$.

Hence, $G \leq \mathbb{M}_2(\mathbb{R})$.

Now, consider the second part. Let us verify that f is well-defined. If $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ in G, then $a = c, b = d$. So $a + ib = c + id$ in $\mathbb{C}$, i.e., $f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$. Therefore, f is well-defined.

Next, for $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ in G,

$$\begin{aligned} f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) &= f\left(\begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}\right) = (a+c) + i(b+d) \\ &= (a+ib) + (c+id) \\ &= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right). \end{aligned}$$

Therefore, f is a homomorphism.

Now,

$$\text{Ker } f = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G \middle| a + ib = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G \middle| a = 0, b = 0 \right\} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}.$$

Therefore, by Theorem 4, f is 1-1.

Finally, to check that $\text{Im } f = \mathbb{C},$ take $z \in \mathbb{C}.$ Then $z = a + ib$ for some $a, b \in \mathbb{R}.$

Thus, $z = f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right)$. Hence, f is surjective.

Therefore, f is an isomorphism. Thus, $\mathbb{C} \simeq G \le \mathbb{M}_2(\mathbb{R}).$

***

Example 17: Show that

i) $S_m \le S_n \ \forall \ n \ge m,$ and

ii) $\mathbb{M}_{m\times n}(\mathbb{C}) \lhd \mathbb{M}_{r\times p}(\mathbb{C}) \ \forall \ r \ge m, \ p \ge n.$

iii) $\mathbb{R}^m \lhd \mathbb{R}^n \ \forall \ m \le n.$

Solution: i) $i : S_m \to S_n : i(\sigma) = \sigma',$ where $\sigma'(x) = \begin{cases} \sigma(x), \text{ for } x = 1, \ldots, m, \\ x, \text{ for } x = m+1, \ldots, n. \end{cases}$

You should check that i is a homomorphism.

Hence, $i(S_m) \le S_n.$

Also, since i is 1-1, $S_m \simeq i(S_m).$

Thus, we can treat $i(S_m)$ and S_m as the same, and say $S_m \le S_n.$

ii) Along the lines of Example 5, define

$i : \mathbb{M}_{m\times n}(\mathbb{C}) \to \mathbb{M}_{r\times p}(\mathbb{C}) : i(A) = \begin{bmatrix} A & \mathbf{0_1} \\ \mathbf{0_2} & \mathbf{0_3} \end{bmatrix},$ where $\mathbf{0_1}, \mathbf{0_2}$ and $\mathbf{0_3}$ are zero matrices of orders $m \times (p-n), (r-m) \times n$ and $(r-m) \times (p-n),$ respectively.

By using the argument in (i) above, you can see that $\mathbb{M}_{m\times n}(\mathbb{C}) \le \mathbb{M}_{r\times p}(\mathbb{C}).$

Since $\mathbb{M}_{r\times p}(\mathbb{C})$ is an abelian group, every subgroup is normal. Hence the result.

iii) $i : \mathbb{R}^m \to \mathbb{R}^n : i(a_1, \ldots, a_m) = (a_1, a_2, \ldots, a_m, \underbrace{0, \ldots, 0}_{(n-m)\text{times}})$ is a well-defined monomorphism.

As in (ii) above, $\mathbb{R}^m \lhd \mathbb{R}^n,$ since $\mathbb{R}^n$ is abelian.

***

Before going further, consider the following important remark about the power of an isomorphism.

Remark 7: If $f : G_1 \to G_2$ is a group isomorphism, then f preserves not just the operation, but the complete algebraic structure of G_1. Thus, G_1 and G_2 must have exactly the same algebraic properties. If G_1 is infinite, so must G_2 be. If G_1 is abelian, so must G_2 be. If G_1 has an element of order $n,$ then G_2 must have an element of order $n,$ and so on.

Two isomorphic groups are algebraically the same systems.

Let us now help you understand what is noted in the remark above, through some more examples.

Example 18: If G_1 and G_2 are two groups of the same finite order, then they are isomorphic. True, or false? Give reasons for your choice.

Solution: Consider Table 1 and Table 3 given at the beginning of Sec.8.2. Here $o(\mathbb{Z}_4) = 4 = o(K_4)$, but their Cayley tables are very different. For instance, Table 1 shows that $\mathbb{Z}_4$ has two elements of order 4. But Table 3 shows that K_4 has no element of order 4. Thus, their algebraic structures are different.
In fact, $\mathbb{Z}_4$ is cyclic, but K_4 is not. Hence, they are not isomorphic. Thus, the given statement is false.

***

'$\not\simeq$' denotes 'is not isomorphic to'.

Example 19: Show that $\mathbb{Z} \not\simeq \mathbb{Q}$.

Solution: You know that $\mathbb{Z}$ is cyclic. Also, from Unit 4, you know that $\mathbb{Q}$ is not cyclic. Hence, $\mathbb{Z} \not\simeq \mathbb{Q}$.

***

What Example 19 tells us is that two infinite groups need not be isomorphic. Note that, from your course, Real Analysis, you know that $\mathbb{Q}$ is countable. Hence, there is a bijection between $\mathbb{Z}$ and $\mathbb{Q}$. But this bijection does not preserve the operation, as you can see from Example 19.

The following result also clarifies what is noted in Remark 7, i.e., that isomorphic groups are algebraically alike.

Theorem 7: If $f: G \to H$ is a group isomorphism and $x \in G$, then $< x > \simeq < f(x) >$. Further,

i) if x is of finite order, then $o(x) = o(f(x))$.

ii) if x is of infinite order, so is $f(x)$.

Proof: If we restrict f to any subgroup K of G, we have the function $f|_K : K \to f(K)$. Since f is bijective, so is its restriction $f|_K$. Hence, $K \simeq f(K)$, for any subgroup K of G.
In particular, for any $x \in G, < x > \simeq f(< x >) \simeq < f(x) >$, by Theorem 5.

Now if x has finite order, then $o(x) = o(< x >) = o(< f(x) >) = o(f(x))$. Hence, (i) is proved.

To prove (ii), assume that x is of infinite order. Then $< x >$ is an infinite group. Therefore, $< f(x) >$ is an infinite group, and hence, $f(x)$ is of infinite order. So, we have proved (ii). ■

Try the following exercises now.

E15) Show that $\mathbb{Z} \simeq n\mathbb{Z}$, for each $n \in \mathbb{Z}$.
(**Hint:** Consider $f: (\mathbb{Z}, +) \to (n\mathbb{Z}, +): f(k) = nk$.)

E16) In Example 16, you saw why $\mathbb{C}$ is isomorphic to a subgroup of $\mathbb{M}_2(\mathbb{R})$. Can you think of a subgroup of $GL_2(\mathbb{R})$ to which $\mathbb{R}$ is isomorphic? Could it be $\left\{\begin{bmatrix}1 & x\\0 & 1\end{bmatrix}\middle| x\in\mathbb{R}\right\}\subseteq GL_2(\mathbb{R})$?

E17) Is $f:\mathbb{Z}\to\mathbb{Z}:f(x)=0$ a homomorphism? Is f an isomorphism?

E18) Let G be a group. Under what conditions on G will $f:G\to G:f(a)=a^{-1}$ be an isomorphism?

E19) If $\phi:G\to H$ and $\theta:H\to K$ are two group isomorphisms, then show that $\theta\circ\phi$ is an isomorphism from G onto K.

E20) Let $f:G_1\to G_2$ be a group isomorphism, and let $g_1\in G_1$. Then show that the equation $x^k=g_1$ has exactly the same number of solutions in G_1 as $x^k=f(g_1)$ has in G_2, for $k\in\mathbb{Z}$.

E21) Check whether or not $f:U_{15}\to U_{15}:f(\zeta)=\zeta^2$ is an isomorphism, where $U_{15}=<\zeta>$.

E22) For any group G, prove that $G\times\{e\}\simeq G\simeq\{e\}\times G$, where e is the identity of some group.

You must have noticed that the definition of an isomorphism just says that the homomorphism is bijective, i.e., its inverse map exists. It does not tell us any algebraic properties of the inverse. The next result does this.

Theorem 8: If $f:G_1\to G_2$ is an isomorphism of groups, then $f^{-1}:G_2\to G_1$ is also an isomorphism.

Proof: From your course, Calculus, you know that f^{-1} is bijective. (Verify this!) So, we only need to show that f^{-1} is a homomorphism.

To see this, let $a', b'\in G_2$ and $a=f^{-1}(a'), b=f^{-1}(b')$.

Then $f(a)=a'$ and $f(b)=b'$.

Therefore, $f(ab)=f(a)f(b)=a'b'$.

On applying f^{-1}, we get $f^{-1}(a'b')=ab=f^{-1}(a')f^{-1}(b')$.

Thus, f^{-1} is a homomorphism, and hence, an isomorphism. ■

From Example 14 and Theorem 8, we can immediately say that $\phi^{-1}:T\to\mathbb{R}^2:\phi^{-1}(f_{a,\,b})=(a,b)$ is an isomorphism.

Theorem 8 tells us that if $G_1\simeq G_2$, then $G_2\simeq G_1$. Let us use this result to prove the next theorem, which essentially reiterates what was noted in Remark 7.

Theorem 9: The relation R, given by $'G_1\,R\,G_2$ iff $G_1\simeq G_2'$, is an equivalence relation on the set of all groups.

Proof: First, let G be a group, then $I: G \to G: I(x) = x$ is an isomorphism. So $G \simeq G$. Hence, $'\simeq'$ is reflexive.

Next, if G_1, G_2 are groups such that $G_1 \simeq G_2$, then by Theorem 8, $G_2 \simeq G_1$. Hence, $'\simeq'$ is symmetric.

Finally, if $G_1 \simeq G_2$ and $G_2 \simeq G_3$, then by E19 you know that $G_1 \simeq G_3$. Hence, $'\simeq'$ is transitive.

Thus, $'\simeq'$ is an equivalence relation. ■

From Unit 1, and Theorem 9, you know that 'isomorphism' partitions the set of all groups into disjoint equivalence classes, called **isomorphism classes**. A lot of research and study in group theory is about finding the isomorphism class of a given group. This is because if we know which class a group G lies in, then G has all the algebraic properties of any group in that class. This helps us to understand G.

Now, as you have already seen, groups in the same isomorphism class have to have the same algebraic properties. For instance, S_3 and $\mathbb{Z}_6$ are both of order 6, but they are not in the same isomorphism class, i.e., $[S_3] \neq [\mathbb{Z}_6]$. (Why?). Also, Example 19 tells us that $[\mathbb{Z}] \neq [\mathbb{Q}]$. Consider a related example.

Example 20: Give an element of $[\mathbb{Z}_6]$, apart from $\mathbb{Z}_6$. Also, check if $[\mathbb{R}] = [\mathbb{Q}]$ or not.

Solution: Define $g: \mathbb{Z}_6 \to U_6 : g(\overline{1}) = \zeta$, where ζ is a primitive 6th root of unity. Extend g to all the elements of $\mathbb{Z}_6$ so that it becomes a homomorphism, i.e., $g(\overline{m}) = mg(\overline{1}) = \zeta^m$. Then you should show that g is an isomorphism.

So, $U_6 \in [\mathbb{Z}_6]$.

Next, you have seen in Unit 6, that every element of $\mathbb{Q}$ has finite order but not every element of $\mathbb{R}$ has finite order. Hence, $[\mathbb{R}] \neq [\mathbb{Q}]$.

***

Try some related exercises now.

E23) List 3 properties that groups in the same isomorphism class must share.

E24) Reference Remark 7, if $f: G \to H$ is an isomorphism of groups and G is abelian, then show that H is also abelian. Is the converse true? Why, or why not?

E25) Can a group and its proper subgroup lie in the same isomorphism class? Why, or why not?

E26) Check whether or not the relation $'\sim'$, given by $'G_1 \sim G_2$ iff there is a group homomorphism from G_1 to G_2' is an equivalence relation on the set of all groups.

E27) Let A_1, A_2, B_1, B_2 be groups s.t. $A_1 \simeq B_1$ and $A_2 \simeq B_2$. Show that $A_1 \times A_2 \simeq B_1 \times B_2$.

So far we have not really considered how to prove that $G_1 \not\simeq G_2$. In Example 19, you saw one way of disproving an isomorphism. Let us consider another way of doing this, using Theorem 7.

Example 21: Show that $(\mathbb{R}^*, \cdot)$ is not isomorphic to $(\mathbb{C}^*, \cdot)$.

Solution: Suppose they are isomorphic, and $f : \mathbb{C}^* \to \mathbb{R}^*$ is an isomorphism.
Then $o(i) = o(f(i))$, by Theorem 7. Now $o(i) = 4$. $\therefore o(f(i)) = 4$.
However, the order of any real number different from ± 1 is infinite, and $o(1) = 1, o(-1) = 2$.
So we reach a contradiction. Therefore, our supposition must be wrong. That is, $\mathbb{R}^*$ and $\mathbb{C}^*$ are not isomorphic.

***

In Example 21, we have again used the fact that isomorphic groups have the same algebraic properties. Use this to solve the following exercises.

E28) Show that $(\mathbb{C}^*, \cdot)$ is not isomorphic to $(\mathbb{R}, +)$.

E29) Is $\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$, for any $n \geq 2$? Why, or why not?

E30) Check whether or not $(\mathbb{Q}, +) \simeq (\mathbb{Q}^*, \cdot)$.

Let us now look at a very important theorem about isomorphism classes, and its applications. In Block 3, you will study its analogue in ring theory, and in the Linear Algebra course you will study its analogue for linear transformations.

8.4 THE ISOMORPHISM THEOREMS

In Unit 7, you studied about quotient groups. Over there we also told you that this concept was very important for group theory. Now you will study the reason behind this remark. We shall prove results about the relationship between homomorphisms and quotient groups. These theorems will give you a feel about the importance of quotient groups, and hence, of normal subgroups.

The first result is the **Fundamental Theorem of Homomorphism for groups**. You will see why this result is 'fundamental'. This result is also called **the first isomorphism theorem**.

First, let us look at a particular example to help you understand what the theorem talks about. Consider $f : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} : f(m) = \overline{m}$.
You know that f is the natural homomorphism, and $\text{Im } f = \mathbb{Z}/6\mathbb{Z}$. Now, what is $\text{Ker } f$?

$\text{Ker } f = \{m \in \mathbb{Z} \mid \overline{m} = \overline{0}\} = \{m \in \mathbb{Z} \mid m \in 6\mathbb{Z}\} = 6\mathbb{Z}$.

So, you can see that $(\mathbb{Z}/\text{Ker } f) \simeq \text{Im } f$ in this case; in fact, here $\mathbb{Z}/\text{Ker } f = \text{Im } f$.
Is this conclusion true only for this case? The following theorem answers this question.

We shall often abbreviate 'Fundamental Theorem of Homomorphism' to 'FTH'.

Theorem 10 (Fundamental Theorem of Homomorphism): Let G_1 and G_2 be two groups, and let $f : G_1 \to G_2$ be a group homomorphism. Then $(G_1/\text{Ker } f) \simeq \text{Im } f$.

In particular, if f is surjective, then $(G_1/\text{Ker } f) \simeq G_2$.

Proof: Let $\text{Ker } f = H$. You know that $H \triangleleft G_1$. Let us define the function $\psi : (G_1/H) \to \text{Im } f : \psi(Hx) = f(x)$.

At first glance it seems that the definition of ψ depends on the coset representative, x. If this is so, the function ψ may not be well-defined. So let us check if the definition of ψ is independent of the coset representative. That is, if $x, y \in G_1$ such that $Hx = Hy$, then is $\psi(Hx) = \psi(Hy)$? Let's see.

Now, $Hx = Hy \Rightarrow xy^{-1} \in H = \text{Ker } f \Rightarrow f(xy^{-1}) = e_2$, the identity of G_2.

$$\Rightarrow f(x)[f(y)]^{-1} = e_2 \Rightarrow f(x) = f(y)$$
$$\Rightarrow \psi(Hx) = \psi(Hy).$$

Therefore, ψ is a well-defined function.

Now, let us check that ψ is a homomorphism. For $Hx, Hy \in G_1/H$,

$$\begin{aligned}\psi((Hx)(Hy)) &= \psi(Hxy)\\ &= f(xy)\\ &= f(x)\,f(y), \text{ since } f \text{ is a homomorphism}\\ &= \psi(Hx)\,\psi(Hy).\end{aligned}$$

Therefore, ψ is a group homomorphism.

Next, let us see whether ψ is injective or not.

$$\begin{aligned}\text{Ker } \psi &= \{Hx \mid x \in G_1 \text{ and } f(x) = e_2\}\\ &= \{Hx \mid x \in \text{Ker } f\}\\ &= \{H\}, \text{ since Ker } f = H.\end{aligned}$$

Since H is the identity of G_1/H, ψ is injective (by Theorem 4).

Finally, let us see if ψ is surjective or not.

Any element of $\text{Im } f$ is $f(x) = \psi(Hx)$, where $x \in G_1$.

$\therefore \text{Im}\,\psi = \text{Im } f$.

So, we have proved that ψ is a bijective homomorphism, that is, an isomorphism. Thus, $(G_1/\text{Ker } f) \simeq \text{Im } f$.

In particular, if f is surjective, $\text{Im } f = G_2$. Thus, in this case $(G_1/\text{Ker } f) \simeq G_2$. ■

The situation in Theorem 10 is shown in Fig.1. Here, p is the natural homomorphism.

$$\begin{tikzcd}
G_1 \arrow[rr, "f"] \arrow[dr, "p"'] & & G_2 \\
& G_1/\text{Ker } f \arrow[ur, "\psi"'] &
\end{tikzcd}$$

Fig.1: $\psi \circ p = f$.

The diagram says that if you first apply p, and then ψ, to the elements of G_1, it is the same as applying f to them. That is, $\psi \circ p = f$.

Also, note that Theorem 10 says that **two elements of $\mathbf{G_1}$ have the same image under $\mathbf{f}$ iff they belong to the same coset of $\mathbf{Ker\ f}$.**

Let us now look at a few applications of the Fundamental Theorem of Homomorphism.

One of the simplest situations we can consider is $I_G : G \to G$, for any group G. On applying Theorem 10 here, we see that $\mathbf{G/\{e\} \simeq G}$, which you have already seen in Example 13. We will be using this identification of $G/\{e\}$ and G quite often.

Now, let us consider some non-trivial examples.

Example 22: You have seen that $\mathbb{C} \not\simeq \mathbb{R}$. However, is $\mathbb{C}/\mathbb{R} \simeq \mathbb{R}$? Why, or why not?

Solution: Define $f : \mathbb{C} \to \mathbb{R} : f(a + ib) = b$. Then, from E9 you know that f is a homomorphism and $\text{Ker } f = \mathbb{R}$. Also, you should show that $\text{Im } f = \mathbb{R}$. Therefore, on applying Theorem 10, we find that $\mathbb{C}/\mathbb{R} \simeq \mathbb{R}$.

***

Example 23: Use FTH to prove that $\mathbb{R}^5/\mathbb{R}^2 \simeq \mathbb{R}^3$, where $\mathbb{R}^m$ is the direct product of m copies of $\mathbb{R}$.

Solution: Define $\phi : \mathbb{R}^5 \to \mathbb{R}^3 : \phi[(a, b, c, d, e)] = (a, b, c)$. (We could also have defined ϕ s.t. $\phi(a, b, c, d, e) = (b, c, d)$, or any other such choice.)
If $(a_1, a_2, a_3, a_4, a_5) = (b_1, b_2, b_3, b_4, b_5)$ in $\mathbb{R}^5$, then $a_i = b_i \ \forall$ i. So $(a_1, a_2, a_3) = (b_1, b_2, b_3)$, i.e., $\phi[(a_1, \ldots, a_5)] = \phi[(b_1, \ldots, b_5)]$.
Thus, ϕ is well-defined.

Next, $\phi[(a_1, \ldots, a_5) + (b_1, \ldots, b_5)] = \phi[(a_1 + b_1, \ldots, a_5 + b_5)]$
$= (a_1 + b_1, a_2 + b_2, a_3 + b_3) = (a_1, a_2, a_3) + (b_1, b_2, b_3)$
$= \phi[(a_1, \ldots, a_5)] + \phi[(b_1, \ldots, b_5)]$.
Thus, ϕ is a group homomorphism.

Now $\text{Ker } \phi = \{(a, b, c, d, e) \in \mathbb{R}^5 \mid (a, b, c) = (0, 0, 0)\}$
$= \{(0, 0, 0, x, y) \mid x, y \in \mathbb{R}\} \simeq \mathbb{R}^2$, as in E22.
Also, verify that $\text{Im } \phi = \mathbb{R}^3$.
Hence, by FTH, $\mathbb{R}^5/\mathbb{R}^2 \simeq \mathbb{R}^3$.
(Note that as in Example 17, here $\mathbb{R}^2$ can be treated as a subgroup of $\mathbb{R}^5$, via i.)

***

Example 24: Consider $f:\mathbb{Z} \to (\{1, -1\}, \cdot) : f(n) = \begin{cases} 1, \text{ if } n \text{ is even,} \\ -1, \text{ if } n \text{ is odd.} \end{cases}$

In Example 1, you saw that f is a homomorphism. Obtain $\text{Ker } f$ and $\text{Im } f$. What does FTH say in this case?

Solution: Let $\mathbb{Z}_E$ and $\mathbb{Z}_O$ denote the set of even and odd integers, respectively. Then $\mathbb{Z}_E = 2\mathbb{Z}$ and $\mathbb{Z}_O = 1 + 2\mathbb{Z}$.

Here, $\text{Ker } f = \{n \in \mathbb{Z} \mid f(n) = 1\} = 2\mathbb{Z},$ and

$\text{Im } f = \{f(n) \mid n \in \mathbb{Z}\} = \{1, -1\}.$

Thus, by FTH, $\mathbb{Z}/2\mathbb{Z} \simeq \{1, -1\}.$

Note that this also tells us that $o(\mathbb{Z}/2\mathbb{Z}) = 2.$ The two cosets of $2\mathbb{Z}$ in $\mathbb{Z}$ are $2\mathbb{Z}$ and $1 + 2\mathbb{Z}.$

So, $(\{2\mathbb{Z}, 1 + 2\mathbb{Z}\}, +) \simeq (\{1, -1\}, \cdot).$

***

Example 25: Show that $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \simeq \mathbb{R}^*,$ where $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\}.$

Solution: From E3 you know that $f : GL_2(\mathbb{R}) \to \mathbb{R}^* : f(A) = \det(A)$ is a homomorphism, and $\text{Ker } f = SL_2(\mathbb{R}),$ $\text{Im } f = \mathbb{R}^*.$

Thus, using Theorem 10, $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \simeq \mathbb{R}^*.$

(Note that here we see another example of a non-abelian group G with an abelian quotient group.)

***

Example 26: Define $f:\mathbb{Z} \to \mathbb{Z}_n : f(m) = \overline{m}.$ Show that f is a homomorphism. What does the Fundamental Theorem tell us in this case?

Solution: Since $f(r+s) = \overline{r+s} = \overline{r} + \overline{s} \;\forall\; r, s \in \mathbb{Z},$ f is a homomorphism.

Next, any element of $\mathbb{Z}_n$ is $\overline{a},$ where $0 \le a < n,$ $a \in \mathbb{Z}.$

As $\overline{a} = f(a) \in \text{Im } f,$ $\mathbb{Z}_n = \text{Im } f.$

Now, $\text{Ker } f = \{m \in \mathbb{Z} \mid f(m) = \overline{0}\} = \{m \in \mathbb{Z} \mid m \in n\mathbb{Z}\} = n\mathbb{Z}.$

Hence, by Theorem 10, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$

***

What Example 26 tells us is that $\mathbb{Z}_n$ is the same as the quotient group $\mathbb{Z}/n\mathbb{Z}$ algebraically. You have noted this earlier too, in Unit 7. You will often call on this fact.

Now consider an important remark about FTH.

Remark 8: From the examples above, you can see that any epimorphism $f : G_1 \to G_2$ is actually the natural (or normal) homomorphism. This is because, by the FTH, $f : G_1 \to G_2$ is actually $p : G_1 \to (G_1/H),$ where $H = \text{Ker } f$ and $p(x) = Hx.$

This is why the map in Example 7 is called the 'canonical', meaning 'standard', homomorphism. This is also the reason why Theorem 10 is called the **Fundamental** Theorem of Homomorphism. It tells us that every homomorphism is essentially the canonical one.

Try solving the following exercises now.

E31) Let G be a group, and let $f : G \to G : f(g) = e,$ the identity of $G.$ Show that f is a homomorphism. What does the Fundamental Theorem of Homomorphism say in this case?

E32) What does FTH tell us in Example 2, Example 4(i) and (iii), Example 7 and Example 12?

E33) Let $m, n \in \mathbb{N}.$ Under what conditions on m and n is $\phi : \mathbb{Z}_m \to \mathbb{Z}_n : \phi(a + m\mathbb{Z}) = a + n\mathbb{Z}$ a well-defined homomorphism? And then, what does FTH tell us in this situation?

E34) Let S^1 be the circle group $\{z \in \mathbb{C} \,|\, |z| = 1\}.$ Show that $\mathbb{R}/\mathbb{Z} \simeq S^1.$

(**Hint:** See if Example 12 helps you.)

Now we will apply the Fundamental Theorem of Homomorphism to prove a very important result. This gives us the isomorphism classes of all cyclic groups.

Theorem 11: Any cyclic group is isomorphic to $(\mathbb{Z}, +)$ or $(\mathbb{Z}_n, +),$ for $n \in \mathbb{N}.$

Proof: Let $G = < x >$ be a cyclic group.

Define $f : \mathbb{Z} \to G : f(n) = x^n.$

Check that f is well-defined.

Also, f is a homomorphism because

$f(n+m) = x^{n+m} = x^n \cdot x^m = f(n)f(m) \;\forall\; n, m \in \mathbb{Z}.$

You should verify that $\text{Im}\, f = G.$

Now, we have two possibilities for $\text{Ker}\, f$ – either $\text{Ker}\, f = \{0\}$ or $\text{Ker}\, f \neq \{0\}.$

Case 1 $(\mathbf{Ker\ f = \{0\}})$**:** In this case f is 1-1. Therefore, f is an isomorphism. Therefore, by Theorem 8, f^{-1} is an isomorphism. That is, $G \simeq (\mathbb{Z}, +).$ Hence, G is infinite, and the order of x is infinite.

Case 2 $(\mathbf{Ker\ f \neq \{0\}})$**:** Since $\text{Ker}\, f \leq \mathbb{Z},$ from Unit 4 you know that $\text{Ker}\, f = n\mathbb{Z},$ for some $n \in \mathbb{N}.$ Therefore, by the Fundamental Theorem of Homomorphism, $\mathbb{Z}/n\mathbb{Z} \simeq G.$

$\therefore G \simeq (\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}_n, +).$

Over here note that since $< x > \simeq \mathbb{Z}_n,$ $o(x) = n.$ So, **a finite cyclic group is isomorphic to** $\mathbb{Z}_n,$ **where** n **is the order of the group**. ■

Let us consider some important and immediate corollaries of Theorem 11.

Corollary 3: Any two infinite cyclic groups are isomorphic. ■

Corollary 4: Any two finite cyclic groups of the same order are isomorphic. ■

We leave the proof of these corollaries to you, as an exercise (see E35).

And now let us look at an application of Theorem 11 and FTH.

Example 27: If $(m, n) = 1,$ prove that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$
Further, if A and B are cyclic groups of orders m and n, respectively, where $(m, n) = 1,$ then prove that $A \times B$ is cyclic of order $mn.$

Solution: Define $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n : f(r) = (r + m\mathbb{Z},\ r + n\mathbb{Z}).$
Note that f is well-defined because if $r = s$ in $\mathbb{Z},$ then $\bar{r} = \bar{s}$ in $\mathbb{Z}_m$ and in $\mathbb{Z}_n.$
Now, f is a homomorphism because

$$\begin{aligned} f(r+s) &= ((r+s) + m\mathbb{Z},\ (r+s) + n\mathbb{Z}) \\ &= (r + m\mathbb{Z}, r + n\mathbb{Z}) + (s + m\mathbb{Z},\ s + n\mathbb{Z}) \\ &= f(r) + f(s). \end{aligned}$$

Next, $\text{Ker } f = \{r \in \mathbb{Z} \,|\, (r + m\mathbb{Z},\ r + n\mathbb{Z}) = (0 + m\mathbb{Z},\ 0 + n\mathbb{Z})\}$

$= \{r \in \mathbb{Z} \,|\, r \in m\mathbb{Z} \cap n\mathbb{Z}\}$

$= \{r \in \mathbb{Z} \,|\, r \in mn\mathbb{Z}\},$ since $mn =$ l.c.m of m and n (see Unit 4).

$= mn\mathbb{Z}.$

Finally, we will show that f is surjective.
Let $(u + m\mathbb{Z},\ v + n\mathbb{Z}) \in \mathbb{Z}_m \times \mathbb{Z}_n.$
Since $(m, n) = 1, \exists\, s, t \in \mathbb{Z}$ such that $ms + nt = 1$ (see Unit 1).
Using this equation, we see that $f(u(1 - ms) + v(1 - nt)) = (u + m\mathbb{Z},\ v + n\mathbb{Z}),$
since $vms \in m\mathbb{Z}$ and $unt \in n\mathbb{Z}.$
i.e., $(u + m\mathbb{Z},\ v + n\mathbb{Z}) \in \text{Im } f.$
Thus, f is surjective.

Now, we apply the Fundamental Theorem of Homomorphism, to find that $(\mathbb{Z}/\text{Ker } f) \simeq \text{Im } f,$ that is, $(\mathbb{Z}/mn\mathbb{Z}) \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$
Hence, $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$

Now, let $A = \langle x \rangle$ and $B = \langle y \rangle,$ where $o(x) = m, o(y) = n.$ Then $A \simeq \mathbb{Z}_m$ and $B \simeq \mathbb{Z}_n,$ by Theorem 11.
Thus, by E27, $A \times B \simeq \mathbb{Z}_{mn},$ that is, $A \times B$ is cyclic, of order $mn.$

***

Try solving some exercises now.

E35) Prove Corollaries 3 and 4.

E36) Find all possible homomorphisms $f : \mathbb{Z}_8 \to U_{10}.$ For all such $f,$ find $\text{Ker } f.$

E37) i) If m and n are not coprime integers, is $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$? Why, or why not?

ii) Let ϕ be the Euler phi-function defined in Unit 4. Prove that if $m, n \in \mathbb{Z}$ such that $(m, n) = 1,$ then $\phi(mn) = \phi(m)\phi(n).$

We will now discuss **the second isomorphism theorem**. It is concerned with intersections and products of subgroups. Let us first understand what the theorem will tell us, through an example of S_3. Let $H = <(1\ 2)>$ and $K = <(1\ 2\ 3)>$. Then you know that $K \triangleleft S_3$. Therefore, from Unit 6, you know that $HK \le S_3$. In fact, $HK = S_3$. Also $H \cap K = \{I\}$. Now $H/(H \cap K)$ and $HK/K (= S_3/K)$ are both of the same order, 2. Is there any other relation between them? It turns out that both these groups are isomorphic, as the second isomorphism theorem will tell you.

Theorem 12 (Second Isomorphism Theorem): If H and K are subgroups of a group G, with K normal in G, then $(H/(H \cap K)) \simeq (HK/K)$.

Proof: We must first verify that the quotient groups $H/(H \cap K)$ and $(HK)/K$ are well-defined. From E25, Unit 6, you know that $H \cap K \triangleleft H$. Also, from Theorem 4 and E27 of Unit 6, you know that $HK \le G$, and that $K \triangleleft HK$. Thus, the given quotient groups are meaningful.

Now, what we want to do is to find an epimorphism $f : H \to (HK)/K$ with kernel $H \cap K$. Then we can apply the Fundamental Theorem of Homomorphism to get the required result.

So, let us define $f : H \to (HK)/K : f(h) = hK$.

You should verify that f is well-defined.

Now, for $x, y \in H$,

$f(xy) = xyK = (xK)(yK) = f(x)f(y)$.

Therefore, f is a homomorphism.

$\text{Im } f = \{f(h) | h \in H\} = \{hK | h \in H\}$.

We will show that $\text{Im } f = (HK)/K$.

For this, take any element $hK \in \text{Im } f$. Since $h \in H$, we see that $h \in HK$.

$\therefore hK \in (HK)/K$.

$\therefore \text{Im } f \subseteq (HK)/K$. …(1)

On the other hand, any element of $(HK)/K$ is of the form $hkK = hK$, where $h \in H, k \in K$.

$\therefore hkK = f(h) \in \text{Im } f$.

$\therefore ((HK)/K) \subseteq \text{Im } f$. …(2)

From (1) and (2), we get $\text{Im } f = ((HK)/K)$.

Finally, $\text{Ker } f = \{h \in H | f(h) = K\}$

$= \{h \in H | hK = K\}$

$= \{h \in H | h \in K\}$

$= H \cap K$.

Thus, on applying the Fundamental Theorem, we get $(H/(H \cap K)) \simeq (HK/K)$. ■

We would like to make a comment here about what Theorem 12 says for abelian groups.

Remark 9: If H and K are subgroups of $(G, +)$, then Theorem 12 says that $((H + K)/K) \simeq (H/(H \cap K))$.

Let us consider an example of how Theorem 12 is useful. Through this result, we look at the relationship between internal direct products and quotient groups.

Theorem 13: Let H and K be normal subgroups of a group G such that $\mathrm{G} = \mathrm{H} \times \mathrm{K}$. Then $(\mathrm{G}/\mathrm{H}) \simeq \mathrm{K}$ and $(\mathrm{G}/\mathrm{K}) \simeq \mathrm{H}$.

Proof: By definition, $\mathrm{G} = \mathrm{HK}$ and $\mathrm{H} \cap \mathrm{K} = \{\mathrm{e}\}$. Therefore,
$\mathrm{G}/\mathrm{H} = \mathrm{HK}/\mathrm{H} \simeq \mathrm{K}/\mathrm{H} \cap \mathrm{K} = \mathrm{K}/\{\mathrm{e}\} \simeq \mathrm{K}$.
You can similarly prove that $\mathrm{G}/\mathrm{K} \simeq \mathrm{H}$. ■

We now give a result which immediately follows from Theorem 13.

Corollary 5: Let G be a finite group and H and K be its normal subgroups such that $\mathrm{G} = \mathrm{H} \times \mathrm{K}$. Then $\mathrm{o}(\mathrm{G}) = \mathrm{o}(\mathrm{H})\mathrm{o}(\mathrm{K})$. ■

Now, why don't you use Theorems 12 and 13 to solve the following exercises?

E38) Prove Corollary 5.

E39) Let H and K be subgroups of a finite group G, and $\mathrm{H} \triangleleft \mathrm{G}$. Use Theorem 12 to show that $\mathrm{o}(\mathrm{HK}) = \dfrac{\mathrm{o}(\mathrm{H})\,\mathrm{o}(\mathrm{K})}{\mathrm{o}(\mathrm{H} \cap \mathrm{K})}$. (You have already proved this in Unit 3, of course!)

E40) Show that ${}^{3\mathbb{Z}}\!\big/_{12\mathbb{Z}} \simeq \mathbb{Z}_4$.
(**Hint:** Take $\mathrm{H} = 3\mathbb{Z}, \mathrm{K} = 4\mathbb{Z}$).

E41) Prove that if G_1 and G_2 are groups, then
$((\mathrm{G}_1 \times \mathrm{G}_2)/(\mathrm{G}_1 \times \{\mathrm{e}_2\})) \simeq \mathrm{G}_2$.

E42) Prove that $(\mathbb{Q}^3/\mathbb{Q}) \simeq \mathbb{Q}^2$.

And now for the third isomorphism theorem. This is also really an immediate application of FTH.

Theorem 14 (Third Isomorphism Theorem): Let H and K be normal subgroups of a group G such that $\mathrm{K} \subseteq \mathrm{H}$. Then ${}^{(\mathrm{G}/\mathrm{K})}\!\big/_{(\mathrm{H}/\mathrm{K})} \simeq \mathrm{G}/\mathrm{H}$.

Proof: First, note that from Theorem 7, Unit 7, you know that $(\mathrm{H}/\mathrm{K}) \triangleleft (\mathrm{G}/\mathrm{K})$. So the quotient groups given in the statement of the theorem are well-defined.

Now, to apply Theorem 10, we need to define a homomorphism from G/K onto G/H, whose kernel will turn out to be H/K.
Consider an obvious candidate, $\mathrm{f} : \mathrm{G}/\mathrm{K} \to \mathrm{G}/\mathrm{H} : \mathrm{f}(\mathrm{Kx}) = \mathrm{Hx}$.
f is well-defined because, for $\mathrm{x}, \mathrm{y} \in \mathrm{G}$,
$\mathrm{Kx} = \mathrm{Ky} \Rightarrow \mathrm{xy}^{-1} \in \mathrm{K} \subseteq \mathrm{H} \Rightarrow \mathrm{xy}^{-1} \in \mathrm{H} \Rightarrow \mathrm{Hx} = \mathrm{Hy} \Rightarrow \mathrm{f}(\mathrm{Kx}) = \mathrm{f}(\mathrm{Ky})$.
Now we leave the rest of the proof to you (see E43). ■

E43) Show that f, defined in the proof of Theorem 14, is an epimorphism and $\text{Ker } f = H/K.$ Hence complete the proof of Theorem 14.

E44) Prove that $(\mathbb{Z}_{10}/<\overline{5}>) \simeq \mathbb{Z}_5.$

Let us now discuss isomorphisms of a group onto itself.

8.5 AUTOMORPHISMS

Automorphisms are used very often in group theory. In fact, the set of automorphisms of a group has some special properties. Hence, we have devoted a separate section to discuss them. In this section, you will first see why the set of all automorphisms of a group forms a group. Then we shall define a special subgroup of this group, and see why it is important.

Automorphisms are not new to you. You are familiar with a basic automorphism, $I_G : G \to G,$ for any group $G.$ You also know that $\phi : G \to G : \phi(g) = g^{-1}$ is an automorphism of G iff G is abelian.

Let us now consider the set of automorphisms of a group $G,$

$\textbf{Aut G} = \{f : G \to G \mid f$ is an isomorphism$\}$.

You have just seen that $\text{Aut } G \neq \emptyset,$ since $I_G \in \text{Aut } G.$

From E19 you know that $\text{Aut } G$ is closed under the binary operation of composition.

Also, Theorem 8 says that if $f \in \text{Aut } G,$ then $f^{-1} \in \text{Aut } G.$

Thus, we have just proved the following theorem.

Theorem 15: Let G be a group. The set of automorphisms of $G, \text{Aut } G,$ is a group w.r.t. the composition of functions. ■

Let us look at some examples of $\text{Aut } G.$

Example 28: Show that $\text{Aut } \mathbb{Z} \simeq \mathbb{Z}_2.$

Solution: Let $f : \mathbb{Z} \to \mathbb{Z}$ be an automorphism. Let $f(1) = n.$ We will show that $n = 1$ or $-1.$

Since f is an onto function and $1 \in \mathbb{Z}, \exists\ m \in \mathbb{Z}$ such that $f(m) = 1,$ i.e., $mf(1) = 1,$ i.e., $mn = 1.$

$\therefore n = 1$ or $n = -1.$

If $n = 1, f(m) = m\ \forall\ m \in \mathbb{Z},$ i.e., $f = I.$

If $n = -1, f(m) = -m\ \forall\ m \in \mathbb{Z},$ i.e., $f = -I.$

Thus, there are only two elements in $\text{Aut } \mathbb{Z}, I$ and $-I.$

So $\text{Aut } \mathbb{Z} = < -I > \simeq \mathbb{Z}_2,$ by Theorem 11.

***

Now, given an element of a group $G,$ we will define an automorphism of G corresponding to it, in the next example.

Example 29: Let G be a group and $g \in G.$ Define $f_g : G \to G : f_g(x) = gxg^{-1}.$ Show that f_g is an automorphism of $G.$ (The element $gxg^{-1} \in G$ is called the **conjugate** of x by $g.$)

Solution: We will show that f_g preserves the operation on $G,$ and is a bijection.

$\mathbf{f_g}$ **is well-defined:** If $x = y$ in $G,$ then $gxg^{-1} = gyg^{-1},$ i.e., $f_g(x) = f_g(y).$ Thus, f_g is well-defined.

$\mathbf{f_g}$ **is a homomorphism:** If $x, y \in G,$ then

$$\begin{aligned} f_g(xy) &= g(xy)g^{-1} \\ &= gx(g^{-1}g)yg^{-1}, \text{ since } g^{-1}g = e, \text{ the identity of } G. \\ &= (gxg^{-1})(gyg^{-1}) \\ &= f_g(x)f_g(y). \end{aligned}$$

Thus, f_g is a homomorphism, $\forall\ g \in G.$

$\mathbf{f_g}$ **is 1-1:** $$\begin{aligned} \text{Ker } f_g &= \{x \in G \mid f_g(x) = e\} = \{x \in G \mid gxg^{-1} = e\} \\ &= \{x \in G \mid x = e\} \\ &= \{e\}. \end{aligned}$$

Hence, f_g is injective, $\forall\ g \in G.$

$\mathbf{f_g}$ **is surjective:** If $y \in G,$ then

$$\begin{aligned} y &= (gg^{-1})y(gg^{-1}) = g(g^{-1}yg)g^{-1} \\ &= f_g(g^{-1}yg) \in \text{Im } f_g, \text{ since } g^{-1}yg \in G. \end{aligned}$$

Hence, f_g is an onto function, $\forall\ g \in G.$

Thus, f_g is an automorphism of $G, \forall\ g \in G.$

***

Consider the following remark in the context of conjugation.

Remark 10: If G is an abelian group, then $f_g(x) = g + x - g = x\ \forall\ g \in G.$ Thus, $f_g = I\ \forall\ g \in G.$

We give the automorphism in Example 29 a special name.

Definition: Let G be a group and $g \in G.$ The automorphism $f_g : G \to G : f_g(x) = gxg^{-1}$ is called the **inner automorphism** of G **induced by the element** $\mathbf{g}$ in $G.$

The subset of $\text{Aut } G,$ consisting of all inner automorphisms of $G,$ is denoted by $\mathbf{Inn\ G}$.

Let us consider examples of some inner automorphisms.

Example 30: Consider $S_3.$ Compute $f_g(I), f_g((1\,3))$ and $f_g((1\,2\,3)),$ where $g = (1\,2).$ Also verify that $\text{Im } f_g = S_3$ and $\text{Ker } f_g = \{I\}.$

Solution: Note that $(1\ 2)^{-1} = (1\ 2)$. So $g^{-1} = g$.

Now, $f_g(I) = g \circ I \circ g^{-1} = I$,

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

$f_g((1\ 2\ 3)) = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$.

[In all these cases, note that if $\sigma \in S_3$ is a cycle of length 2 (or 3), then $g\sigma g^{-1}$ is also a cycle of length 2 (or 3, respectively). In Unit 9, you will see why this is so.]

Note that $\text{Im } f_g = \{f_g(\sigma) \mid \sigma \in S_3\} = \{g\sigma g^{-1} \mid \sigma \in S_3\}$.

You should verify that $f_g((2\ 3)) = (1\ 3), f_g((1\ 2)) = (1\ 2)$ and $f_g((1\ 3\ 2)) = (1\ 2\ 3)$.

Hence, $\text{Im } f_g = S_3$, and

$\text{Ker } f_g = \{\sigma \in S_3 \mid g\sigma g^{-1} = I\} = \{I\}$.

***

Solving the following exercises will give you some practice in obtaining inner automorphisms.

E45) Let G be a group and $g \in G$. Define $f : G \to G : f(x) = gx$. Does $f \in \text{Aut } G$? Why, or why not?

E46) Is $\text{Inn } G$ abelian for every G? If G is non-abelian, is $\text{Aut } G$ non-abelian? Give reasons for your answers.

E47) Let G be a group and $H \le G$. Show that $f_g(H) \subseteq H \ \forall \ g \in G$ iff $H \triangleleft G$. In particular, if $x \in G$ such that $f_g(x) = x \, \forall g \in G$, then show that $< x > \triangleleft G$.

E48) Verify that the image of $f_g \in \text{Inn } G$ is G, where

i) $G = GL_2(\mathbb{R})$ and $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$,

ii) $G = \mathbb{Z}$ and $g = 3$,

iii) $G = \mathbb{Z}/5\mathbb{Z}$ and $g = \overline{4}$,

iv) $G = Q_8$ and $g = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ (see Example 5, Unit 5).

E49) Is $|G| = |\text{Inn } G| \ \forall \ G$? Why?

So, we have a subset, $\text{Inn } G$, of $\text{Aut } G$ that seems to be in 1-1 correspondence with G, given by $f_g \mapsto g$. But, you have shown in E49 that this is not a 1-1 correspondence. So, the question is – is there any relationship between G and $\text{Inn } G$? To understand this, let us first see whether $\text{Inn } G$ has any group structure on it. It turns out that not only is $\text{Inn } G$ a group, it is something more!

Theorem 16: For any group G, $\text{Inn } G$ is a normal subgroup of $\text{Aut } G$.

Proof: $\text{Inn } G$ is non-empty, because $I_G = f_e \in \text{Inn } G$, where e is the identity in G.

Now, let us see if $f_g \circ f_h \in \text{Inn } G$ for $g, h \in G$.

For any $x \in G$, $f_g \circ f_h(x) = f_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1}$
$$= f_{gh}(x)$$

Thus, $f_g \circ f_h = f_{gh}$. …(3)

So, $\text{Inn } G$ is closed under composition.

Also $f_e = I_G$ is the identity in $\text{Inn } G$.

Now, for $f_g \in \text{Inn } G$, $\exists\, f_{g^{-1}} \in \text{Inn } G$ such that

$f_g \circ f_{g^{-1}} = f_{gg^{-1}} = f_e = I_G$, using (3).

Thus, $f_{g^{-1}} = (f_g)^{-1}$, that is, every element of $\text{Inn } G$ has an inverse in $\text{Inn } G$.

Thus, $\text{Inn } G \le \text{Aut } G$.

Now, to prove that $\text{Inn } G \lhd \text{Aut } G$, let $\phi \in \text{Aut } G$ and $f_g \in \text{Inn } G$.

Then, for any $x \in G$,

$$\begin{aligned}\phi^{-1} \circ f_g \circ \phi(x) &= \phi^{-1} \circ f_g(\phi(x))\\ &= \phi^{-1}(g\phi(x)g^{-1})\\ &= \phi^{-1}(g)\phi^{-1}(\phi(x))\phi^{-1}(g^{-1})\\ &= \phi^{-1}(g)x[\phi^{-1}(g)]^{-1}\\ &= f_{\phi^{-1}(g)}(x). \text{ (Note that } \phi^{-1}(g) \in G.)\end{aligned}$$

$\therefore \phi^{-1} \circ f_g \circ \phi = f_{\phi^{-1}(g)} \in \text{Inn } G\ \forall\ \phi \in \text{Aut } G$ and $f_g \in \text{Inn } G$.

$\therefore \text{Inn } G \lhd \text{Aut } G$. ■

Let us find $\text{Inn } G$ in some cases to give you a better feel about this normal subgroup.

Example 31: Find $\text{Inn } \mathbb{R}$ and $\text{Inn } \mathbb{Z}_n\ \forall\ n \in \mathbb{N}$.

Solution: Since $\mathbb{R}$ and $\mathbb{Z}_n$ are abelian $\forall\ n \in \mathbb{N}$, by Remark 10, $\text{Inn } \mathbb{R} = \{I\}$, and $\text{Inn } \mathbb{Z}_n = \{I\}\ \forall\ n \in \mathbb{N}$.

***

Before looking at more examples, let us consider an important theorem that will help us find $\text{Inn } G$, when G is not abelian. If you go back to Remark 10, it seems to suggest that the size of $\text{Inn } G$ gives a measure of how far G is from being commutative. Remember, this is also what $G/Z(G)$ tells us, where $Z(G)$ is the centre of G. So, is there some relationship between the factor group $G/Z(G)$ and the group $\text{Inn } G$? The following theorem will answer this question.

Theorem 17: Let G be a group. Then $(G/Z(G)) \simeq \text{Inn } G$.

Proof: As you may have guessed, we will use the powerful Fundamental Theorem of Homomorphism to prove this result. To do so, let us define $f : G \to \text{Inn } G : f(g) = f_g$, a natural choice!

f is well-defined: If $g_1 = g_2$ in G, then $g_1xg_1^{-1} = g_2xg_2^{-1}\ \forall\ x \in G$. So $f_{g_1}(x) = f_{g_2}(x)\ \forall\ x \in G$, i.e., $f_{g_1} = f_{g_2}$.

f is a homomorphism: For $g, h \in G$,

$$\begin{aligned} f(gh) &= f_{gh} \\ &= f_g \circ f_h, \text{ as noted in (3) of the proof of Theorem 16.} \\ &= f(g) \circ f(h). \end{aligned}$$

f is surjective: $\text{Im } f = \{f_g \mid g \in G\} = \text{Inn } G.$

Finding $\text{Ker } f$:
$$\begin{aligned} \text{Ker } f &= \{g \in G \mid f_g = I_G\} \\ &= \{g \in G \mid f_g(x) = x\ \forall\ x \in G\} \\ &= \{g \in G \mid gxg^{-1} = x\ \forall\ x \in G\} \\ &= \{g \in G \mid gx = xg\ \forall\ x \in G\} \\ &= Z(G). \end{aligned}$$

Therefore, by the Fundamental Theorem of Homomorphism, $(G/Z(G)) \simeq \text{Inn } G.$ ■

So, we had earlier mentioned a possible 1-1 correspondence between G and $\text{Inn } G$. Theorem 17 says this is only possible if $Z(G) = \{e\}$.

Now let us use Theorem 17 to consider some non-abelian examples of G.

Example 32: Find $\text{Inn } S_3$ and $\text{Inn } Q_8$.

Solution: You have seen earlier that $Z(S_3) = \{e\}$. Hence, by Theorem 17 $\text{Inn } S_3 \simeq S_3$.

You have also seen, in Unit 6, that $Z(Q_8) = \{\pm I\}$. Hence, $\text{Inn } Q_8 \simeq (Q_8/< -I >)$, which is of order 4.

Also, $f_I, f_A, f_B, f_{AB}(= f_C) \in \text{Inn } Q_8$, with $f_A^2 = I = f_B^2 = f_C^2$.

Hence, $\text{Inn } Q_8 = < f_A > \times < f_B >$ is the Klein 4-group.

***

Now you should use Theorem 17 to solve the following exercises.

E50) Find $\text{Inn } G$ for $G = D_8$ and $G = D_{10}$. More generally, what is $\text{Inn } D_{2n}$?

E51) If G is infinite, must $\text{Inn } G$ be infinite? Why, or why not?

With this we come to the end of this discussion on group homomorphisms of all kinds! As we said earlier, you will be working with them in later units too.

Let us take a brief look at what you have studied in this unit.

8.6 SUMMARY

In this unit, we have discussed the following points.

1. The definition, and examples, of a group homomorphism.

2. Let $f : G_1 \to G_2$ be a group homomorphism. Then
   i) $f(e_1) = e_2$,
   ii) $[f(x)]^{-1} = f(x^{-1}) \ \forall \ x \in G_1$,
   iii) $\text{Im } f \le G_2$,
   iv) $\text{Ker } f \lhd G_1$.

3. A homomorphism is 1-1 iff its kernel is the trivial subgroup.

4. The definition, and examples, of a group isomorphism.

5. Two groups are isomorphic iff they have exactly the same algebraic structure and properties.

6. The composition of group homomorphisms (respectively, isomorphisms) is a group homomorphism (respectively, isomorphism).

7. The proof, and many applications, of the Fundamental Theorem of Homomorphism (FTH), which says that if $f : G_1 \to G_2$ is a group homomorphism, then $(G_1/\text{Ker } f) \simeq \text{Im } f$.

8. Because of FTH, any group homomorphism $f : G_1 \to G_2$ is essentially the natural homomorphism $p : G_1 \to (G_1/\text{Ker } f)$. This is why the map p is called the natural, or canonical, map.

9. Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. Any finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$, $n \in \mathbb{N}$.

10. Let G be a group, $H \le G$, $K \lhd G$. Then $H/(H \cap K) \simeq (HK)/K$.

11. Let G be a group, $H \lhd G$, $K \lhd G$, $K \subseteq H$. Then $\frac{(G/K)}{(H/K)} \simeq G/H$.

12. The set of automorphisms of a group G, $\text{Aut } G$, is a group with respect to the composition of functions.

13. The definition, and examples, of an inner automorphism.

14. $\text{Inn } G \lhd \text{Aut } G$, for any group G.

15. $(G/Z(G)) \simeq \text{Inn } G$, for any group G.

8.7 SOLUTIONS / ANSWERS

E1) $I(gh) = gh = I(g)I(h) \ \forall \ g, h \in G$. So I is an endomorphism.
Also $I(g) = I(h) \Rightarrow g = h$. Hence, I is 1-1.
Thus, I is a group monomorphism.

E2) First, if $x = y$ in $\mathbb{R}^+$, then $\ln x = \ln y$, i.e., $f(x) = f(y)$. So f is well-defined.

For any $x, y \in \mathbb{R}^+, f(xy) = \ln(xy) = \ln x + \ln y = f(x) + f(y)$.

$\therefore f$ is a group homomorphism.

$\text{Ker } f = \{x \in \mathbb{R}^+ \mid f(x) = 0\} = \{1\}$.

$\text{Im } f = \{f(x) \mid x \in \mathbb{R}^*\} = \{\ln x \mid x \in \mathbb{R}^+\}$.

$= \mathbb{R}$ (because for any $r \in \mathbb{R}, f(e^r) = \ln(e^r) = r$).

E3) For any $A, B \in GL_2(\mathbb{R})$ s.t. $A = B$, $\det(A) = \det(B)$, i.e., $f(A) = f(B)$. Thus, f is well-defined.

Next, for $A, B \in GL_2(\mathbb{R})$,

$f(AB) = \det(AB) = \det(A)\det(B) = f(A)\,f(B)$.

$\therefore f$ is a homomorphism.

$\text{Ker } f = \{A \in GL_2(\mathbb{R}) \mid f(A) = 1\} = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\}$

$= SL_2(\mathbb{R})$.

$\text{Im } f = \{\det(A) \mid A \in GL_2(\mathbb{R})\}$

$= \mathbb{R}^*$ (because for any $r \in \mathbb{R}^*, \exists\ A = \begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$ such that

$\det(A) = r$).

E4) i) For $z_1, z_2 \in \mathbb{Z}, f(z_1 + z_2) = 5(z_1 + z_2) = 5z_1 + 5z_2 = f(z_1) + f(z_2)$.

Also, $f(z_1) = f(z_2) \Rightarrow 5z_1 = 5z_2 \Rightarrow z_1 = z_2$.

Thus, f is a 1-1 homomorphism.

So the given statement is true.

ii) False. Note that $\mathbb{R}^*$ is a group w.r.t. multiplication.

For $r_1, r_2 \in \mathbb{R}^*$, $f(r_1r_2) = 5r_1r_2 \neq f(r_1) \cdot f(r_2)$.

Hence, f is not a homomorphism. Hence, it is not a monomorphism.

iii) Check that $f(x + y) \neq f(x) + f(y)$. Hence, this is false.

iv) For $x, y \in \mathbb{R}^*, f(xy) = (xy)^2 = x^2y^2$, since $\mathbb{R}^*$ is abelian.

Hence, f is a homomorphism.

v) False. For example, consider $f : \mathbb{Z} \to 5\mathbb{Z} : f(z) = 5z$. In (i) you have shown that this is a homomorphism.

E5) $p : S_3 \to S_3/A_3 : p(x) = A_3x$.

Note that $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

Now, from Example 7, you know that $\text{Ker } p = A_3$. $\therefore (1\ 2) \notin \text{Ker } p$.

$\text{Im } p = \{A_3x \mid x \in S_3\}$. $\therefore (1\ 2) \notin \text{Im } p$.

E6) For any $x, y \in \mathbb{R}, f(x + y) = e^{2i(x+y)} = e^{2ix} \cdot e^{2iy}$

$= f(x) \cdot f(y)$.

$\therefore f$ is a homomorphism.

$$\text{Ker } f = \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid e^{2ix} = 1\}$$
$= \{x \in \mathbb{R} \mid 2x \in 2\pi\mathbb{Z}\},$ as you know from Unit 4 of Calculus.
$= \pi\mathbb{Z}.$

E7) From Example 7, you know that if we take $G_1 = G/H$ and take f to be the natural homomorphism $p: G \to (G/H),$ then $\text{Ker } f = H.$

E8) ϕ is not well-defined. For example, $\phi((1\ 3)) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H.$ Thus, ϕ cannot be a homomorphism from S_3 to $<(1\ 2)>$.

On the other hand, take K to be $<(1\ 2\ 3)>,$ and take ψ to be defined by $\psi(\sigma) = \sigma(1\ 2\ 3)\sigma^{-1}.$ You should show that ψ is a homomorphism. Here you could have taken K to be $\{e\}$ or S_3 also, and defined ψ appropriately. Then, too, ψ would be a homomorphism.

E9) First check that both f and g are homomorphisms.

Now, $g \circ f: \mathbb{C} \to \mathbb{C}: g \circ f(x + iy) = iy.$ So
$g \circ f[(x + iy) + (a + ib)] = g \circ f[(x + a) + i(y + b)] = i(y + b) = iy + ib$
$= g \circ f(x + iy) + g \circ f(a + ib),$ for $x, y, a, b \in \mathbb{R}.$
$\therefore g \circ f$ is a homomorphism.

Check that $\text{Ker } f = \mathbb{R} \subseteq \mathbb{C}, \text{Ker } g = \{0\}$ and $\text{Ker } (g \circ f) = \mathbb{R}.$
So $\text{Ker } (g \circ f) \subseteq \text{Ker } f$ and $\text{Ker } (g \circ f) \not\subset \text{Ker } g.$

Also $\text{Im } (g \circ f) = \{iy \mid y \in \mathbb{R}\}.$

E10) For any $\bar{r}, \bar{s} \in \mathbb{Z}_n,$
$f(\bar{r} + \bar{s}) = f(\overline{r + s}) = \zeta^{r+s} = \zeta^r \cdot \zeta^s = f(\bar{r}) \cdot f(\bar{s}).$
$\therefore f$ is a homomorphism.
$\text{Ker } f = \{\bar{r} \mid \zeta^r = 1\} = \{\bar{0}\}.$ Thus, f is injective.

$$\text{Im } f = \{f(\bar{r}) \mid \bar{r} \in \mathbb{Z}_n\}$$
$$= \{\zeta^r \mid 0 \le r \le n - 1\}$$
$$= U_n.$$
Hence, f is surjective.

E11) **f is well-defined:** If $g_1 = g_2,$ then $Hg_1 = Hg_2$ and $Kg_1 = Kg_2.$ Thus, $(Hg_1, Kg_1) = (Hg_2, Kg_2),$ i.e., $f(g_1) = f(g_2).$

f is a homomorphism: Let $g_1, g_2 \in G.$ Then
$$f(g_1g_2) = (Hg_1g_2, Kg_1g_2) = (Hg_1 \cdot Hg_2, Kg_1 \cdot Kg_2) = (Hg_1, Kg_1) \cdot (Hg_2, Kg_2)$$
$$= f(g_1) \cdot f(g_2).$$

$$\text{Ker } f = \{g \in G \mid Hg = H \text{ and } Kg = K\} = \{g \in G \mid g \in H \text{ and } g \in K\}$$
$$= H \cap K.$$

$\operatorname{Im} f = \{f(g) \mid g \in G\} = \{(Hg, Kg) \mid g \in G\}.$

f will be a monomorphism iff $\operatorname{Ker} f = \{e\}$, i.e., iff $H \cap K = \{e\}$.

f is **not** surjective, because for any $(Hg_1, Kg_2) \in G/H \times G/K$, with $g_1 \neq g_2$, there may be no $g \in G$ s.t. $Hg = Hg_1$ and $Kg = Kg_2$.
For instance, if $H = \{e_1\}$, $K = \{e_2\}$, then $Hg = Hg_1$ iff $g = g_1$. Similarly, $Kg = Kg_2$ iff $g = g_2$.

E12) **Proof of Corollary 1:** Let $G = < x >$ and $f: G \to G'$ be a homomorphism. Then $f: G \to f(G)$ is an onto homomorphism. Therefore, by Theorem 5, $f(G) = < f(x) >$, i.e., $f(G)$ is cyclic.

Proof of Corollary 2: Let $G = < S >$, where S is a finite set, and let $f: G \to G'$ be a homomorphism. Then $f(G)$ is the homomorphic image of G. So, by Theorem 5, $f(G) = < f(S) >$, where $f(S)$ is a finite set. Thus, $f(G)$ is finitely generated.

Converse of Corollary 1: If the homomorphic image of a group is cyclic, then the group is cyclic.
This is false. For instance, consider $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : f((x, 0)) = x.$
You have seen that f is a homomorphism which is surjective. Also, $\mathbb{Z}$ is cyclic, but $\mathbb{Z} \times \mathbb{Z}$ is not (as you have seen in Unit 4).

E13) **Statement:** If $f: G_1 \to G_2$ is a group homomorphism such that $f(G_1)$ is abelian, then G_1 is abelian.
This is false. Conside the situation in E5. There $p(S_3) = (S_3/A_3)$, which is of order 2. Hence, $p(S_3)$ is cyclic, and hence, abelian. But, as you know, S_3 is not abelian.

E14) Let G be a cyclic group, and G/H be a quotient group of G. Then, by Example 7 and Corollary 1, G/H is cyclic.

E15) The function $f: \mathbb{Z} \to n\mathbb{Z} : f(k) = nk$ is well-defined.
Now, $f(m + r) = n(m + r) = nm + nr = f(m) + f(r) \ \forall \ m, r \in \mathbb{Z}.$
$\therefore f$ is a homomorphism.

$\operatorname{Ker} f = \{0\}$. $\therefore f$ is 1-1.

$\operatorname{Im} f = n\mathbb{Z}$. $\therefore f$ is surjective.

$\therefore f$ is an isomorphism, and $\mathbb{Z} \simeq n\mathbb{Z}$.

E16) First, you should check that $G = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \middle| x \in \mathbb{R} \right\} \leq GL_2(\mathbb{R}).$

Now define $f: \mathbb{R} \to G : f(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}.$

Check that f is a well-defined epimomorphism.

Note that $\text{Ker } f = \left\{ x \in \mathbb{R} \middle| \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} = \{0\}$. So f is 1-1.

Thus, $\mathbb{R} \simeq G$.

E17) Show that f is a homomorphism, but not 1-1. $\therefore f$ is not an isomorphism.

E18) If f is a homomorphism, $f(ab) = f(a)f(b)$, i.e.,

$(ab)^{-1} = a^{-1}b^{-1} \; \forall \; a, b \in G$.

Thus, $b^{-1}a^{-1} = a^{-1}b^{-1} \; \forall \; a, b \in G$, i.e., G must be abelian.

Check that f is 1-1 and surjective.
Hence, f is an isomorphism only if G is abelian.

E19) By Theorem 2, $\theta \circ \phi$ is a homomorphism.

Now let $x \in \text{Ker}(\theta \circ \phi)$.
Then, $(\theta \circ \phi)(x) = 0$
$\Rightarrow \theta(\phi(x)) = 0$
$\Rightarrow \phi(x) = 0$, since θ is 1-1.
$\Rightarrow x = 0$, since ϕ is 1-1.
$\therefore \text{Ker}(\theta \circ \phi) = \{0\}$. $\therefore \theta \circ \phi$ is 1-1.

Finally, take any $k \in K$. Then $k = \theta(h)$, for some $h \in H$, since θ is onto.
Now, $h = \phi(g)$, for some $g \in G$, since ϕ is onto.
$\therefore k = \theta \circ \phi(g)$. $\therefore \theta \circ \phi$ is onto.
$\therefore \theta \circ \phi$ is an isomorphism.

E20) $\alpha \in G_1$ is a solution of $x^k = g_1$
$\Leftrightarrow \alpha^k = g_1$
$\Leftrightarrow [f(\alpha)]^k = f(g_1)$
$\Leftrightarrow f(\alpha) \in G_2$ is a solution of $x^k = f(g_1)$.
Hence the result.

E21) From Unit 4 you know that $o(\zeta^2) = \dfrac{15}{(15,\, 2)} = 15$. Hence, $U_{15} = <\zeta^2>$.

Now $f(\zeta^r \zeta^s) = \zeta^{2(r+s)} = \zeta^{2r} \cdot \zeta^{2s} = f(\zeta^r) f(\zeta^s)$.
So f is a homomorphism.

Also, $\text{Ker } f = \{\zeta^r \in U_{15} \,|\, \zeta^{2r} = 1\} = \{\zeta^r \in U_{15} \,|\, 15 | 2r\}$

$= \{\zeta^r \in U_{15} \,|\, 15 | r\}$, since $(15,\, 2) = 1$.

$= \{\zeta^{15}\}$

$= \{1\}$.

Finally, since $U_{15} = <\zeta^2>$, any element of U_{15} is of the form $\zeta^{2r} = f(\zeta^r)$, for some $r = 1, \ldots, 15$.
Hence, $\text{Im } f = U_{15}$.

Thus, f is an isomorphism.

E22) Let $f: G \to G \times \{e\}: f(x) = (x, e)$. Then verify that f is a well-defined group homomorphism.

$\text{Ker } f = \{e'\}$, where e' is the identity of G.

Also, $\text{Im } f = G \times \{e\}$.

Hence, f is an isomorphism.

Similarly, show that $\{e\} \times G \simeq G$.

E23) For instance, being cyclic, their cardinality, the number of distinct subgroups they have.
There are many other properties, which you should add.

E24) By Theorem 6, H is abelian.

The converse is: If $f: G \to H$ is an isomorphism and H is abelian, then so is G.
This is true, since f^{-1} is an isomorphism, by Theorem 8.

E25) Yes, as you have seen in E15.

E26) ~ is reflexive because $I_G: G \to G$ is a homomorphism, for any group G.
~ is symmetric because the zero homomorphism is defined from any group to another.
~ is transitive because the composition of homomorphisms is a homomorphism.

E27) Let $f: A_1 \to B_1$ and $g: A_2 \to B_2$ be isomorphisms. Define
$\theta: A_1 \times A_2 \to B_1 \times B_2 : \theta((x, y)) = (f(x), g(y))$.
Check that θ is a well-defined homomorphism. Also verify that
$\text{Ker } \theta = \text{Ker } f \times \text{Ker } g$

$= \{(e_1, e_2)\}$, where e_1, e_2 are the identities of A_1, A_2, respectively.

Further, check that $\text{Im } \theta = \text{Im } f \times \text{Im } g = B_1 \times B_2$.
Hence the result.

E28) Suppose $\mathbb{C}^* \simeq \mathbb{R}$ and $f: \mathbb{C}^* \to \mathbb{R}$ is an isomorphism. Then $o(f(i)) = 4$.
But, apart from 0, every element of $(\mathbb{R}, +)$ is of infinite order; and $o(0) = 1$. So, we reach a contradiction.
$\therefore \mathbb{C}^*$ and $\mathbb{R}$ are not isomorphic.

E29) Since $\mathbb{Z}$ is infinite and $\mathbb{Z}/n\mathbb{Z}$ is finite, the two groups can't be isomorphic.

E30) Note that $0 \in \mathbb{Q}$ is the only element of finite order, 1.

However, in $\mathbb{Q}^*$, (-1) is of order 2. Hence, $\mathbb{Q} \not\simeq \mathbb{Q}^*$.

E31) Note that f is well-defined. Check that $f(g_1g_2) = f(g_1)f(g_2)$.

Further, $\text{Ker } f = G$ and $\text{Im } f = \{e\}$.

Thus, $(G/G) \simeq \{e\}$.

You have already seen, and applied, the fact that $(G/G) = \{G\}$ (the identity) in Unit 7.

E32) Re Example 2, $\text{Im exp} = \mathbb{R}^+$, and $\text{Ker exp} = \{0\}$.
Thus, by the Fundamental Theorem of Homomorphism, and the fact that $(\mathbb{R}/\{0\}) \simeq \mathbb{R}^+$, $\mathbb{R} \simeq \mathbb{R}^+$.

Re Example 4(i), $\text{Im f} = < I_3 >$, where $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $\text{Ker f} = \{0\}$.

Thus, by FTH, $\mathbb{Z} \simeq < I_3 >$.

Re Example 4(iii), $\text{Ker f} = \{z \in \mathbb{C}^* \,\|\, |z| = 1\} = S^1$, the unit circle.

$\text{Im f} = \mathbb{R}^+$.

Thus, by FTH, $(\mathbb{C}^*/S^1) \simeq \mathbb{R}^+$.

Re Example 7, we find $(G/H) \simeq (G/H)$.

Re Example 12, we see that $\mathbb{R}/_{2\pi\mathbb{Z}} \simeq S^1$.

E33) If $a + m\mathbb{Z} = b + m\mathbb{Z}$, for $a, b \in \mathbb{Z}$, then $m \,|\, (a - b)$.
We need $n \,|\, (a - b)$ for ϕ to be well-defined. This will be true if $n|m$.
And then, $\bar{a} = \bar{b}$ in $\mathbb{Z}_n$, i.e., $\phi(\bar{a}) = \phi(\bar{b})$.
[Note that if $m|n$ this need not be true. Take, for example, $\phi : \mathbb{Z}_2 \to \mathbb{Z}_6$.
Then $\bar{1} = \bar{3}$ in $\mathbb{Z}_2$, but not in $\mathbb{Z}_6$.]
So, let us now assume that $n|m$. Then

$$\begin{aligned}\phi(\bar{a} + \bar{b}) = \phi(\overline{a + b}) &= (a + b) + n\mathbb{Z} \\ &= (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \\ &= \phi(a + m\mathbb{Z}) + \phi(b + m\mathbb{Z}).\end{aligned}$$

Thus, ϕ is a homomorphism.

$$\begin{aligned}\text{Ker } \phi &= \{a + m\mathbb{Z} | \bar{a} = \bar{0} \text{ in } \mathbb{Z}_n\} = \{a + m\mathbb{Z} | a \in n\mathbb{Z}\} \\ &= n\mathbb{Z}_m.\end{aligned}$$

$\text{Im } \phi = \mathbb{Z}_n$, since for any $a + n\mathbb{Z}$, $\exists\ a + m\mathbb{Z}$ s.t. $\phi(a + m\mathbb{Z}) = a + n\mathbb{Z}$.
Hence, by FTH, $(\mathbb{Z}_m/< n >) \simeq \mathbb{Z}_n$.
Thus, $\mathbb{Z}_m/_{n\mathbb{Z}_m} \simeq \mathbb{Z}/_{n\mathbb{Z}}$, where $n|m$.

E34) Define $f : \mathbb{R} \to S^1 : f(x) = e^{2\pi i x}$. Then f is well-defined because $e^{2\pi i x} \in S^1\ \forall\ x \in \mathbb{R}$, as $|e^{2\pi i x}| = |\cos 2\pi x + i \sin 2\pi x| = 1$.
Now $f(x + y) = e^{2\pi i (x+y)} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x)f(y)$.
$\therefore f$ is a homomorphism.

Note that any element of S^1 is of the form

$$\cos\theta + i\sin\theta = \cos 2\pi\frac{\theta}{2\pi} + i\sin 2\pi\frac{\theta}{2\pi} = f\left(\frac{\theta}{2\pi}\right),\text{ where } \theta \in \mathbb{R}.$$

$\therefore f$ is onto.

Also, $\text{Ker } f = \{x \in \mathbb{R} \mid e^{2\pi i x} = 1\}$

$= \{x \in \mathbb{R} \mid \cos 2\pi x + i\sin 2\pi x = 1\}$

$= \mathbb{Z}$, since $\cos\theta + i\sin\theta = 1$ iff $\theta \in 2\pi\mathbb{Z}$.

Therefore, by the Fundamental Theorem of Homomorphism, $(\mathbb{R}/\mathbb{Z}) \simeq S^1$.

E35) **Proof of Corollary 3:** Let A and B be infinite cyclic groups. Then, by Theorem 11, $A \simeq \mathbb{Z}$, $B \simeq \mathbb{Z}$. Hence, by Theorem 9, $A \simeq B$.

Proof of Corollary 4: Let A and B be cyclic groups of order n. Then $A \simeq \mathbb{Z}_n$, $B \simeq \mathbb{Z}_n$. Thus, by Theorem 9, $A \simeq B$.

E36) $U_{10} \simeq \mathbb{Z}_{10}$, by Theorem 11.

Now, if $\exists\, f : \mathbb{Z}_8 \to \mathbb{Z}_{10}$, then by the FTH, $(\mathbb{Z}_8/\text{Ker } f) \simeq \text{Im } f \le \mathbb{Z}_{10}$.

So, $o(\mathbb{Z}_8/\text{Ker } f) = 1, 2, 5$ or 10, by Lagrange's Theorem.

Also $o(\mathbb{Z}_8/\text{Ker } f) = \dfrac{8}{o(\text{Ker } f)}$. Hence, $o(\mathbb{Z}_8/\text{Ker } f) = 1, 2, 4$ or 8.

Putting both these possibilities together, we get $o(\mathbb{Z}_8/\text{Ker } f) = 1$ or 2, so that $o(\text{Ker } f) = 8$ or 4, respectively.

If $o(\text{Ker } f) = 8$, $\text{Ker } f = \mathbb{Z}_8$, i.e., $f : \mathbb{Z}_8 \to \mathbb{Z}_{10} : f(\overline{m}) = \overline{0}$.

If $o(\text{Ker} f) = 4$, then $\text{Ker } f = <\overline{2}>$. So $\text{Im } f$ must be generated by an element of order 2. Hence, define $f : \mathbb{Z}_8 \to \mathbb{Z}_{10} : f(1(\text{mod } 8)) = 5(\text{mod } 10)$, and extend f to be a homomorphism. You should check that f is well-defined, i.e., if $\overline{x} = \overline{y}$ in $\mathbb{Z}_8$, then $\overline{5x} = \overline{5y}$ in $\mathbb{Z}_{10}$.

Thus, the possibilities are

$f : \mathbb{Z}_8 \to U_{10} : f(\overline{m}) = 1$ and $g : \mathbb{Z}_8 \to U_{10} : g(\overline{m}) = \zeta^{5m}$.

E37) i) No. For instance, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. It is generated by $(\overline{1}, \overline{0})$ and $(\overline{0}, \overline{1})$. But $\mathbb{Z}_4$ is cyclic.
Hence, they are not isomorphic.

ii) From Unit 4, you know that $\phi(mn)$ is the number of distinct generators of $\mathbb{Z}_{mn}$. Also $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, by Example 27.
Further, for each generator $\overline{x}$ of $\mathbb{Z}_m$, and $\overline{y}$ of $\mathbb{Z}_n$, $\{(\overline{x}, \overline{0}), (\overline{0}, \overline{y})\}$ is a distinct set of generators of $\mathbb{Z}_m \times \mathbb{Z}_n$.
Hence, $\phi(mn) = \phi(m)\phi(n)$.

E38) Since $(G/H) \simeq K$, $o(G/H) = o(K)$, i.e., $\dfrac{o(G)}{o(H)} = o(K)$.

$\therefore o(G) = o(H) \cdot o(K)$.

E39) By Theorem 12, $(HK/H) \simeq (K/(H \cap K))$.

$$\therefore \frac{o(HK)}{o(H)} = \frac{o(K)}{o(H \cap K)}, \text{ i.e., } o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

E40) Let $H = 3\mathbb{Z}$, $K = 4\mathbb{Z}$. By Theorem 12 we know that
$((H+K)/K) \simeq (H/(H \cap K))$.
Now $H + K = 3\mathbb{Z} + 4\mathbb{Z} = \mathbb{Z}$, since $(3, 4) = 1$ (see Unit 4).
Also $H \cap K = 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$, since l.c.m $(3, 4) = 12$ (see Unit 4).
Thus, by Theorem 12, $\mathbb{Z}/4\mathbb{Z} \simeq 3\mathbb{Z}/12\mathbb{Z}$.
You also know that $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4$.
$\therefore 3\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_4$.

E41) $G_1 \times G_2 \simeq (G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$, as you have seen in Example 11, Unit 6.
Thus, by Theorem 13, $(G_1 \times G_2)/(G_1 \times \{e_2\}) \simeq \{e_1\} \times G_2 \simeq G_2$, by E22.

E42) $\mathbb{Q}^3 = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ and $\mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q}$.
Define $f : \mathbb{Q}^3 \to \mathbb{Q}^2 : f[(a, b, c)] = (a, b)$.
Check that f is well-defined.

Now, for (a, b, c) and (p, q, r) in $\mathbb{Q}^3$,

$$\begin{aligned} f[(a, b, c) + (p, q, r)] &= f[(a+p, b+q, c+r)] = (a+p, b+q) \\ &= (a, b) + (p, q) \\ &= f[(a, b, c)] + f[(p, q, r)]. \end{aligned}$$

Hence, f is a homomorphism.

$$\begin{aligned} \text{Ker } f &= \{(a, b, c) \in \mathbb{Q}^3 \mid (a, b) = (0, 0)\} \\ &= \{(0, 0, c) \mid c \in \mathbb{Q}\} \\ &\simeq \mathbb{Q}, \text{ as in E22.} \end{aligned}$$

Also $\text{Im } f = \mathbb{Q}^2$, since for any $(p, q) \in \mathbb{Q}^2$, $(p, q) = f[(p, q, 0)]$.
Thus, by Example 17 and FTH, $(\mathbb{Q}^3/\mathbb{Q}) \simeq (\mathbb{Q}^3/\text{Ker } f) \simeq \mathbb{Q}^2$.

E43) For any Kx, Ky in G/K,
$f((Kx)(Ky)) = f(Kxy) = Hxy = (Hx)(Hy) = f(Kx)f(Ky)$.
$\therefore f$ is a homomorphism.
Now, any element of G/H is of the form Hx. And
$Hx = f(Kx) \in \text{Im } f$.
$\therefore \text{Im } f = G/H$.

$$\begin{aligned} \text{Finally, Ker } f &= \{Kx \in G/K \mid f(Kx) = H\} \\ &= \{Kx \in G/K \mid Hx = H\} \\ &= \{Kx \in G/K \mid x \in H\} \\ &= H/K \end{aligned}$$

Therefore, by Theorem 10, $(G/K)/(H/K) \simeq G/H$.

E44) Note that $10\mathbb{Z} \le 5\mathbb{Z}$.
So, by Theorem 14, $(\mathbb{Z}/10\mathbb{Z}) / (5\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$

Also, ${}^{\mathbb{Z}}\!/_{10\mathbb{Z}} \simeq \mathbb{Z}_{10}$, ${}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \simeq \mathbb{Z}_5$ and ${}^{5\mathbb{Z}}\!/_{10\mathbb{Z}} = \bar{5}\mathbb{Z}_{10}$.

Hence the result.

E45) If f is a homomorphism, you know from Theorem 1 that $f(e) = e$. But here, $f(e) = g$.

Hence, $f \in \text{Aut } G$ iff $g = e$, and then $f = I_G$.

E46) If G is abelian, then $\text{Inn } G = \{I\}$. Hence, $\text{Inn } G$ is trivially abelian.

Now, suppose G is not abelian. Let $g, h \in G$ s.t. $gh \neq hg$.

Now $(f_g \circ f_h)(x) = f_g(hxh^{-1}) = ghxh^{-1}g^{-1} = f_{gh}(x) \; \forall \; x \in G$.

Hence, $f_g \circ f_h = f_{gh}$ and $f_h \circ f_g = f_{hg} \neq f_{gh}$.

Thus, $f_g \circ f_h \neq f_h \circ f_g$, i.e., $\text{Inn } G$ is not abelian.

Thus, $\text{Aut } G$ is not abelian in this case.

E47) For any $h \in H$ and $g \in G$,

$f_g(h) \in H \Leftrightarrow ghg^{-1} \in H \Leftrightarrow H \lhd G$.

E48) i) $f_g : GL_2(\mathbb{R}) \to GL_2(\mathbb{R}) : f_g\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = g\begin{bmatrix} a & b \\ c & d \end{bmatrix}g^{-1}$

Now, $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. $\therefore g^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

$\therefore g\begin{bmatrix} a & b \\ c & d \end{bmatrix}g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$.

Now, for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$, $\exists \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \in GL_2(\mathbb{R})$ s.t.

$f_g\left(\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

$\therefore f_g(GL_2(\mathbb{R})) = GL_2(\mathbb{R})$.

ii) $f_g : \mathbb{Z} \to \mathbb{Z} : f_g(x) = g + x + (-g) = x$.

$\therefore f_g = I$. $\therefore f_g(\mathbb{Z}) = \mathbb{Z}$.

iii) Here too, since G is abelian, $f_g = I$. Thus, $\text{Im } f_g = {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$.

iv) $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $C^{-1} = C^3 = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$.

Now $f_C(\pm I) = \pm I$.

Also $f_C(A) = CAC^{-1} = -A$, $f_C(-A) = A$,

$f_C(\pm B) = \mp B$, $f_C(\pm C) = \mp C$.

Hence, $\text{Im } f_C = Q_8$.

E49) If $G = \mathbb{Z}$, then $\text{Inn } G = \{I\}$. Hence, G is infinite, but $|\text{Inn } G| = 1$.

Hence, their cardinalities are not always equal.

E50) You have shown that $Z(D_8) = < R^2 >$ in E21, Unit 7. So $o(Z(D_8)) = 2$.

Hence, $o(\text{Inn } Q_8) = \frac{o(D_8)}{2} = 4$.

Also $\text{Inn } D_8$ is not cyclic, since by Theorem 5, Unit 7, $D_8 / Z(D_8)$ is not cyclic. You should verify that $\text{Inn } D_8$ is the Klein 4-group $\{I, f_r, f_{R^2}, f_{rR^2}\}$.

$Z(D_{10}) = \{e\}$. Hence, $\text{Inn } D_{10} \simeq D_{10}$.

In general, $Z(D_{2n}) = \{I, R_{n/2}\}$ if n is even, and $Z(D_{2n}) = \{e\}$ if n is odd. Thus, if n is even, $\text{Inn } D_{2n}$ is a non-cyclic group of order n.
If n is odd, $\text{Inn } D_{2n} \simeq D_{2n}$.

E51) No, e.g., $\text{Inn } \mathbb{Z} = \{I\}$.

UNIT 9

PERMUTATION GROUPS

Structure Page Nos.

9.1 INTRODUCTION

In this unit, we will discuss, in detail, a group that you studied briefly in Sec.1.5, Unit 1, and Sec.2.4.2, Unit 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 many examples. As you know, the symmetric groups and their subgroups are permutation groups. Historically, it was the study of permutation groups and groups of transformations that gave the foundation to group theory. A lot of work in the study of permutations was undertaken by several European mathematicians in the 18th century. However, the basis of this theory, and the notation that you will study, are mainly due to the French mathematician, Augustin-Louis Cauchy, whose partial theorem you also studied in Unit 7.

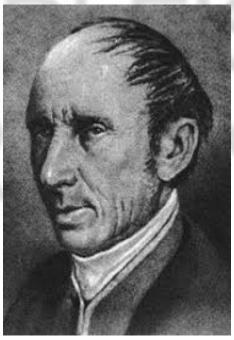

Fig.1: Cauchy (1789-1857)

In Sec.9.2, we will help you recapitulate what you have studied about permutations and permutation groups in Units 1 and 2.

In Sec.9.3, we shall look at several properties of elements of S_n. In particular, you will see why every element of S_n is a cycle or a product of disjoint cycles. Then you will study why 2-cycles generate S_n, for $n \geq 2$.

In Sec.9.4, the focus will be on certain permutations, called even permutations. You will see why the set of even permutations in S_n is a normal subgroup of S_n, called the alternating group. This group has several interesting properties, which you will also study.

Finally, in Sec.9.5, you will study a result by the famous mathematician, Cayley, which says that every group is isomorphic to a permutation group. Thus, every isomorphism class of groups can be represented by a permutation group. This result is what makes permutation groups so important.

Please study this unit carefully, because it gives you a solid basis for studying and understanding the theory of groups. We also suggest that you go through Sec.1.5 and Sec.2.4.2 again, before beginning work on this unit.

Objectives

After studying this unit, you should be able to:

- express any permutation in S_n as a product of disjoint cycles, and as a product of transpositions;
- find out whether an element of S_n is odd or even;
- prove that the alternating group of degree n, A_n, is normal in S_n and is of order $\frac{n!}{2}$;
- prove, and apply, the result that A_n is simple $\forall\ n \geq 5$;
- state, and prove, Cayley's theorem.

9.2 PRELIMINARIES

From Sec.1.5 (Unit 1) and Sec.2.4.2 (Unit 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 now gather some facts that you studied in Sec.2.4.2.
Suppose X is a finite set having n elements. For simplicity, we symbolise these elements by $1, 2, \ldots, n$. Then, you know that the set of all permutations on these n symbols is denoted by S_n.
You also know that we represent any $f \in S_n$ in a 2-line form as

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

How many elements do you think S_n has? To count them, look at f as in (1) above. Now, there are n possibilities for $f(1)$, namely, $1, 2, \ldots, n$. Once $f(1)$ has been specified, there are $(n-1)$ possibilities for $f(2)$, namely, $\{1, 2, \ldots, n\} \setminus \{f(1)\}$, since f is 1-1 and onto. Thus, there are $n(n-1)$ choices for $f(1)$ and $f(2)$. Continuing in this manner, you can see that there are $n!$ different possibilities for $f \in S_n$. Therefore, $\mathbf{S_n}$ **has** $\mathbf{n!}$ **elements**.

Now, let us look at the algebraic structure of $S(X)$, for any set X. From the course Calculus, you know that the composition of bijections from X to X is a bijection from X to X. Hence, if $f, g \in S(X)$, then $f \circ g \in S(X)$. So, composition is a binary operation on $S(X)$. To help you regain practice in computing the composition of permutations, consider an example.

Example 1: Find $f \circ g$, where $f = (1\ 2\ 4\ 3)$ and $g = (1\ 4\ 2)$ in S_4.

Solution: From Unit 2, you know that $f = (1\ 2\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, and

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

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. 2.

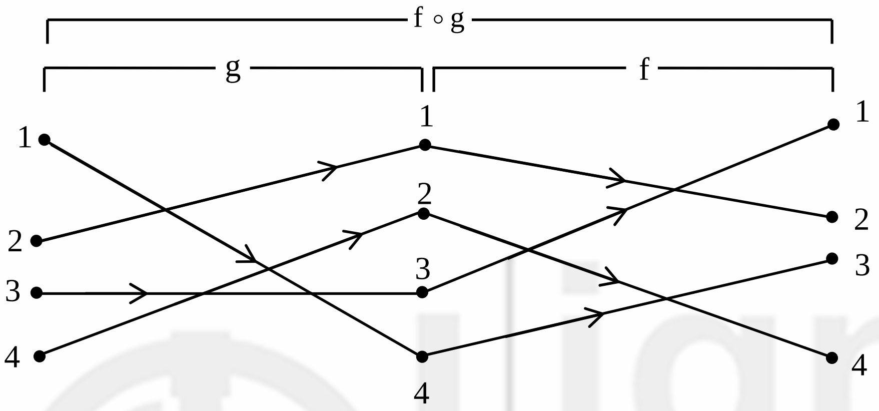

Fig. 2: $(1\ 2\ 4\ 3) \circ (1\ 4\ 2)$ **in** S_4.

***

Now, let us go back to $S(X)$, for any set X. You have studied the proof of the following result in Sec.2.4.2.

Theorem 1: Let X be a non-empty set. Then $(S(X), \circ)$ is a group, called the **permutation group on** $\mathbf{X}$. ■

Thus, S_n is a group of order $n!$. Recall, from Unit 2, that S_n is called the **symmetric group of degree** $\mathbf{n}$.

Now, from Unit 2, you also know that if $f \in S_n$, then

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

With the recap above, and the experience that you have gained in previous units, you should now solve the following exercises.

E1) Show that $(S_n, \circ)$ is a non-commutative group for $n \geq 3$.

E2) Show that $S_m \leq S_n$ if $m \leq n$.

E3) Let G be a group and let $g \in G$. Show that $f : G \to G : f(x) = gx$ is in $S(G)$. (f is called the **left regular representation** by g of G.)

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

Remark 1: In line with Remark 5 of Unit 2, 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 $\mathbf{f \circ g}$ as $\mathbf{fg}$,** unless we want to stress the operation involved.

The two-line notation that we have used for a permutation **of a finite set** is rather cumbersome. Let us see if there is a shorter notation. In case the permutation is a cycle, you know that we can denote it in one line only, as in Example 1.

Let us first recall how a cycle is written in one line from a 2-line format. Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ in S_4. 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 2: $(1\,3\,4\,2)$

Now, since no more symbols are left in f, we write $f = (1\ 3\ 4\ 2)$.

This means that a cycle maps each symbol to the symbol on its right, except for the final symbol in the brackets, which is mapped to the first symbol.

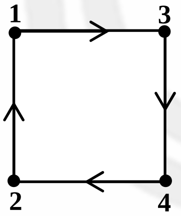

Fig. 3: (1 3 4 2).

If we had chosen 3 as our starting symbol, we would have got $f = (3\ 4\ 2\ 1)$. Note that this cycle is exactly the same as $(1\ 3\ 4\ 2)$, because both cycles show the same value for $f(i),\ i = 1,\ 2,\ 3,\ 4.$ Hence, they both denote the permutation which we have represented diagrammatically in Fig.3. This is an example of a 4-cycle, or a cycle of length $4.$ Fig.3 may give you some indication about why we call this function a cycle.

Now consider $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. You should check that $g = (1\ 2\ 4).$ But what happened to 3? Since $g(3) = 3,$ i.e., g fixes $3,$ we don't include it in the cycle representation of g.

More generally, we have the following definition.

If $f(s) = s,$ then we say f **fixes** s.
If $f(s) \neq s,$ we say that f **moves** s.

Definition: A permutation $f \in S_n$ is called an **r-cycle** (or **cycle of length r**), for $r \leq n,$ if there are r distinct integers $x_1,\ x_2,\ \ldots, x_r$ lying between 1 and n such that $f(x_i) = x_{i+1}\ \forall\ i = 1, \ldots, r-1,\ f(x_r) = x_1,$ and $f(k) = k\ \forall\ k \in \{1,\ 2, \ldots, n\} \setminus \{x_1,\ x_2,\ \ldots, x_r\}.$
Then, we write $\mathbf{f = (x_1\ x_2 \ldots x_r)}$.

In particular, a 2-cycle is called a **transposition**.

For example, the permutation $f = (2\ 3) \in S_3$ is a transposition. Here $f(1) = 1,\ f(2) = 3$ and $f(3) = 2.$

Note that, if we have $f = (2\ \ 3) \in S_7,$ then $f(2) = 3,\ f(3) = 2,$ and $f(k) = k$ for $k = 1,\ 4,\ 5,\ 6,\ 7.$

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

Consider the following important observation about 1-cycles.

Remark 2: Consider any 1-cycle, say $(3),$ in $S_4.$ (3) maps 3 to itself, and maps $1,\ 2$ and 4 to $1,\ 2$ and $4,$ respectively. Thus, $(3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I,$ the identity permutation. Thus, **any 1-cycle (i) in S_n is the identity permutation** $I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$ since it maps i to i and the other $(n-1)$ symbols to themselves.

You are already familiar with cycles in $S_3.$ You know that there are two 3-cycles, $(1\,2\,3)$ and $(1\,3\,2).$ There are also three transpositions in $S_3,$ namely, $(1\,2), (1\,3)$ and $(2\ 3).$ You have worked with these cycles in several examples and exercises of previous units. Now you can work with other cycles while solving the following exercises.

E4) Write down 2 distinct transpositions, 2 distinct 3-cycles and 2 distinct 7-cycles in $S_7.$ Justify your choices.

E5) Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$ as a cycle.

E6) i) Show that $(1\,2)^{-1} = (1\,2), (1\,2\,3)^{-1} = (3\,2\,1)$ and $(2\,5\,6\,8)^{-1} = (8\,6\,5\,2),$ in $S_8.$

ii) If $f = (i_1\ i_2 \dots i_r) \in S_n,\ n \geq r,$ then show that $f^{-1} = (i_r\ i_{r-1} \dots i_2\ i_1).$

E7) Give two distinct elements of $[G, G],$ where $G = S_4.$

Now that we have done a quick review of the basic concepts regarding permutations, let us discuss important properties of elements of $S_n.$

9.3 PROPERTIES OF PERMUTATIONS

From what you have studied in the previous section, you may think that we can express any permutation as a cycle. However, consider the following example from $S_5.$

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

Let us 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, and hence, we close the brackets, even though we have not yet written down all the symbols in g. So, are the leftover symbols, 2 and 5, fixed by g? No. We see that $g(2) \neq 2$ and $g(5) \neq 5$.

So, as the next step, we simply choose any 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 in $\{1, 2, 3, 4, 5\}$ are exhausted. So, what is g in terms of the cycles we have got? Let's see.

If we write $(1\ 3\ 4)(2\ 5)$ in the two-line format, what do we get?

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

which is the same as g.

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

We call this expression for g, as a product of two cycles that move different symbols, the **cycle decomposition** of g. In Fig.4 we represent this by a diagram which shows the decomposition clearly.

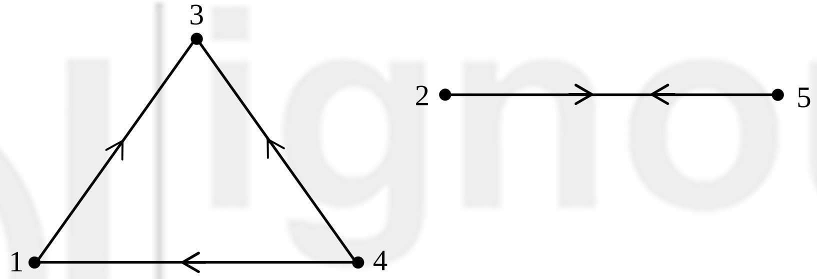

Fig. 4: $g = (1\ 3\ 4)\ (2\ 5)$.

Notice that the symbols in the two cycles that make up g form disjoint sets, $\{1, 3, 4\}$ and $\{2, 5\}$. Further, because of the arbitrary choice of the symbol at the beginning of each cycle, there are many ways of expressing g. For example,

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

However, **within each cycle, the same order has to be maintained**. For instance, we cannot replace $(4\,1\,3)$ by $(4\ 3\ 1)$, as $h = (4\ 3\ 1)(2\ 5)$ is a different function from g. Why? Note that $g(1) = 3$, but $h(1) = 4$.

So, we can write the product of the separate cycles with disjoint symbols in any order. The choice of the starting element within each cycle is arbitrary, ensuring that each cycle represents the same function.

So, you see that in this case g can't be written as a cycle, but as a product of cycles of the kind we now define.

Definition: Two cycles are called **disjoint** if they have no symbol in common.

Thus, disjoint cycles of length 2 or more move disjoint sets of symbols.
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.

Now let us consider one more example.

Example 2: Write $h=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 2 & 5 & 4\end{pmatrix}\in S_5$ as a cycle, or a product of disjoint cycles.

Solution: As we did for g above, we start with the symbol $1.$ However, 1 is fixed by $h.$ So, we ignore $1,$ and move to $2.$ We get the cycle $(2\ 3).$
Now consider $4,$ and we get the cycle $(4\ 5).$ Now all the symbols in h have been exhausted.
So $h=(2\ 3)(4\ 5).$
Note that, by convention, we don't include the 1-cycle in the expression for $h,$ unless we wish to emphasise it, since it is just the identity permutation.
Thus, we simply write $h=(2\ 3)(4\ 5),$ or $h=(4\ 5)(2\ 3),$ ignoring $(1).$

***

Let us now generalise what we have noted above about the disjoint cycles.

Theorem 2: If σ_1 and $\sigma_2\in S_n$ are disjoint cycles, then $\sigma_1\sigma_2=\sigma_2\sigma_1.$

Proof: Let $\sigma_1=(a_1\ a_2\ldots a_r)$ and $\sigma_2=(b_1\ b_2\ldots b_s),$ with $r+s\le n$ and $\{a_1,\ldots,a_r\}\cap\{b_1,\ldots,b_s\}=\emptyset.$

Let $\{1,2,\ldots,n\}=\{a_1,\ldots,a_r,\ b_1,\ldots,b_s,\ c_1,\ c_2,\ldots,c_k\}$ with $k=n-(r+s)\ge 0,$ and $\sigma_1(c_i)=c_i=\sigma_2(c_i)\ \forall\ i=1,\ldots,k.$

Now $\sigma_1\sigma_2(a_i)=\sigma_1(a_i),$ since $\sigma_2(a_i)=a_i\ \forall\ i=1,\ldots,r.$

$=a_{i+1}\ \forall\ i=1,\ldots,r,$ and putting $a_{r+1}=a_1.$

Also $\sigma_2\sigma_1(a_i)=\sigma_2(a_{i+1})=a_{i+1}\ \forall\ i=1,\ldots,r.$

Similarly, you can show that $\sigma_1\sigma_2(b_i)=\sigma_2\sigma_1(b_i)\ \forall\ i=1,\ldots,s,$ taking $b_{s+1}=b_1.$

Finally, $\sigma_1\sigma_2(c_i)=\sigma_1(c_i)=c_i$ and $\sigma_2\sigma_1(c_i)=c_i\ \forall\ i=1,\ldots,k.$

Thus, $\sigma_1\sigma_2(x)=\sigma_2\sigma_1(x)\ \forall\ x\in\{1,\ldots,n\}.$
Hence, $\sigma_1\sigma_2=\sigma_2\sigma_1.$ ■

Theorem 2 is why we had noted earlier that $g=(1\ 3\ 4)(2\ 5)=(2\ 5)(1\ 3\ 4).$

The process we have used earlier, to write g (and h in Example 2) as a product of disjoint cycles, can be used to write any permutation that moves a finite set of symbols in the same way.

Theorem 3 (Cycle decomposition): Every permutation of a finite set is either a cycle or a product of disjoint cycles.

Proof: Note that the identity permutation can be trivially seen as a 1-cycle, or a product of 1-cycles.
Now, $S_1=\{I\},\ S_2=\{I,\ (1\ 2)\},$ and you have also seen that every element of S_3 is a cycle.
So, let's assume $n\ge 4$ and $\sigma\in S_n$ is not a cycle. This means $\sigma\ne I.$

Let $x_1 \in \{1, 2, \ldots, n\}$ s.t. σ moves x_1, and let $x_2 = \sigma(x_1)$.

Then take $x_3 = \sigma(x_2) = \sigma(\sigma(x_1)) = \sigma^2(x_1)$, $x_4 = \sigma(x_3) = \sigma^3(x_1)$, and so on.

Since $\{1, 2, \ldots, n\}$ is finite, by this process symbols will start repeating at some point, say $\sigma^i(x_1) = \sigma^j(x_1)$ for some $i < j$.

If $r = j - i$, then $x_1 = \sigma^r(x_1)$.

Let m be the least positive integer s.t. $\sigma^m(x_1) = x_1$.

Then $\sigma_1 = (x_1\ x_2 \ldots x_m)$ is a cycle, and $\sigma(x_i) = \sigma_1(x_i)\ \forall\ i = 1, \ldots, m$.

Now take $y_1 \in \{1, 2, \ldots, n\} \setminus \{x_1, x_2, \ldots, x_m\}$, where σ moves y_1. Such a y_1 exists since σ is not a cycle.
Then, using the same process as above, we get
$\sigma_2 = (y_1\ y_2 \ldots y_s)$, for some $s \geq 2$, and where $y_i = \sigma^{i-1}(y_1)$ for $i = 1, \ldots, s$.

Are σ_1 and σ_2 disjoint? Suppose they are not. Then, for some i and j, we get $x_i = y_j$, i.e., $\sigma^{i-1}(x_1) = \sigma^{j-1}(y_1)$, i.e., $\sigma^{i-j}(x_1) = y_1$, i.e., $y_1 = x_{i-j+1}$, a contradiction to the way y_1 was chosen.

So σ_1 and σ_2 are disjoint.

We can continue the process by which we got σ_1 and σ_2 till all the symbols moved by σ are exhausted. Note that for each $i \in \{1, 2, \ldots, n\}$ s.t. $\sigma(i) = i$, the 1-cycle (i) is I. Hence, we do not include this in the decomposition.
So, we finally get $\sigma = \sigma_1\sigma_2 \ldots \sigma_t$ as a product of t disjoint cycles of lengths greater than 1. ■

Because of Theorem 3, any permutation in S_n, written in the 2-line format, can be more conveniently expressed as a cycle decomposition. Do you agree?
Also, because of Theorem 2, the order in which the cycles in a decomposition are written doesn't matter.

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

E8) Express each of the following permutations as products of disjoint cycles.

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

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

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

E9) Write $(1\ 4)(2\ 3) \in S_4$, $(6\ 5\ 2\ 4)(3\ 1) \in S_8$ and $(3\ 1\ 2)(4\ 6)(5\ 7) \in S_8$ in the two-line format.

E10) Do the cycles $(1\ 3)$ and $(1\ 5\ 4)$ in S_6 commute? Give reasons for your answer.

E11) If f 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 $f(i_1) = i_2, f^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_r$.)

From E11, you know what the order of a cycle is. So, using this, and the cycle decomposition of an element of S_n, can we obtain the order of an element of S_n easily? Consider an example.

Example 3: Find $o(g)$, where $g = (1\ 3\ 4)(2\ 5)$ in S_5.

Solution: Let $\sigma_1 = (1\ 3\ 4)$ and $\sigma_2 = (2\ 5)$.

Then $o(\sigma_1) = o((1\ 3\ 4)) = 3$, and $o(\sigma_2) = o((2\ 5)) = 2$.

Now, as seen in Theorem 2, $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

So $g^2 = (\sigma_1\sigma_2)^2 = \sigma_1^2\sigma_2^2 = \sigma_1^2 \neq I$, since $o(\sigma_1) = 3$ and $o(\sigma_2) = 2$.

Also, $g^3 = \sigma_1^2 g = \sigma_1^3\sigma_2 = \sigma_2$ since $o(\sigma_1) = 3$.

$\neq I$, since $o(\sigma_2) = 2$.

Similarly, you should verify that

$g^4 \neq I, g^5 \neq I, g^6 = \sigma_1^6\sigma_2^6 = (\sigma_1^3)^2(\sigma_2^2)^3 = I.$

Thus, $o(g) = 6 = \text{l.c.m}(o(\sigma_1), o(\sigma_2))$

$= \text{l.c.m}$ of the lengths of σ_1 and σ_2.

***

What you have found for g, in the example above, is true in general. This is what the following theorem tells us, which was proved by the Italian mathematician, Paolo Ruffini.

Fig.5: Paolo Ruffini (1765-1822)

Theorem 4: Let $\sigma \in S_n$, for $n \geq 3$. Let $\sigma = \sigma_1\sigma_2\ldots\sigma_r$, as a product of disjoint cycles. Then $o(\sigma)$ is the least common multiple of the lengths of $\sigma_1, \sigma_2, \ldots, \sigma_r$.

Proof: In E11 you have proved that the order of a cycle of length p is p.

Now, consider $\sigma = \sigma_1\sigma_2$, where σ_1 and σ_2 are disjoint cycles of lengths r and s, respectively. Thus, $o(\sigma_1) = r$ and $o(\sigma_2) = s$. Let $o(\sigma) = t$ and $\text{l.c.m}(r, s) = m$.

As $r \mid m$ and $s \mid m$, $\sigma_1^m = I = \sigma_2^m$.

$\therefore \sigma^m = \sigma_1^m\sigma_2^m$, since $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

$= I.$

Since $t = o(\sigma)$, we see that $t \mid m$. …(2)

Also $I = \sigma^t = \sigma_1^t\sigma_2^t$, so that $\sigma_1^t = \sigma_2^{-t} = (\sigma_2^{-1})^t$.

Since σ_1 and σ_2 are disjoint, so are σ_1 and σ_2^{-1}, and hence, σ_1^t and σ_2^{-t} are disjoint. Thus, they can only be equal if $\sigma_1^t = I = \sigma_2^{-t}$.

So, $r \mid t, s \mid t$.

Thus, $m \mid t$. …(3)

From (2) and (3), we conclude that $m = t$.

Let us now apply the strong principle of induction on the number of disjoint cycles in the product.

If σ is a cycle, or a product of 2 cycles, you have seen that the theorem is true.
Assume that the theorem is true for all permutations written as a product of $(r-1)$ cycles.

Now, let $\sigma = \sigma_1\sigma_2\ldots\sigma_r$ be a product of r disjoint cycles.

Then $\sigma = \rho\sigma_r$, where $\rho = \sigma_1\sigma_2\ldots\sigma_{r-1}$.

Hence, $o(\rho) = m = \text{l.c.m}$ of the lengths $\ell_1, \ell_2, \ldots, \ell_{r-1}$ of $\sigma_1, \sigma_2, \ldots, \sigma_{r-1}$, respectively.
Now, let ℓ_r be the length of σ_r and let $o(\sigma) = t$.
Then, as in the case for $r = 2$ above, you can show that
$t = \text{l.c.m}(m, \ell_r) = \text{l.c.m}(\ell_1, \ell_2, \ldots, \ell_r)$.
Hence, the result is true for a product of r disjoint cycles.
Thus, by the principle of induction, it is true in general. ■

Using Theorem 4, you can easily find the order of elements in S_n. Let us consider an example.

Example 4: Find the order of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 8 & 5 & 6 & 3 & 4 & 2 & 1 & 9 & 10 \end{pmatrix}$ in S_{10}.

Solution: Note that $\sigma = (1\ 7\ 2\ 8)(3\ 5)(4\ 6)$.

Thus, $\sigma = \sigma_1\sigma_2\sigma_3$, $\ell(\sigma_1) = 4$, $\ell(\sigma_2) = 2 = \ell(\sigma_3)$, where $\ell(\sigma) = \text{length}(\sigma)$.

Hence, $o(\sigma) = \text{l.c.m}(4, 2, 2) = 4$.

***

You can see how the cycle decomposition eases the process of finding the order of an element of S_n. Of course, this representation is also an elegant representation of a permutation in S_n!

Now consider an important property of a cycle, or a product of disjoint cycles.

Example 5(i) shows that **the conjugate of an r-cycle is an r-cycle**. Example 5(ii) tells us that **conjugation preserves the cycle structure** of a permutation.

Example 5: From Unit 6, you know that $\alpha, \beta \in S_n$ are conjugates if $\exists\ \sigma \in S_n$ s.t. $\alpha = \sigma\ \beta\ \sigma^{-1}$. For $\sigma \in S_n$, show that

i) if $\beta = (x_1\ x_2 \ldots x_r)$ in S_n, then $\sigma\beta\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ldots\sigma(x_r))$.

ii) if $\rho = \sigma_1\sigma_2\ldots\sigma_s$ as a product of disjoint cycles in S_n, then $\sigma\rho\sigma^{-1} = \alpha_1\alpha_2\ldots\alpha_s$, a product of disjoint cycles in S_n with $\text{length}(\alpha_i) = \text{length}(\sigma_i)\ \forall\ i = 1, \ldots, s$.

Solution: i) Note that $\sigma\beta\sigma^{-1}(\sigma(x_i)) = \sigma\beta(x_i) = \sigma(x_{i+1})\ \forall\ i = 1, \ldots, r$, taking $x_{r+1} = x_1$.
Also, let $y \in \{1, \ldots, n\} \setminus \{\sigma(x_1), \ldots, \sigma(x_r)\}$.
Then $y = \sigma(z)$ for some $z \neq x_i\ \forall\ i = 1, \ldots, r$, as σ is a 1-to-1 map of $\{1, \ldots, n\}$.
So $\sigma\beta\sigma^{-1}(y) = \sigma\beta\sigma^{-1}(\sigma(z)) = \sigma(z)$, as $\beta(z) = z$.
$\therefore \sigma\beta\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ldots\sigma(x_r))$, a cycle of length r.

ii) Let $\rho = \sigma_1\sigma_2\ldots\sigma_s$, as a product of disjoint cycles. Then by Example 29, Unit 8, you know that conjugation by σ is the inner automorphism f_σ.

$\therefore \sigma\rho\sigma^{-1} = (\sigma\sigma_1\sigma^{-1})(\sigma\sigma_2\sigma^{-1})\ldots(\sigma\sigma_s\sigma^{-1})$ …(4)

Also, by (i), $\sigma\sigma_i\sigma^{-1}$ only moves what σ_i moves.

Hence, (4) is a representation of $\sigma\rho\sigma^{-1}$ as a product of disjoint cycles in S_n, with $\text{length}(\sigma\sigma_i\sigma^{-1}) = \text{length}(\sigma_i)$.

***

What is proved in Example 5 is very useful, and will be used several times in this unit.

Try solving some related exercises now.

E12) Find $o(\sigma)$, where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 6 & 4 & 7 & 9 & 2 & 10 & 1 & 8 \end{pmatrix} \in S_{10}$.

E13) Give an example of cycles σ_1 and $\sigma_2 \in S_n$, where $o(\sigma_1\sigma_2) \neq \text{l.c.m}(\ell(\sigma_1), \ell(\sigma_2))$. Does Theorem 4 fail here? Why, or why not?

E14) If $\sigma \in S_n$, must we have $o(\sigma) \leq n$? Must $o(\sigma) \mid n$? Give reasons for your answers.

Now, let us discuss transpositions. Consider the cycle $(1\ 5\ 3)$ in S_5. You should verify that this is the same as the product $(1\ 3)(1\ 5)$. You should also verify that $(1\ 5\ 3) = (1\ 5)(5\ 3)$. Note that the transpositions in either product are not disjoint.

The same process can be used to show that **any r-cycle $(\mathbf{i_1\ i_2 \ldots i_r}) = (\mathbf{i_1\ i_r})\ (\mathbf{i_1\, i_{r-1}})\ldots(\mathbf{i_1\ i_2})$, a product of transpositions**.

Also $(\mathbf{i_1\ i_2 \ldots i_r}) = (\mathbf{i_1\ i_2})(\mathbf{i_2\ i_3})\ldots(\mathbf{i_{r-1}\ i_r})$, again a product of transpositions. Note that, since the transpositions aren't disjoint, they do not commute (see E16). Further, as you have seen above, t**he expression of a cycle as a product of transpositions is not unique**.

Before discussing the importance of transpositions, try solving the following exercises.

E15) Express the following cycles in S_5 as products of transpositions:

i) $(1\ 3\ 4)$, ii) $(4\ 3\ 1)$, iii) $(2\ 4\ 5\ 3)$.

E16) Show that $(i\ \ j)(j\ k) \neq (j\ k)(i\ \ j)$ in S_n, $n \geq 3$, for any three distinct symbols $i,\ j,\ k$.

Let us now use the cycle decomposition of a permutation to prove a result which shows why transpositions are so important in the theory of permutations.

Theorem 5: Every permutation in S_n, $n \geq 2$, can be written as a product of transpositions.

Proof: By Theorem 3, you know that every permutation is a product of one or more disjoint cycles. Also, you have just seen how every cycle is a product of transpositions. Hence, every permutation is a product of one or more transpositions.
Note that $I = (1\ 2)(1\ 2)$. Thus, I is also a product of transpositions. ■

Let us see how Theorem 5 works in practice, through an example.

Example 6: Write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 2 & 5 & 7 \end{pmatrix}$ as a product of transpositions.

Solution: $\sigma = (1\ 3\ 4)(2\ \ 6\ 5)$, as a product of disjoint cycles
$= (1\ 4)(1\ 3)(2\ 5)(2\ \ 6)$.

***

Consider the following important comment here.

Remark 3: Note that if $\sigma = \tau_1\tau_2 \ldots \tau_t$ as a product of transpositions, you **cannot conclude** that $o(\sigma) = 2$. Theorem 4 cannot be applied here. It holds only for a **disjoint** cycle decomposition, and here the τ_i are not disjoint.

Now, in Theorem 5 you have seen that **the set of transpositions in $\mathbf{S_n}$ generates $\mathbf{S_n}$.** In fact, there is a smaller set that generates S_n. Recall, from Unit 4, that a set S generates a group G if every element of G is of the form $s_1^{r_1}s_2^{r_2} \ldots s_n^{r_n}$, $s_i \in S$ and $r_i \in \mathbb{Z}$.

Theorem 6: $\{(1\ 2), (1\ 3), \ldots, (1\ n)\}$ generates S_n.

Proof: From Theorem 5, you know that any $\sigma \in S_n$ is a product of transpositions. Now take any transposition $(i\ \ j) \in S_n$. Then
$(i\ \ j) = (1\ i)(1\ \ j)(1\ i)$.
Hence, any $\sigma \in S_n$ is a product of transpositions of the form $(1\ r)$, for some $r \in \{1, \ldots, n\}$.
Thus, $\{(1\ 2), (1\ 3), \ldots, (1\ n)\}$ generates S_n. ■

In fact, an even smaller set than the one given in Theorem 6 generates S_n, $n \geq 3$, namely, $\{(1\ 2), (1\ 2 \ldots n)\}$. However, we will not prove this here.

Now you can try your hand at solving some exercises.

E17) Write the permutation in E8(ii) as a product of transpositions.

E18) Write $(1\ 3\ 4)(5\ 7)(2\ \ 6\ 8) \in S_8$ as a product of transpositions of the form $(1\ i)$, for some $i \in \{1, \ldots, 8\}$.

E19) Show that $(1\ 2)(2\ 3) \ldots (9\ 10) = (1\ \ 10)(1\ 9) \ldots (1\ 2)$.

E20) Is the set of all transpositions in S_n a subgroup of S_n? Why, or why not?

The decomposition given in Theorem 5 leads us to focus on a certain important subgroup of S_n that we will now discuss.

9.4 ALTERNATING GROUPS

You have seen that any permutation in S_n can be written as a product of transpositions. You have also seen that the factors in the product are not uniquely determined. Not only this, even the number of factors in the product can vary. For example, in S_4 we have $(1\ 2)(3 4)(1\ 4) = (1\ 2)(3\ 4)(2\ 3)(1\ 4)(3\ 2)$. Here the LHS has 3 transpositions, and the RHS has 5 transpositions. Can the RHS have $4,$ or $6,$ transpositions? Try to find any such representation.

Actually, all representations as a product of transpositions have one thing in common – if a permutation 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 will be a product of an even number of transpositions in any such representation. To see this fact, we first need to define a concept new to you.

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

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

$\prod_{i=1}^{n} \alpha_i = \alpha_1 \alpha_2 \dots \alpha_n$

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 we still need to include the factors involving $f(3)$ for obtaining the signature of f.

So, $\text{sign } f = \dfrac{f(2)-f(1)}{2-1} \cdot \dfrac{f(3)-f(1)}{3-1} \cdot \dfrac{f(3)-f(2)}{3-2}$ (Note that $f(3) = 3$ here.)

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

Try some simple exercises now to get used to the signature of a permutation.

E21) What is the signature of $I \in S_n$?

E22) Find the signature of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \in S_5.$

From the examples you have seen so far, you may have concluded that the signature is a function from S_n to $\mathbb{Z}.$ You will see that it is, in fact, a homomorphism from S_n to $(\{1, -1\}, \cdot).$ Let us first show that sign preserves the operation.

Theorem 7: $\text{sign}: S_n \to \mathbb{Q}^*$ is a well-defined homomorphism, where $n \ge 2$.

Proof: By definition, if $f, g \in S_n$ s.t. $f = g$, then $f(i) = g(i)\ \forall\ i = 1, \ldots, n$.

$\therefore \text{sign } f = \text{sign } g$ in $\mathbb{Q}^*$.

Thus, sign is well-defined.

Next, $\text{sign } (f \circ g) = \prod\limits_{\substack{i,\, j=1 \\ i<j}}^{n} \dfrac{f(g(j)) - f(g(i))}{j - i}$

$$= \prod_{\substack{i,\, j \\ i<j}} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \prod_{\substack{i,\, j \\ i<j}} \frac{g(j) - g(i)}{j - 1}. \qquad \ldots(5)$$

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. So f can be thought of as a permutation of $\{g(1), \ldots, g(n)\}$.

$\therefore \prod\limits_{i<j} \dfrac{f(g(j)) - f(g(i))}{g(j) - g(i)} = \text{sign } f.$

$\therefore$ (5) tells us that $\text{sign } (f \circ g) = (\text{sign } f)(\text{sign } g)$. ■

By Theorem 7, we know that, for instance,
$\text{sign}(1\ 2\ 3\ 4) = \text{sign}((1\ 2)(2\ 3)(3\ 4)) = \text{sign}\,(1\ 2) \cdot \text{sign}\,(2\ 3) \cdot \text{sign}\,(3\ 4)$.

You may think that this way of finding $\text{sign}(1\ 2\ 3\ 4)$ seems to be much longer than finding it directly. However, the following theorem, with Theorem 7, gives us properties of the signature function that shorten the process. Of course, let us not forget the crucial role of Theorem 5 in all this!

Theorem 8: Consider $\text{sign}: S_n \to \mathbb{Q}^*,\ n \ge 2$.

i) If $t \in S_n$ is a transposition, then $\text{sign}\, t = -1$.

ii) $\text{Im (sign)} = \{1, -1\}$.

Proof: i) Let $t = (p\ q)$, where $1 \le p < q \le n$. [To help you understand what is going on, you may like to work with $(1\ 2) \in S_n$, as you go through the proof.]

Now, only one factor of $\text{sign}\, t$ involves both p and q, namely,

$$\frac{t(q) - t(p)}{q - p} = \frac{p - q}{q - p} = -1. \qquad \ldots(6)$$

Every factor of $\text{sign}\, t$ that doesn't contain p or q equals 1, since

$$\frac{t(i) - t(j)}{i - j} = \frac{i - j}{i - j} = 1, \text{ if } i,\ j \ne p,\ q. \qquad \ldots(7)$$

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

$$\left.\begin{aligned} \frac{t(i) - t(p)}{i - p}\,\frac{t(i) - t(q)}{i - q} &= \frac{i - q}{i - p}\,\frac{i - p}{i - q} = 1, \text{ if } i > q, \\ \frac{t(i) - t(p)}{i - p}\,\frac{t(q) - t(i)}{q - i} &= \frac{i - q}{i - p}\,\frac{p - i}{q - i} = 1, \text{ if } q > i > p, \\ \frac{t(p) - t(i)}{p - i}\,\frac{t(q) - t(i)}{q - i} &= \frac{q - i}{p - i}\,\frac{p - i}{q - i} = 1, \text{ if } i < p. \end{aligned}\right\} \qquad \ldots(8)$$

Thus, taking the values of all the factors of $\text{sign } t,$ from (6), (7) and (8) you can see that $\text{sign } t = -1.$

ii) Let $f \in S_n$. By Theorem 5, you know that $f = t_1 t_2 \ldots t_r$ for some transpositions $t_1, \ldots, t_r$ in S_n.

$\therefore \text{sign } f = \text{sign}(t_1\ t_2 \ldots t_r)$

$= (\text{sign } t_1)\ (\text{sign } t_2) \ldots (\text{sign } t_r),$ by Theorem 7.

$= (-1)^r,$ by (i) above.

$\therefore \text{sign } f = 1$ or $-1,$ depending on whether r is even or odd.

Hence, $\text{Im (sign)} \subseteq \{1, -1\}.$

You also know that $\text{sign } t = -1,$ for any transposition $t,$ and $\text{sign } I = 1.$

$\therefore \{1, -1\} \subseteq \text{Im (sign)}.$

$\therefore \text{Im (sign)} = \{1, -1\}.$ ■

So Theorems 7 and 8 tell us that **$\mathbf{sign} : \mathbf{S_n} \to \{\mathbf{1}, -\mathbf{1}\}$ is an epimorphism**, $n \geq 2.$

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

Theorem 9: 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: Let us apply the function $\text{sign} : S_n \to \{1, -1\}$ to $f = t_1 t_2 \ldots t_r.$

By Theorem 8, you know that

$\text{sign } f = (\text{sign } t_1)\ (\text{sign } t_2) \ldots (\text{sign } t_r) = (-1)^r.$ …(9)

Also $f = t'_1 t'_2 \ldots t'_s.$

So $\text{sign } f = (-1)^s.$ …(10)

From (9) and (10) we get $(-1)^r = (-1)^s.$

This can only happen if both s and r are even, or both are odd.

Thus, the number of factors occurring in any factorisation of f into transpositions is always even, or always odd. ■

The theorem above leads us to the following definition.

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

For example, $(1\ 2) \in S_3$ is an odd permutation. In fact, any transposition is an odd permutation. On the other hand, any 3-cycle is an even permutation, since $(i\ \ j\ \ k) = (i\ \ k)(i\ \ j).$ So $\text{sign}(i\ \ j\ \ k) = (-1)(-1) = 1.$

Consider the following remark in this context.

Remark 4: What Theorems 8 and 9 tell us is that $f \in S_n$ is odd iff $\text{sign } f = (-1).$ Thus, $f \in S_n$ is even iff $\text{sign } f = 1.$

Now, here's your chance to work with some odd and even permutations.

E23) Which of the permutations in E15 and E18 are odd?

E24) If $f, g \in S_n$ are odd, then is $f \circ g$ odd too? Why?

E25) Is the identity permutation odd or even? Why?

Now we will consider an important subset of S_n, namely, $\mathbf{A_n} = \{f \in S_n | f$ is even}.
You will see that $A_n \lhd S_n$.

Theorem 10: The set A_n, of even permutations in S_n, forms a normal subgroup of S_n of order $\frac{n!}{2}$.

Proof: You have already seen that the signature function, $\text{sign}: S_n \to \{1, -1\}$ is an epimorphism.

Now $\text{Ker}(\text{sign}) = \{f \in S_n | \text{sign } f = 1\}$

$= \{f \in S_n | f$ is even}

$= A_n$.

Thus, $A_n \lhd S_n$.

Further, by the Fundamental Theorem of Homomorphism, $(S_n/A_n) \simeq \{1, -1\}$.

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

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

Theorem 10 leads us to make the following important comments.

Remark 5: Note that Theorem 10 tells us that

i) **the number of even permutations in $\mathbf{S_n}$ equals the number of odd permutations in $\mathbf{S_n}$**, and

ii) A_n has only 2 cosets in S_n, A_n and σA_n, where σ is any odd permutation in S_n. Thus, $S_n = A_n \cup (1\ 2)A_n$.

Theorem 10 leads us to the following definition.

Definition: $\mathbf{A_n}$, the group of even permutations in S_n, is called the **alternating group of degree $\mathbf{n}$**.

Let us consider what A_3 looks like. Theorem 10 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, $I \in A_3$. Also $(1\ 2) \notin A_3$. Similarly, $(2\ 3)$ and $(1\ 3)$ are not in A_3.

$\therefore A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

You have already been working with this subgroup of S_3 in several examples of the earlier units.

Do the following exercises now.

E26) Prove that an r-cycle is odd if r is even, and even if r is odd.

E27) Write down all the elements of A_4. Is A_4 abelian? Why?

E28) Give the two elements of S_5/A_5.

E29) Check whether or not all the odd permutations in S_n form a subgroup of S_n, $n \geq 3$.

Now, for a moment, let us go back to Unit 5 and Lagrange's theorem. This theorem says that the order of the subgroup of a finite group divides the order of the group. However, we did not give you an example there to show you why the converse is not true. Now that you know what A_4 looks like, we are in a position to disprove the converse.

The converse of Lagrange's Theorem for finite groups is not true.

Example 7: Show that $6 \mid o(A_4)$, but A_4 has no subgroup of order 6.

Solution: Suppose, to the contrary, A_4 has a subgroup H of order 6. Then $o(H) = 6$, $o(A_4) = 12$. $\therefore |A_4 : H| = 2$. $\therefore H \lhd A_4$ (see Theorem 2, Unit 6).

Thus, A_4/H is a quotient group of order 2, and hence, is cyclic. Let $A_4/H = <Hg>$.

Then $(Hg)^2 = H \ \forall \ g \in A_4$. (Remember H is the identity of A_4/H.)

$\therefore g^2 \in H \ \forall \ g \in A_4$.

As $(1\ 2\ 3) \in A_4$, $(1\ 2\ 3)^2 = (1\ 3\ 2) \in H$.

Similarly, $(1\ 3\ 2)^2 = (1\ 2\ 3) \in H$.

By the same reasoning all the 3-cycles in A_n are in H.

Thus, $(1\ 4\ 2), (1\ 2\ 4), (1\ 4\ 3), (1\ 3\ 4), (2\ 3\ 4), (2\ 4\ 3)$ are also distinct elements 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 will use A_4 to provide another counterexample too. (See how useful A_4 is!) In Unit 6 you studied that if $H \lhd N$ and $N \lhd G$, then H need not be normal in G. Well, here's an example as an exercise for you (se E30).

'$\lhd$' is not a transitive relation.

E30) Consider the subset $V_4 = \{I, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$ of A_4. Show that $V_4 \lhd A_4$. Also show that $H = \{I, (1\ 2)(3\ 4)\}$ is a normal subgroup of V_4, but $H \not\lhd A_4$. (Hence, $H \lhd V_4$, $V_4 \lhd A_4$ but $H \not\lhd A_4$.)

E31) How many elements does A_5 have of order

i) 2? ii) 3? iii) 5? iv) 15?

Give reasons for your answers.

Now, let us find a generating set for A_n. You have already seen that $S = \{(1\ i) \mid 2 \le i \le n\}$ generates S_n. Since no transposition lies in A_n, $S \cap A_n = \emptyset$. So, what could a generating set for A_n be, apart from the set A_n itself (of course!)?

Theorem 11: The set of 3-cycles in S_n generates A_n, $n \ge 3$.

Proof: Let S be the set of all 3-cycles in S_n. Since any 3-cycle is an even permutation, $< S > \subseteq A_n$.
Now, in Theorem 6, you have seen that $\{(1\ i) \mid 1 < i \le n\}$ generates S_n.
So, let $\sigma \in A_n$. Then $\sigma \in S_n$.
So $\sigma = (1\ i_1)(1\ i_2)\ldots(1\ i_r)$, where the $i_j s$ are not necessarily distinct.
However, $r = 2m$ for some $m \in \mathbb{N}$, since $\sigma \in A_n$.
Also, if $i_j = i_{j+1}$, then $(1\ i_j)(1\ i_{j+1}) = I$.
So let us assume $i_j \ne i_{j+1}\ \forall\ j = 1, \ldots, r-1$.
Now, $(1\ i_1)(1\ i_2) = (1\ i_2\ i_1)$.
Similarly, $(1\ i_3)(1\ i_4) = (1\ i_4\ i_3)$.
In this way, taking pairs of adjacent transpositions, we get σ as the product of m 3-cycles of the form $(1\ i\ j)$, $i, j = 2, \ldots, n$, $i \ne j$.
Thus, $\sigma \in < S >$.
$\therefore A_n = < S >$. ■

Let us consider an application of Theorem 11.

Example 8: Let $H \lhd A_n$, $n \ge 3$, and let $(1\ 2\ 3) \in H$. Show that $(1\ 3\ 2) \in H$. Further, show that $(1\ i\ 3)(1\ 2\ 3)(1\ 3\ i) \in H$ for $i \in \{1, 2, \ldots, n\} \setminus \{1, 3\}$.

Solution: Since $(1\ 3\ 2) = (1\ 2\ 3)^{-1}$ and $H \le A_n$, $(1\ 3\ 2) \in H$.
Next, $(1\ i\ 3) \in A_n$ and $H \lhd A_n$. Hence,
$(1\ i\ 3)(1\ 2\ 3)(1\ i\ 3)^{-1} = (1\ i\ 3)(1\ 2\ 3)(1\ 3\ i) \in H$.

***

Now try solving an exercise which we shall require for proving a very important corollary of Theorem 11.

E32) Let $H \lhd A_n$, $n \ge 3$, and let $(1\ 2\ 3) \in H$. Calculate the following:

i) $(1\ i\ 3)(1\ 2\ 3)(1\ 3\ i)$,

ii) $(j\ 1\ i)(1\ i\ 2)(j\ i\ 1)$,

iii) $(1\ 2\ k)(j\ 2\ i)(1\ k\ 2)$,

where $i, j, k \in \{1, 2, \ldots, n\}$ are distinct, and are such that all the 3-cycles in the products above are defined.
Show that all the elements you have just calculated lie in H. Hence show that $H = A_n$.

Now let us use E32 to prove a corollary of Theorem 11.

Corollary 1: Let $H \lhd A_n$, $n \geq 3.$ If H contains a 3-cycle, then $H = A_n.$

Proof: From Example 5, you know that every conjugate of a 3-cycle is a 3-cycle, and that conjugation preserves the operation in $A_n.$
Now, let $(i\ j\ k) \in H,$ and let $(r\ s\ t)$ be any 3-cycle.
As in E32, taking $\sigma_1 = (i\ r\ k),\ \sigma_2 = (s\ i\ r)$ and $\sigma_3 = (j\ t\ i),$ you should verify that $\sigma_3\sigma_2\sigma_1(i\ j\ k)(\sigma_3\sigma_2\sigma_1)^{-1} = (r\ s\ t).$
Hence, $(r\ s\ t) \in H.$
Thus, all the 3-cycles are in $H.$ Hence, by Theorem 11, $H = A_n.$ ■

Consider the impact of the result above. It says that if any normal subgroup of A_n has one 3-cycle, then it must be all of $A_n.$ You will see how this is applied as we discuss the simplicity of $A_n.$

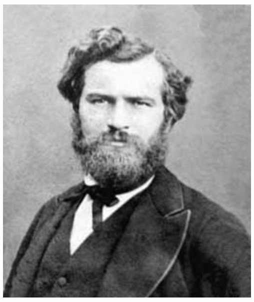

Fig.6: Camille Jordan (1838-1922)

For $i = 1, 2, 3,\ A_i$ is simple. Why? Well, $A_1 = \{I\};\ A_2 = \{I\};\ A_3 = <(1\ 2\ 3)>,$ which is of order $3,$ and hence simple (see Unit 6).
Also, in E30 you have seen that A_4 is not simple. What about A_5? The following theorem answers this. This theorem was known to the young mathematician, Galois. However, the first formal proof was given by the French analyst and algebraist, Camille Jordan, in 1870.

Theorem 12: A_n is simple for $n \geq 5.$

Proof: Let $n \geq 5.$ Suppose A_n has a non-trivial normal subgroup $H.$
Since $H \neq \{I\},\ \exists\ \sigma' \in H,\ \sigma' \neq I.$ Out of all such $\sigma',$ pick $\sigma \in H$ such that σ moves the least number of integers from 1 to $n,$ say σ moves k integers.
Firstly, $k \neq 1,$ since if σ moves one element, it must move at least $2,$ being a non-identity bijection.
However, $k \neq 2,$ since $\sigma \in A_n,$ and hence, σ cannot be a transposition.
If $k = 3,$ then σ must be a 3-cycle. Then, by Corollary 1, $H = A_n.$

Next, let $k \geq 4,$ and suppose $\sigma = (x_1\ x_2 \ldots x_r)\rho$ is a disjoint product, where $3 \leq r < k.$
Now, let $\alpha = (x_1\ x_2\ x_3),$ and $\beta = \sigma^{-1}\alpha\sigma\alpha^{-1}.$
Since $H \lhd A_n,\ \alpha\sigma\alpha^{-1} \in H.$ Hence, $\beta \in H.$
Now, if ρ moves an element, then it must move more than one element at least.
Assume $\rho(x_{r+1}) = y_1 \neq x_{r+1}$ and $\rho(x_{r+2}) = y_2 \neq x_{r+2},$ where $x_{r+1}, x_{r+2}, y_1, y_2$ are not any of the x_is, $i = 1, \ldots, r.$
Then $\sigma(x_{r+1}) = y_1,$ and $\sigma(x_{r+2}) = y_2.$
Now $\beta(x_{r+1}) = \sigma^{-1}\alpha\sigma\alpha^{-1}(x_{r+1}) = \sigma^{-1}\alpha\sigma(x_{r+1}),$ since α fixes $x_{r+1}.$

$= \sigma^{-1}\alpha(y_1) = \sigma^{-1}(y_1),$ since α fixes $y_1.$

$= x_{r+1}.$

Also $\beta(x_1) = \sigma^{-1}\alpha\sigma(x_3) = \sigma^{-1}\alpha(x_4) = \sigma^{-1}(x_4) = x_3 \neq x_1.$
So $\beta \neq I.$

Further, for any t fixed by σ, $t \notin \{x_1, x_2, \ldots, x_r\}$. So t is also fixed by β. So $\beta \in H$, with β moving one less element than σ (since $\beta(x_{r+1}) = x_{r+1}$). This is a contradiction to the way we chose σ. Hence, our assumption that σ can be written as a disjoint product with one factor being a cycle of length ≥ 3 is not possible.

So, now we are left with the possibility of $k \geq 4$ and σ is a disjoint product of transpositions, say,

$\sigma = (x_1\ x_2)(x_3\ x_4)\rho$,

where ρ is a product of an even number of disjoint transpositions.

Take $\gamma = (x_1\ x_2\ x_3)$ and $\delta = \sigma^{-1}\gamma\sigma\,\gamma^{-1}$. Then, you should show why $\delta \in H$.

Further, you should check that

$\delta = (\sigma^{-1}(x_1)\ \sigma^{-1}(x_2)\ \sigma^{-1}(x_3))(x_3\ x_2\ x_1) = (x_2\ x_1\ x_4)(x_3\ x_2\ x_1) = (x_3\ x_1)(x_2\ x_4)$.

So $(x_3\ x_1)(x_2\ x_4) \in H$.

Now, **since $\mathbf{n \geq 5}$,** $\exists\ i \neq x_1, x_2, x_3, x_4$ in $\{1, 2, \ldots, n\}$.

Let $\mu = (x_1\ x_3\ i)$. Then $\mu^{-1} = (i\ x_3\ x_1)$.

Again, you should check that $\mu^{-1}\delta\mu\delta \in H$.

Now $\mu^{-1}\delta\mu\delta = (\mu^{-1}(x_3)\ \mu^{-1}(x_1))(\mu^{-1}(x_2)\ \mu^{-1}(x_4))(x_3\,x_1)(x_2\,x_4)$

$= (x_1\ i)(x_2\,x_4)(x_3\,x_1)(x_2\,x_4)$

$= (x_1\ i)(x_1\ x_3) = (x_1\ x_3\ i)$

$= \mu$.

Thus, $\mu \in H$.

Hence, as in the case $k = 3$, $H = A_n$.

Hence, in all the cases if $H \lhd A_n$, $H = \{I\}$ or $H = A_n$.

Thus, A_n is simple for $n \geq 5$. ■

Though the proof above may seem a bit involved, please study it carefully, doing each step yourself.

Using Theorem 12, we can now show what the non-trivial normal subgroups of S_n look like. You have already seen that $S_1 = \{I\}$, and that $S_2 = \{I, (1\ 2)\}$ is simple. You also know that the only non-trivial normal subgroup of S_3 is A_3. You have seen that S_4 has at least two normal subgroups, V_4 and A_4. What about S_n for $n \geq 5$? You know that $A_n \lhd S_n\ \forall\ n \in \mathbb{N}$. Are there any other normal subgroups, as in S_4? Consider the following result.

Theorem 13: A_n is the only non-trivial proper normal subgroup of $S_n\ \forall\ n \geq 5$.

Proof: Let H be a non-trivial normal subgroup of S_n, $n \geq 5$.

Then $H \cap A_n \lhd A_n$.

Hence, by Theorem 12, $H \cap A_n = \{I\}$ or $H \cap A_n = A_n$.

If $H \cap A_n = A_n$, $A_n \subseteq H \subseteq S_n$.

So $(H/A_n) \lhd (S_n/A_n)$, and $o(S_n/A_n) = 2$.

Hence, $(H/A_n) = \{I\}$ or $(H/A_n) = (S_n/A_n)$.

Thus, $H = A_n$ or $H = S_n$.

If $H \cap A_n = \{I\}$, then H has no even permutation, apart from I.

Hence, if $\sigma \in H, \sigma \neq I, \sigma$ is an odd permutation.

Now, suppose H has two distinct non-trivial elements σ_1, σ_2. Then both are odd. So $\sigma_1\sigma_2$ is even. Also $\sigma_1\sigma_2 \in H$, since $H \leq S_n$.

Hence, $\sigma_1\sigma_2 \in H \cap A_n = \{I\}$.

Thus, $\sigma_2 = \sigma_1^{-1}$. Hence, $H = <\sigma_1>$, where $o(\sigma_1) = 2$. Say, $\sigma_1 = (i\ j)$.

Since $n \geq 5, \exists\ k \in \{1, \ldots, n\} \setminus \{i, j\}$.

Then, since $H \triangleleft S_n$, $(i\ k)(i\ j)(i\ k)^{-1} \in H$, i.e., $(j\ k) \in H$, a contradiction, since $H = \{I, \sigma_1\}$. Hence $H \cap A_n \neq \{I\}$, i.e., $H \cap A_n = A_n$.

Thus, the only proper normal subgroups of S_n are $\{I\}$ and A_n. ■

In the proofs of both Theorems 12 and 13, we have left several steps for you to check. So please do every step yourself.

Let us consider an example of how Theorems 12 and 13 are of help.

Example 9: Find all possible group homomorphisms from S_6 to $\mathbb{Z}_7$.

Solution: Let $f : S_6 \to \mathbb{Z}_7$ be a homomorphism.

Then $\text{Ker } f \triangleleft S_6$. Hence, $\text{Ker } f = \{I\}$, or $\text{Ker } f = A_6$, or $\text{Ker } f = S_6$.

If $\text{Ker } f = \{I\}$, then $S_6 \simeq \text{Im } f \leq \mathbb{Z}_7$. But $o(S_6) > 7 = o(\mathbb{Z}_7)$.

Hence, we reach a contradiction. $\therefore \text{Ker } f \neq \{I\}$.

If $\text{Ker } f = A_6$, then $S_6/A_6 \simeq \text{Im } f \leq \mathbb{Z}_7$. Here $o(\text{Im } f) = o(S_6/A_6) = 2$. But $2 \nmid o(\mathbb{Z}_7)$. Hence, we reach a contradiction. $\therefore \text{Ker } f \neq A_6$.

Thus, the only possibility is $\text{Ker } f = S_6$, i.e., $f(\sigma) = \overline{0}\ \forall\ \sigma \in S_6$, i.e., f is the zero map.

***

Try solving the following exercises now.

E33) Let $f : A_7 \to G$ be a group homomorphism. Show that $o(G) \geq 2520$ or $f(x) = e\ \forall\ x \in A_7$.

E34) What are the possible group homomorphisms from S_5 to U_5, and why? (**Hint:** Analyse the possibilities of $\text{Ker } f$, for each such f.)

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

9.5 CAYLEY'S THEOREM

In this course you have studied all kinds of groups – finite, infinite, abelian, non-abelian, cyclic, non-cyclic. You have studied subgroups of $\mathbb{C}$ and $\mathbb{C}^*$, subgroups of $\mathbb{M}_{m\times n}(\mathbb{C})$, those of D_{2n}, S_n, U_n, and of so many other groups. You have also seen that there are infinitely many isomorphism classes of groups. Yet, it turns out, amazingly, that each of these isomorphism classes has a permutation group in it. This was noticed, and proved, by Arthur Cayley, the English mathematician by whose name we also call the group operation tables that you have used again and again. Let us see what Cayley's theorem precisely says.

Recall that $S(G)$ is the group of all bijections from G to G.

Theorem 14 (Cayley): Any group G is isomorphic to a subgroup of the permutation group $S(G)$. Thus, G can be viewed as a permutation group.

Proof: For $a \in G$, we define the left regular representation

$f_a : G \to G : f_a(x) = ax.$

In E3, you have shown that $f_a \in S(G) \ \forall \ a \in G.$

Now let us define a function $f : G \to S(G) : f(a) = f_a.$

f is well-defined: If $a = b$ in G, then $ax = bx \ \forall \ x \in G$. So $f_a = f_b$ in $S(G)$.

f is a homomorphism: To prove this, we note that

$(f_a \circ f_b)\ (x) = f_a(bx) = abx = f_{ab}(x) \ \forall \ a, b \in G.$

$\therefore f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b) \ \forall \ a, b \in G.$

f is 1-1: To prove this, consider

$$
\begin{aligned}
\text{Ker } f &= \{a \in G \mid f_a = I_G\} \\
&= \{a \in G \mid f_a(x) = x \ \forall \ x \in G\} \\
&= \{a \in G \mid ax = x \ \forall \ x \in G\} \\
&= \{e\}, \text{ by left cancellation.}
\end{aligned}
$$

Thus, by the Fundamental Theorem of Homomorphism,

$G/\text{Ker } f \simeq \text{Im } f \le S(G),$

i.e., $G \simeq \text{Im } f \le S(G)$, since $G \simeq (G/\{e\})$.

i.e., G is isomorphic to a subgroup of $S(G)$. ■

The importance of Theorem 14 needs to be stressed. Consider the following comment in this regard.

Remark 6: If we put Theorem 14 above, together with Theorem 9, Unit 8, what do you see? We find that there are as many non-isomorphic groups as the number of non-isomorphic permutation groups, i.e., infinite. Each isomorphism class is $[H]$, where $H \le S(X)$ for some X.

Let us consider an example of representing a group using Cayley's theorem.

Example 10: Find a subgroup of S_4 to which the Klein 4-group K_4 is isomorphic.

Solution: Consider the multiplication table for K_4 :

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Now using the left representation function, let us see what $\text{Im } f$ (in Theorem 14) gives us. Using this table, you can see that $f_e = I$, since

$f_e(x) = x \ \forall \ x \in G.$

Next, looking at the second row of the table, we see that

$f_a(e) = a, f_a(a) = e, f_a(b) = c, f_a(c) = b.$

So $f_a = (e \ a)(b \ c).$

Similarly, you should show that $f_b = (e \ b)(a \ c)$ and $f_c = (e \ c)(a \ b).$

Hence, $K_4 \simeq \{I, (e \ a)(b \ c), (e \ b)(a \ c), (e \ c)(a \ b)\}.$

Now, just replace the symbols e, a, b, c by $1, 2, 3, 4,$ and you'll get $\text{Im } f = V_4$ (in E30), sitting in S_4.

$\therefore K_4 \simeq V_4.$

***

The example above leads us to make the following observation.

Remark 7: Note that a subgroup of $S(G)$ need not have all the algebraic properties of $S(G)$. So, for example, if G is abelian of order 6, $S(G)$ would be non-abelian, but the subgroup of $S(G)(= S_6$ here) to which G is isomorphic must be abelian. Thus, in Example 10, S_4 is non-abelian, but $K_4 \simeq V_4$, which is abelian.

Try solving the following exercises now.

E35) Obtain the subgroup of S_4 to which $\mathbb{Z}_4$ is isomorphic. Is $\mathbb{Z}_4 \simeq A_4$? Why, or why not?

E36) If G is a finite group of order n, then show that G is isomorphic to a subgroup of S_n.

E37) For each of the following groups, find a subgroup of S_8 to which it is isomorphic:

i) D_8, ii) $\mathbb{Z}_8$, iii) U_8, iv) Q_8.

With this we wind up our discussion on permutation groups. We also close our discussion on group theory. In the next block you will start studying ring theory. Of course, you will keep using what you have learnt in the first two blocks, because every ring is a group also, as you will see.

So, let us see what you have studied in this unit.

9.6 SUMMARY

In this unit, we have discussed the following points.

1. A brief recap about permutations, in general, with the focus on the group $(S_n, \circ)$, in particular. S_n is a finite non-abelian group of order $n!$, for $n \geq 3$.

2. The definition, 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. The set of all transpositions generates S_n, $n \geq 2$. Also, $\{(1\ 2), (1\ 3), \ldots, (1, n)\}$ generates S_n, $n \geq 2$.

5. For $n \geq 2$, the function $\text{sign} : S_n \to \{1, -1\} : \text{sign}(\sigma) = \prod_{\substack{i, j=1 \\ i<j}}^{n} \frac{\sigma(j) - \sigma(i)}{(j-i)}$ is an epimorphism.

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. A_n is generated by the set of 3-cycles in S_n, for $n \geq 3$.

9. A_n is simple for $n \geq 5$.

10. The only non-trivial proper normal subgroup of $S_n (n \geq 5)$ is A_n.

11. **Cayley's Theorem:** Each group is isomorphic to some permutation group.

9.7 SOLUTIONS / ANSWERS

E1) In Unit 2, you have seen that $(S_n, \circ)$ is a group $\forall\ n \in \mathbb{N}$.
Since $S_1 = \{I\}$, and $o(S_2) = 2$, these groups are abelian. Now let us look at S_3.
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
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, these two permutations don't commute.

$\therefore S_3$ is non-abelian.

Now, consider any S_n, $n \geq 3$. Since $(1\ 2\ 3)$ and $(1\ 3)$ are in S_n, the same argument above shows that S_n is non-abelian $\forall\ n \geq 3$.

E2) See Example 17, Unit 8.

E3) If $x = y$ in G, then $gx = gy$, i.e., $f(x) = f(y)$. So f is well-defined.
Next, f is 1-1 because $f(x) = f(y) \Rightarrow gx = gy \Rightarrow x = y$, by the left cancellation law.
Also, for any $x \in G$, $f(g^{-1}x) = x$. So f is surjective.
Hence, $f \in S(G)$.

E4) There can be several answers.
Our answer is $(1\ 2)$ and $(2\ 4)$, $(1\ 3\ 5)$ and $(1\ 2\ 3)$, $(1\ 2\ 3\ 4\ 5\ 6\ 7)$ and $(2\ 1\ 3\ 4\ 5\ 6\ 7)$.

Note that $(1\ 2) \neq (2\ 4)$, since $(1\ 2)$ takes 2 to 1 and $(2\ 4)$ takes 2 to 4.
Similarly, explain why the permutations in your answer are distinct.

E5) Here $1 \to 5,\ 5 \to 4,\ 4 \to 1,\ 2 \to 2,\ 3 \to 3.$ Thus, this is the cycle $(1\ 5\ 4)$.

E6) i) $(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 8 \\ 2 & 1 & 3 & 4 & \dots & 8 \end{pmatrix},\ (1\ 2)^{-1} = \begin{pmatrix} 2 & 1 & 3 & 4 & \dots & 8 \\ 1 & 2 & 3 & 4 & \dots & 8 \end{pmatrix},$

i.e., $(1\ 2)^{-1} = (2\ 1) = (1\ 2)$.

$$(1\ 2\ 3) \circ (3\ 2\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & 8 \\ 2 & 3 & 1 & 4 & 5 & \dots & 8 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & 8 \\ 3 & 1 & 2 & 4 & 5 & \dots & 8 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & \dots & 8 \\ 1 & 2 & 3 & \dots & 8 \end{pmatrix} = \mathrm{I}.$$

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

ii) $f(i_k) = i_{k+1}$ and $f(x) = x\ \forall\ x \neq i_k$, where $k = 1, \dots, r$, putting $i_{r+1} = i_1$.
So $f^{-1}(i_{k+1}) = i_k$ and $f^{-1}(x) = x\ \forall\ x \neq i_k$, where $k = 1, \dots, r$.
Thus, $f^{-1} = (i_r\ i_{r-1} \dots i_2\ i_1)$.

E7) Consider $g^{-1}h^{-1}gh$, where $g = (1\ 2),\ h = (1\ 3)$ and $g = (2\ 3),\ h = (2\ 4)$.
Then you should verify that $(1\ 2)(1\ 3)(1\ 2)(1\ 3) = (3\ 1\ 2)$, and
$(2\ 3)(2\ 4)(2\ 3)(2\ 4) = (4\ 2\ 3)$.
Note that $(3\ 1\ 2) \neq (4\ 2\ 3)$, since, for example, $(3\ 1\ 2)$ takes 4 to 4, and $(4\ 2\ 3)$ takes 4 to 2.

E8) i) $(1\ 5\ 3\ 2\ 4)$.

ii) Here $1 \to 8 \to 5 \to 1.$ All the symbols haven't been covered as yet, for instance, 2 is left. So we look at $2.$ We get $2 \to 4 \to 2.$
Still all the symbols haven't been covered, one of them being $3.$
So we look at $3.$ We get $3 \to 7 \to 6 \to 3.$
Now all the symbols are covered. Hence, the permutation is the product $(1\ 8\ 5)(2\ 4)(3\ 7\ 6)$.

iii) $(1\ 4)(2\ 5)$.

E9) $(1\ 4)(2\ 3) = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \end{pmatrix},\ (6\ 5\ 2\ 4)(3\ 1) = \begin{pmatrix} 6 & 5 & 2 & 4 & 3 & 1 & 7 & 8 \\ 5 & 2 & 4 & 6 & 1 & 3 & 7 & 8 \end{pmatrix},$

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

E10) No, because $(1\ 3)(1\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 3 & 4 & 6 \end{pmatrix}$ and

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

Since, for example, $(1\ 3)(1\ 5\ 4)$ takes 3 to 1 and $(1\ 5\ 4)(1\ 3)$ takes 3 to $5,$ the two are different.

E11) Let $f = (i_1\ i_2 \ldots i_r).$ Then, as you have seen in the proof of Theorem 3, $f(i_1) = i_2,\ f(i_2) = f^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_r,\ f^r(i_1) = f(i_r) = i_1.$

Similarly, $f^r(i_k) = i_k\ \forall\ k = 2, \ldots, r.$

$\therefore f^r = I.$

Also, for $s < r,\ f^s(i_1) = i_{s+1} \neq i_1.\ \therefore f^s \neq I.$

$\therefore o(f) = r.$

E12) $\sigma = (1\ 3\ 6\ 9)(2\ 5\ 7)(8\ 10).$

$\therefore o(\sigma) = \text{l.c.m}(4,\ 3,\ 2)$

$= 12.$

E13) Consider $\sigma_1 = (1\ 2) = \sigma_2,$ in $S_3.$ Then $\sigma_1\sigma_2 = I.$

So $o(\sigma_1\sigma_2) = 1.$

But $\text{l.c.m}(2,\ 2) = 2.$

Theorem 4 doesn't fail here because it doesn't apply here. It only applies to a product of **disjoint** cycles. Here σ_1 and σ_2 are not disjoint.

E14) No, e.g., see E12 for both questions.

E15) i) $(1\ 4)(1\ 3).$

ii) $(4\ 1)(4\ 3)(= (1\ 4)(3\ 4)).$

iii) $(2\ 3)(2\ 5)(2\ 4).$

E16) $(i\ \ j)(j\ k) = (i\ \ j\ \ k)$ and $(j\ k)(i\ \ j) = (i\ \ k\ \ j) \neq (i\ \ j\ \ k).$

E17) $(1\ 5)(1\ 8)(2\ 4)(3\ 6)(3\ 7).$

E18) $(1\ 3\ 4) = (1\ 4)(1\ 3),\ (5\ 7) = (1\ 5)(1\ 7)(1\ 5),$

$(2\ 6\ 8) = (2\ 8)(2\ 6) = (1\ 2)(1\ 8)(1\ 2)(1\ 2)(1\ 6)(1\ 2) = (1\ 2)(1\ 8)(1\ 6)(1\ 2),$

since $(12)(12) = I.$

$\therefore (1\ 3\ 4)(5\ 7)(2\ 6\ 8) = (1\ 4)(1\ 3)(1\ 5)(1\ 7)(1\ 5)(1\ 2)(1\ 8)(1\ 6)(1\ 2).$

E19) 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.

$\therefore (1\ 2)(2\ 3) \ldots (9\ 10)$

$= (1\ 2\ 3)(3\ 4) \ldots (9\ 10)$

$= (1\ 2\ 3\ 4) \ldots (9\ 10)$

$= (1\ 2\ 3 \ldots 10)$

$= (1\ \ 10)(1\ 9) \ldots (1\ 2).$

E20) No. Since I is not a transposition, it doesn't lie in this set.

E21) $\text{sign } I = \prod_{\substack{i,\,j=1\\ i<j}}^{n} \dfrac{I(j)-I(i)}{j-1} = \prod_{\substack{i,\,j=1\\ i<j}}^{n} \dfrac{j-i}{j-i} = 1.$

E22) $$\text{sign } \sigma = \frac{\sigma(2)-\sigma(1)}{2-1}\cdot\frac{\sigma(3)-\sigma(1)}{3-1}\cdot\frac{\sigma(3)-\sigma(2)}{3-2}\cdot\frac{\sigma(4)-\sigma(3)}{4-3}\cdot\frac{\sigma(4)-\sigma(2)}{4-2}$$
$$\cdot\frac{\sigma(4)-\sigma(1)}{4-1}\cdot\frac{\sigma(5)-\sigma(4)}{5-4}\cdot\frac{\sigma(5)-\sigma(3)}{5-3}\cdot\frac{\sigma(5)-\sigma(2)}{5-2}\cdot\frac{\sigma(5)-\sigma(1)}{5-1}$$
$$=\frac{3-4}{1}\cdot\frac{2-4}{2}\cdot\frac{2-3}{1}\cdot\frac{1-2}{1}\cdot\frac{1-3}{2}\cdot\frac{1-4}{3}\cdot\frac{5-1}{1}\cdot\frac{5-2}{2}\cdot\frac{5-3}{3}\cdot\frac{5-4}{4}=1.$$

E23) The permutation in E15(iii) is odd, because it is a product of 3 transpositions.
Similarly, explain why the others are odd or not odd.

E24) $\text{sign}(f) = \text{sign}(g) = -1.$

$\therefore \text{sign}(f \circ g) = (-1)(-1) = 1.$

$\therefore f \circ g$ is even.

E25) $\text{sign } I = 1.$ $\therefore I$ is even.
You could also have argued that $I = (1\ 2)(1\ 2),$ and hence I is even.

E26) You have seen that $\sigma = (i_1\ i_2 \ldots i_r) = (i_1\, i_2)(i_2\ i_3)\ldots(i_{r-1}\ i_r),$ a product of $(r-1)$ transpositions.
Thus, σ is odd if r is even, and σ is even if r is odd.

E27) You know that $o(A_4) = \dfrac{4!}{2} = 12.$
Now $I \in A_4$. Then all the 3-cycles are in A_4.
So $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$ are in A_4.
Then all the possible disjoint products of two transpositions lie in A_4.
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.

Regarding commutativity, note that
$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$ and $(1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3).$
Thus, $(1\ 2\ 3)$ and $(1\ 2\ 4)$ don't commute. Hence, A_4 is not abelian.

E28) $o(S_5/A_5) = 2.$ One element is the coset $A_5,$ another is $(1\ 2)A_5,$ since $(1\ 2) \notin A_5.$
Note that $(1\ 2)A_5 = \sigma A_5$ for any odd σ in $S_n,$ since $\sigma^{-1}(1\ 2) \in A_5.$

E29) $(1\ 2)$ and $(1\ 3)$ are odd permutations in $S_n,$ but $(1\ 2)(1\ 3)$ is an even permutation.
Hence, this set is not a subgroup of S_n.

You could also have argued this by noting that I is even, and hence doesn't lie in this set. Hence, this set is not a subgroup of S_n.

E30) From Example 5, you know that $\sigma\nu\sigma^{-1}$ has the same disjoint cycle decomposition structure as that of $\nu \ \forall \ \nu \in V_4$ and $\sigma \in A_4$.

Also V_4 contains all elements that are products of two disjoint transpositions in S_4.

Hence, $\sigma\nu\sigma^{-1} \in V_4 \ \forall \ \sigma \in A_4, \ \nu \in V_4$.

Thus, $V_4 \triangleleft A_4$.

Since $|V_4 : H| = 2, \ H \triangleleft V_4$.

Now $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin H$. Hence, $H \ntriangleleft A_4$.

E31) We will use a counting argument to find this. The elements in A_5 are 3-cycles, 5-cycles and products of 2 disjoint transpositions.

i) The only even permutations of order 2 in S_5 are those of the form $(1\ 2)(3\ 4)$, using 4 distinct symbols.
Also $(1\ 2) = (2\ 1)$ and $(1\ 2)(3\ 4) = (3\ 4)(2\ 1)$.
Hence, the total number of such elements in A_5 is
$$\frac{1}{2}\left[\frac{5\times 4}{2}\ \frac{3\times 2}{2}\right] = 15.$$

ii) The only even permutations of order 3 are 3-cycles.
Also $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.
Hence, the number of distinct 3-cycles in S_5 is $\frac{1}{3}(5\times 4\times 3) = 20$.

iii) This is the number of distinct 5-cycles in S_5, i.e.,
$\frac{1}{5}(5\times 4\times 3\times 2\times 1) = 24$.

iv) Since we have already found 59 elements of A_5, and $o(A_5) = 60$, these are all the non-trivial elements of A_5. Hence, A_5 has no element of order 15.

E32) We will use Example 5 to calculate the elements.

i) Let $i \neq 2$. If $\sigma_1 = (1\ i\ 3)$, then the given element is
$\sigma_1(1\ 2\ 3)\sigma_1^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))$, from Example 5.
$= (i\ 2\ 1) \in H$, since $H \triangleleft A_n$, and $\sigma_1 \in A_n$.
If $i = 2$, then $\sigma_1 = (1\ 2\ 3)$. Hence, $\sigma_1(1\ 2\ 3)\sigma_1^{-1} = (1\ 2\ 3) \in H$.

ii) Here $\sigma_2 = (j\ 1\ i)$, and the given element is
$\sigma_2(1\ i\ 2)\sigma_2^{-1} = (i\ \ j\ 2) \in H$, using (i) above, and since $\sigma_2 \in A_n$.
Here we have assumed $j \neq 1, 2$.
As in (i), if $j = 2$, then $\sigma_2 = (1\ i\ 2)$, so that
$\sigma_2(1\ i\ 2)\sigma_2^{-1} = (1\ i\ 2) \in H$.

iii) Here $\sigma_3 = (1\ 2\ k)$, and the given element is
$\sigma_3(i\ \ j\ 2)\sigma_3^{-1} = (i\ \ j\ k) \in H$, using (ii), and since $\sigma_3 \in A_n$.

Here too $i, j, k \neq 1, 2.$

Hence, for any $(i\ j\ k) \in A_n,$ (i), (ii), (iii) tell us
$(i\ j\ k) = (\sigma_3\sigma_2\sigma_1)(1\ 2\ 3)(\sigma_3\sigma_2\sigma_1)^{-1} \in H.$
Thus, every 3-cycle is in $H.$ Hence, by Theorem 11, $H = A_n.$

E33) $\text{Ker } f \lhd A_7.$ Hence, $\text{Ker } f = \{I\}$ or $\text{Ker } f = A_7.$
If $\text{Ker } f = \{I\},$ then f is 1-1, and $f(A_7) \leq G,$ where
$o(f(A_7)) = o(A_7) = 2520.$
$\therefore o(G) \geq 2520.$
If $\text{Ker } f = A_7,$ then $f(x) = I\ \forall\ x \in A_7.$

E34) Let $f: S_5 \to U_5$ be a group homomorphism.
Then $\text{Ker } f \lhd S_5.$ So $\text{Ker } f = \{I\},$ or $\text{Ker } f = A_5,$ or $\text{Ker } f = S_5.$
If $\text{Ker } f = \{I\},$ then $S_5 \simeq \text{Im } f \leq U_5.$
But then $o(\text{Im } f) = 5!$ and $o(U_5) = 5.$
So we reach a contradiction.
Hence, $\text{Ker } f \neq \{I\}.$

If $\text{Ker } f = A_5,$ then $\text{Im } f \simeq (S_5/A_5).$ Hence, $\text{Im } f \leq U_5$ of order $2.$ But $2 \nmid o(U_5).$ So, by Lagrange's theorem, this case is not possible.

Hence, the only possibility is $\text{Ker } f = S_5,$ i.e., $f: S_5 \to U_5 : f(\sigma) = 1.$

E35) You know that $\mathbb{Z}_4 = <\overline{1}>$ and $o(\overline{1}) = 4.$ Therefore, the subgroup of S_4 isomorphic to $\mathbb{Z}_4$ must be cyclic of order $4.$
Further, it is generated by the permutation $f_{\overline{1}}.$
Now $f_{\overline{1}}(x) = \overline{1} + x\ \forall\ x \in \mathbb{Z}_4.$
$\therefore f_{\overline{1}} = (\overline{1}\ \ \overline{2}\ \ \overline{3}\ \ \overline{0}),$ which is the same as the cycle $(1\ 2\ 3\ 4).$
$\therefore \mathbb{Z}_4 \simeq <(1\ 2\ 3\ 4)>,$ which is certainly not isomorphic to $A_4,$ as $(1\ 2\ 3\ 4) \notin A_4.$ Also note that A_4 is not cyclic. (Why?)

E36) Let $G = \{g_1, g_2, \ldots, g_n\}.$ Then $S(G)$ is the set of permutations on n symbols. Hence, $S(G) = S_n.$
Thus, $G \simeq \text{Im } f \leq S_n,$ where f is as in the proof of Cayley's theorem.

E37) i) $D_8 = <\{r, R \mid r^2 = I, R^4 = I, rR = R^{-1}r\}>.$
Hence, D_8 must be isomorphic to a subgroup generated by
$\{\sigma_1, \sigma_2 \mid \sigma_1^2 = I, \sigma_2^4 = I, \sigma_1\sigma_2 = \sigma_2^{-1}\sigma_1\}.$
Recall also, from Unit 2, that if we take r and R to be the reflection and rotation shown in Fig.3 there, then $\sigma_1 = (2\ 4)$ and $\sigma_2 = (1\ 2\ 3\ 4).$
You should also check that all the required conditions are satisfied.
So $D_8 \simeq <(2\ 4), (1\ 2\ 3\ 4)> \leq S_8.$

ii) As in E35, $\mathbb{Z}_8 \simeq <(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)> \leq S_8.$

iii) Since $U_8 \simeq \mathbb{Z}_8, U_8 \simeq <(1\,2\ldots 8)> \le S_8.$

iv) Verify that the Cayley table of Q_8 is as below.

$\bullet$	I	$-I$	A	$-A$	B	$-B$	C	$-C$
I	I	$-I$	A	$-A$	B	$-B$	C	$-C$
$-I$	$-I$	I	$-A$	A	$-B$	B	$-C$	C
A	A	$-A$	$-I$	I	C	$-C$	$-B$	B
$-A$	$-A$	A	I	$-I$	$-C$	C	B	$-B$
B	B	$-B$	$-C$	C	$-I$	I	A	$-A$
$-B$	$-B$	B	C	$-C$	I	$-I$	$-A$	A
C	C	$-C$	B	$-B$	$-A$	A	$-I$	I
$-C$	$-C$	C	$-B$	B	A	$-A$	I	$-I$

So, by looking at each row of the table, you can see that $f_I = I_G$; $f_{-I}(x) = -x \;\forall\; x \in Q_8$. So, $f_{-I} = (I\;\; -I)(A\;\; -A)(B\;\; -B)(C\;\; -C)$.
If we replace $I, -I, A, -A, B, -B, C, -C$ by $1, \ldots, 8,$ respectively, in f_{-I}, we get $f_{-I} = (1\,2)(3\,4)(5\,6)(7\,8)$.
Similarly, you should check that

$$f_A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix} = (1\,3\,2\,4)(5\,7\,6\,8),$$

$f_{-A} = (1\,4\,2\,3)(5\,8\,6\,7),$

$f_B = (1\,5\,2\,6)(3\,8\,4\,7),$

$f_{-B} = (1\,6\,2\,5)(3\,7\,4\,8),$

$f_C = (1\,7\,2\,8)(3\,5\,4\,6),$

$f_{-C} = (1\,8\,2\,7)(3\,6\,4\,5).$

$\therefore Q_8 \simeq \{f_x | x \in Q_8\} \le S_8.$

MISCELLANEOUS EXAMPLES AND EXERCISES

As in the previous block, the few examples and exercises given below cover the concepts and processes you have studied in this block. Studying the examples, and solving the exercises, will give you a better understanding of the concepts concerned. This will also give you more practice in solving such problems.

Example 1: Find the largest possible order an element of S_7 can have.

Solution: Every non-identity element of S_7 is a product of disjoint cycles, each cycle being of length $2, 3, 4, 5, 6$ or $7.$

Also, if $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n$ are disjoint cycles of lengths $\ell_1, \ell_2, \ldots, \ell_n,$ respectively, then $o(\sigma_1\sigma_2 \ldots \sigma_n)$ is the l.c.m of $\ell_1, \ell_2, \ldots, \ell_n.$

Further, since there are only 7 symbols, the sum of the lengths of disjoint cycles is at most $7.$

You should look at all possible such products. You will find that the maximum order possible is that of $\sigma_1\sigma_2,$ where $\ell_1 = 4, \ell_2 = 3,$ i.e., $o(\sigma_1\sigma_2) = 4 \times 3 = 12.$

***

Example 2: Show that every element of $\mathbb{Q}/\mathbb{Z}$ is of finite order.

Solution: Any element of $\mathbb{Q}/\mathbb{Z}$ is of the form $\frac{p}{q} + \mathbb{Z},$ where $(p, q) = 1.$

Now, $q\left(\frac{p}{q} + \mathbb{Z}\right) = p + \mathbb{Z} = \mathbb{Z},$ since $p \in \mathbb{Z}.$

$\therefore o\left(\frac{p}{q} + \mathbb{Z}\right) \le q.$

$\therefore \frac{p}{q} + \mathbb{Z}$ is of finite order.

***

Example 3: Let $U(n)$ denote the set of elements in $\mathbb{Z}_n$ that have an inverse w.r.t. multiplication. (In Unit 10 you will study more about such sets.) Show that $(U(n), \cdot)$ is a group.

Further, show that if $(m, n) = 1,$ then $U(mn) \simeq U(m) \times U(n).$

Solution: Firstly, since $\overline{1} \in U(n), U(n) \ne \emptyset.$

Note that $\overline{x} \in U(n)$ iff $(x, n) = 1.$ (Why?)

Now, show that multiplication is a well-defined binary operation on $U(n).$

Next, since multiplication is associative in $\mathbb{Z}_n,$ it is so in $U(n).$

Fourthly, show that $\overline{1}$ is the multiplicative identity of $U(n).$

Finally, the way $U(n)$ is defined, each element has an inverse.

Hence, $(U(n), \cdot)$ is a group.

Next, define

$\phi : U(mn) \to U(m) \times U(n) : \phi(x(\text{mod}\, mn)) = (x(\text{mod}\, m),\ x(\text{mod}\, n)).$

Now, $\overline{x} \in U(mn)$

$\Rightarrow (mn, x) = 1$

$\Rightarrow (m, x) = 1$ and $(n, x) = 1,$ as $(a, b) = 1$ iff $ar + bs = 1$ for some $r, s \in \mathbb{Z}.$
$\Rightarrow x(\text{mod}\, m) \in U(m)$ and $x(\text{mod}\, n) \in U(n).$
Also, if $\overline{x} = \overline{y}$ in $U(mn)$, then $mn \mid (x-y)$. So $m \mid (x-y)$ and $n \mid (x-y)$.
$\therefore \overline{x} = \overline{y}$ in $U(m)$ and $\overline{x} = \overline{y}$ in $U(n)$.
Thus, ϕ is a well-defined function.

Next, you should show that ϕ is a group homomorphism.

Now, to see why ϕ is a monomorphism, let $x, y \in \mathbb{Z}$ s.t.
$\phi(x(\text{mod}\, mn)) = \phi(y(\text{mod}\, mn))$
$\Rightarrow x(\text{mod}\, m) = y(\text{mod}\, m)$ and $x(\text{mod}\, n) = y(\text{mod}\, n)$.
$\Rightarrow m \mid (x-y)$ and $n \mid (x-y)$.
$\Rightarrow mn \mid (x-y)$, as $(m, n) = 1$.
$\therefore x(\text{mod}\, mn) = y(\text{mod}\, mn)$.
Thus, ϕ is $1\text{-}1$.

Finally, to see why ϕ is surjective let $(x(\text{mod}\, m), y(\text{mod}\, n)) \in U(m) \times U(n)$.
Then $(m, x) = 1$ and $(n, y) = 1$.
Since $(m, n) = 1$, $\exists\, r, s \in \mathbb{Z}$ s.t. $mr + ns = 1$. …(1)
Now $\phi(\overline{nsx + mry}) = (nsx(\text{mod}\, m), mry(\text{mod}\, n))$.
Also, by (1), $x = mrx + nsx \equiv nsx(\text{mod}\, m)$, and $y = mry + nsy \equiv mry(\text{mod}\, n)$.
$\therefore (x(\text{mod}\, m), y(\text{mod}\, n)) = (nsx(\text{mod}\, m), mry(\text{mod}\, n)) = \phi(\overline{nsx + mry})$.
Thus, ϕ is onto.

Hence, $U(mn) \simeq U(m) \times U(n)$.

***

Example 4: Find the order of the quotient group $(\mathbb{Z}_{10} \times U(10) \big/ < (\overline{2}, \overline{9}) >$.

Solution: If $o(\overline{2}, \overline{9}) = m$, then
$(\overline{2m}, \overline{9}^m) = (\overline{0}, \overline{1})$ and $(\overline{2(m-1)}, \overline{9}^{m-1}) \neq (\overline{0}, \overline{1})$.
Now $\overline{2m} = \overline{0} \Rightarrow m = 5, 10, 15, \ldots$
$\overline{9}^m = \overline{1} \Rightarrow m = 2, 4, 6, 8, \ldots$
So the least m s.t. $\overline{2m} = \overline{0}$ and $\overline{9}^m = \overline{1}$ is $m = 10$.
$\therefore o(\overline{2}, \overline{9}) = 10$, and hence, $o(< (\overline{2}, \overline{9}) >) = 10$.
Also, the order of $\mathbb{Z}_{10} \times U(10) = 10 \times 4 = 40$, since $o(U(10)) = 4$.
$\therefore$ the order of the given quotient group is $\frac{40}{10} = 4$.

***

Example 5: Check whether or not there is a non-trivial group homomorphism from $\mathbb{Z}_p$ to $\mathbb{Z}_q$, where $q > p$, p, q are primes.

Solution: Suppose $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_q$ is a non-trivial homomorphism.
Let $\overline{a}$ denote $a(\text{mod}\, p)$ for $a \in \mathbb{Z}$.
Now, $f(\overline{0}) = 0(\text{mod}\, q)$, as f is a homomorphism.

Note that f is determined by $f(\bar{1})$, since $\mathbb{Z}_p = <\bar{1}>$.

Let $f(\bar{1}) = m(\mathrm{mod}\, q) \neq 0(\mathrm{mod}\, q)$, since $f \neq \mathbf{0}$.

Then $f(\bar{p}) = f(\bar{0}) = 0(\mathrm{mod}\, q)$

$\Rightarrow pf(\bar{1}) = 0(\mathrm{mod}\, q)$

$\Rightarrow pm(\mathrm{mod}\, q) = 0(\mathrm{mod}\, q)$

$\Rightarrow q \mid pm$

$\Rightarrow q \mid m$, as $(p, q) = 1$.

$\Rightarrow m(\mathrm{mod}\, q) = 0(\mathrm{mod}\, q)$

$\Rightarrow f(\bar{1}) = 0(\mathrm{mod}\, q)$, a contradiction.

$\therefore$ No such f exists.

***

Example 6: Find all the possible group homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{30}$.

Solution: Let $g: \mathbb{Z}_{20} \to \mathbb{Z}_{30}$ be a group homomorphism.

Since $\mathbb{Z}_{20} = <\bar{1}>$, g is determined by $g(\bar{1})$.

Now $o(\bar{1}) = 20$. So $o(g(\bar{1})) \mid 20$.

Also, as $g(\bar{1}) \in \mathbb{Z}_{30}$, $o(g(\bar{1})) \mid 30$.

$\therefore g(\bar{1})$ is an element of $\mathbb{Z}_{30}$ whose order is a common divisor of 20 and 30, i.e., 1, 2, 5 or 10.

Accordingly, we have the following 4 cases:

i) $o(g(\bar{1})) = 1$: Here $g(\bar{1}) = \bar{0}$, i.e., $g = \mathbf{0}$, the trivial homomorphism.

ii) $o(g(\bar{1})) = 2$: Here $g(\bar{1})$ generates a subgroup of $\mathbb{Z}_{30}$ of order 2. So $\mathrm{Im}\, g = \{\bar{0}, \overline{15}\}$ in $\mathbb{Z}_{30}$.

Now, $\overline{15}$ is the only generator of $<\overline{15}>$, and $g(\bar{1}) = \bar{x}$, where $\bar{x}$ is a generator of $<\overline{15}>$.

$\therefore g: \mathbb{Z}_{20} \to \mathbb{Z}_{30} : g(\bar{1}) = \overline{15}$ is the only homomorphism in this case.

iii) $o(g(\bar{1})) = 5$: Here $g(\bar{1})$ generates a subgroup of $\mathbb{Z}_{30}$ of order 5. So $\mathrm{Im}\, g = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}, \overline{24}\}$.

Now $g(\bar{1})$ generates $<\bar{6}>$.

So $g(\bar{1}) = \bar{x}$, where $\bar{x}$ is a generator of $<\bar{6}>$.

You also know that $o(\bar{6}) = 5$. So $<\bar{6}>$ has $\phi(5) = 4$ generators, where ϕ is the Euler phi-function (see Unit 4).

These generators are $\bar{6}, \overline{12}, \overline{18}$ and $\overline{24}$.

Thus, in this case g can be one of four homomorphisms:

$g_1: \mathbb{Z}_{20} \to \mathbb{Z}_{30} : g_1(\bar{1}) = \bar{6}$, or

$g_2: \mathbb{Z}_{20} \to \mathbb{Z}_{30} : g_2(\bar{1}) = \overline{12}$, or

$g_3: \mathbb{Z}_{20} \to \mathbb{Z}_{30} : g_3(\bar{1}) = \overline{18}$, or

$g_4: \mathbb{Z}_{20} \to \mathbb{Z}_{30} : g_4(\bar{1}) = \overline{24}$.

iv) $o(g(\overline{1}))=10:$ Here $g(\overline{1})$ generates a group of order 10.

So $\text{Im } g=\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$.

So $g(\overline{1})$ has $\phi(10)=4$ possibilities, namely, $\overline{3}, \overline{9}, \overline{21}, \overline{27}$.

Accordingly, g can be one of 4 homomorphisms, $g_1, g_2, g_3, g_4,$ given by $g_1(\overline{1})=\overline{3}, g_2(\overline{1})=\overline{9}, g_3(\overline{1})=\overline{21}, g_4(\overline{1})=\overline{27}$.

Thus, there can be a total of $1+1+4+4=10$ homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{30}$.

Example 7: Give an example, with justification, of an infinite abelian group which cannot be written as a direct product of two proper subgroups.

Solution: For example, take $\mathbb{Q}$. Suppose, if possible, $\mathbb{Q}$ can be written as $H\times K$, where H and K are proper subgroups of $\mathbb{Q}$. Then, neither H nor K can be trivial. Also, by definition, $H\cap K=\{0\}$.
Now, let $x\in H, y\in K$ s.t. $x\neq 0, y\neq 0$.

Then $x=\frac{p}{q}, y=\frac{s}{t}$ for $p, q, s, t\in\mathbb{Z}$.

Then $qsx=ps=pty$.
Also $qsx\in H$ and $qsx=pty\in K$. So $qsx\in H\cap K$.
Since $qsx\neq 0, H\cap K\neq\{0\}$.
This is a contradiction.
Hence, our assumption is wrong, and hence, $\mathbb{Q}\neq H\times K$.

***

Example 8: Show that if G is a group s.t. $Z(G)=\{e\}$, then $\text{Aut } G$ has a trivial centre.

Solution: Since $Z(G)=\{e\}, G\simeq \text{Inn } G\leq \text{Aut } G$.
Let $\phi\in Z(\text{Aut } G)$.
Now, let $a\in G$. Then the inner automorphism $f_a\in \text{Aut } G$.
So $\phi f_a=f_a\phi$.

$\Rightarrow \phi(axa^{-1})=a\phi(x)a^{-1}\ \forall\ x\in G$

$\Rightarrow \phi(a)\phi(x)[\phi(a)]^{-1}=a\phi(x)a^{-1}\ \forall\ x\in G$

$\Rightarrow a^{-1}\phi(a)\phi(x)=\phi(x)a^{-1}\phi(a)\ \forall\ x\in G$.

Since $\phi\in \text{Aut } G, \phi(G)=G$. So, we find that $a^{-1}\phi(a)$ commutes with every element of G, i.e., $a^{-1}\phi(a)\in Z(G)=\{e\}$, i.e., $\phi(a)=a$. This is true for each $a\in G$.
Hence, $\phi=I$, the identity map, i.e., $Z(\text{Aut } G)=\{I\}$, the trivial group.

***

Miscellaneous Exercises

E1) Give two distinct non-trivial elements of the group $\mathbb{C}[x]/<x(x^2+i)>$.

E2) If G is a group and $H\lhd G$, must every element of G/H have finite order? Why?

E3) Check whether or not there is a non-trivial group homomorphism from $\mathbb{Z}_p$ to S_4, where p is a prime.

E4) Give an example, with justification, of two distinct cosets of the subgroup $<(1\ 3)>$ in S_5.

E5) Show that $G = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ is a group w.r.t. multiplication modulo 12. Apply Cayley's theorem to find a permutation group isomorphic to G.

E6) Show that $\mathbb{R}^* \simeq \mathbb{R}^+ \times \{1, -1\}$, where $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$.

E7) Let G be a non-abelian group. Can $\text{Aut } G$ be cyclic? Why?

E8) Check whether or not the greatest integer function, $f : \mathbb{R} \to \mathbb{R} : f(x) = [x]$, is a homomorphism.

E9) Check whether or not $f : \mathbb{Z}_5 \to \mathbb{Z}_{10} : f(\overline{x}) = 2x(\text{mod}10)$ is a monomorphism.

E10) i) Prove that $\sum\limits_{d|m} \phi(d) = \phi(m)$, where $m \in \mathbb{N}$ and ϕ is the Euler-phi function.

ii) Using (i), prove that the number of group homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ is the g.c.d of m and n, where $m, n \in \mathbb{N}$.

[**Hint:** See Example 6.]

iii) Show that the number of group homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ is the same as the number of homomorphisms from $\mathbb{Z}_n$ into $\mathbb{Z}_m$, where $m, n \in \mathbb{Z}$.

E11) Prove that σ^2 is an even permutation for every $\sigma \in S_n$, $n \in \mathbb{N}$.

E12) Let G be a group and $H \lhd G$ s.t. $|G : H| = p$, a prime. For any subgroup K of G, show that either $K \leq H$ or $G = HK$. In the second case, also show that $|K : H \cap K| = p$.

E13) Among the following groups, find those pairs that are isomorphic. Justify your answers.

i) $(\mathbb{Z}_4, +)$, ii) $(S_2, \circ)$, iii) $(Q_8, \cdot)$, iv) $(\mathbb{Z}_5^*, \cdot)$, v) $\text{Aut } \mathbb{Z}_6$,

vi) $\text{Inn } S_3$, vii) $(\mathbb{R}^+, \cdot)$, viii) $(S_3, \circ)$, ix) $(\mathbb{R}, +)$, x) $(D_8, \circ)$.

E14) How many epimorphisms are there from $\mathbb{Z}_{11}$ to $\mathbb{Z}_8$? Why?

E15) Show that D_8 cannot be expressed as a direct product of two proper subgroups.

SOLUTIONS / ANSWERS

E1) As you know, there are infinitely many such elements. For instance, two of them are $2+<x^3+ix>$ and $x+<x^3+ix>$.
Since neither 2 nor x are in $<x^3+ix>$, both the cosets are non-trivial.
Further, since $\deg\,(x-2)=1$ and $\deg\,(x^3+ix)=3$, $x-2\notin<x^3+ix>$.
Hence, these cosets are distinct.

E2) No. For instance, from Unit 7 you know that $\mathbb{R}/\mathbb{Z}$ is a counter-example.

E3) Suppose $f:\mathbb{Z}_p\to S_4$ is a group homomorphism s.t. $f\neq\mathbf{0}$.
Then $\text{Ker } f$ is a proper normal subgroup of $\mathbb{Z}_p$.
Since $\mathbb{Z}_p$ is simple, $\text{Ker } f=\{0\}$, i.e., f is 1-1.
So $f(\mathbb{Z}_p)\leq S_4$ which satisfies all the properties that $\mathbb{Z}_p$ satisfies.
In particular, let $f(\overline{1})=\sigma\in S_4$.
Then $p\cdot f(\overline{1})=f(\overline{p})=f(\overline{0})=I$, as f is a homomorphism.
Thus, $\sigma^p=I$. So $o(\sigma)=p$, as p is a prime.
$\therefore\ \sigma$ is a p-cycle or a disjoint product of p-cycles.
If $p=2$ or 3, $f:\mathbb{Z}_2\to S_4$ and $g:\mathbb{Z}_3\to S_4$, defined by $f(\overline{1})=(1\ 2)$ and $g(\overline{1})=(1\ 2\ 3)$, are homomorphisms from $\mathbb{Z}_p$ to S_4.
However, for any prime $p>3$, there is no non-trivial homomorphism from $\mathbb{Z}_p$ to S_4, since S_4 has no p-cycles.

E4) For instance, $(1\ 2\ 3)\circ<(1\ 3)>$ and $(1\ 4)\circ<(1\ 3)>$.
Show why they are distinct.

E5) The Cayley table for $(G,\cdot)$ is

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Using the table, you should prove that G satisfies all the axioms for being a group.
Let $\phi:G\to S_G:\phi(x)=\phi_x$, where $\phi_x(y)=xy\ \forall\ y\in G$.
Then $\phi(\overline{1})=I$ (from the first row of the table above),

$\phi(\overline{5})=\begin{pmatrix}\overline{1} & \overline{5} & \overline{7} & \overline{11}\\ \overline{5} & \overline{1} & \overline{11} & \overline{7}\end{pmatrix}$ (you can see this from Row 2 of the table),

$$\phi(\overline{7})=\begin{pmatrix}\overline{1} & \overline{5} & \overline{7} & \overline{11}\\ \overline{7} & \overline{11} & \overline{1} & \overline{5}\end{pmatrix},$$

$$\phi(\overline{11})=\begin{pmatrix}\overline{1} & \overline{5} & \overline{7} & \overline{11}\\ \overline{11} & \overline{7} & \overline{5} & \overline{1}\end{pmatrix}.$$

So $\phi(\overline{1}) = I,\ \phi(\overline{5}) = (\overline{1}\ \overline{5})(\overline{7}\ \overline{11}),\ \phi(\overline{7}) = (\overline{1}\ \overline{7})(\overline{5}\ \overline{11}),\ \phi(\overline{11}) = (\overline{1}\ \overline{11})(\overline{5}\ \overline{7}).$

Thus, if we change the symbols in S_G from $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ to $1, 2, 3, 4,$ we find

$$G \simeq \{I,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$
$$= V_4.$$

E6) First, for $r \in \mathbb{R}^+$, $r^{-1} \in \mathbb{R}^+$. Also, $r, s \in \mathbb{R}^+ \Rightarrow rs^{-1} \in \mathbb{R}^+$.

So, $\mathbb{R}^+ \le \mathbb{R}^*$.

Similarly, check that $\{1, -1\} \le \mathbb{R}^*$.

Since $\mathbb{R}^*$ is abelian, both these subgroups are normal in $\mathbb{R}^*$.

Also, $\mathbb{R}^+ \cap \{1, -1\} = \{1\}$.

$\therefore\ \mathbb{R}^+ \times \{1, -1\}$ is a well-defined internal direct product of $\mathbb{R}^*$.

Next, define $\phi : \mathbb{R}^* \to \mathbb{R}^+ \times \{1, -1\} : \phi(r) = \begin{cases} (r, 1), & \text{if } r > 0, \\ (-r, -1), & \text{if } r < 0. \end{cases}$

Check that ϕ is well-defined.

Now, for $r, s \in \mathbb{R}^*$, four cases arise:

i) $r > 0, s > 0:$ $\phi(rs) = (rs, 1) = (r, 1)(s, 1) = \phi(r)\phi(s).$

ii) $r < 0, s < 0:$ $\phi(rs) = (rs, 1) = (-r, -1)(-s, -1) = \phi(r)\phi(s).$

iii) $r < 0, s > 0:$ $\phi(rs) = (-rs, -1) = (-r, -1)(s, 1) = \phi(r)\phi(s).$

iv) $r > 0, s < 0:$ Do it as in (iii) above.

Thus, ϕ is a group homomorphism.

Also, for any $(r, 1) \in \mathbb{R}^+ \times \{1, -1\}, (r, 1) = \phi(r).$

Similarly, $(r, -1) = \phi(-r).$

$\therefore\ \phi$ is surjective.

Finally, $\text{Ker}\ \phi = \{r \in \mathbb{R}^* \mid \phi(r) = (1, 1)\}$

$= \{r \in \mathbb{R}^+ \mid (r, 1) = (1, 1)\}$

$= \{1\}.$

$\therefore\ \phi$ is 1-1, and hence an isomorphism.

E7) Suppose $\text{Aut } G$ is cyclic. Then $\text{Inn } G$ will be cyclic. So $G/Z(G)$ will be cyclic. This contradicts Theorem 5 of Unit 7. $\therefore$ $\text{Aut } G$ is not cyclic.

E8) First check that f is well-defined.

Next, $f\left(\frac{1}{2}\right) = 0$ and $f(1) = 1$.

So $f\left(\frac{1}{2} + \frac{1}{2}\right) = 1 \ne f\left(\frac{1}{2}\right) + f\left(\frac{1}{2}\right).$

Hence, f is not a homomorphism.

E9) Check that f is well-defined.

Next, $f(\overline{x} + \overline{y}) = f(\overline{x + y}) = 2x(\text{mod}10) + 2y(\text{mod}10)$

$= f(\overline{x}) + f(\overline{y}).$

Thus, f is a homomorphism.

Now, $\text{Ker } f = \{\overline{x} \in \mathbb{Z}_5 \mid 10 \text{ divides } 2x \text{ in } \mathbb{Z}\}$

$= \{\bar{x} \in \mathbb{Z}_5 \mid 5 \text{ divides } x \text{ in } \mathbb{Z}\}$

$= \{\bar{0}\}.$

$\therefore$ f is 1-1.

E10) i) Let G be a cyclic group of order m. For each $d \mid m$, G has a unique subgroup of order d. Further, any such subgroup has $\phi(d)$ distinct generators. Counting all these elements covers all the elements of G, since each element of G generates some subgroup of G.

Hence, $\sum_{d \mid m} \phi(d) = m.$

ii) As in Example 6, if $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is a group homomorphism, then $o(f(\bar{1}))$ must be a common divisor of m and n, and hence, must divide (m, n).

Now, if c is a common divisor of m and n, then c divides (m, n). Also, then $\mathbb{Z}_n$ has a unique subgroup of order c, since $\mathbb{Z}_n$ is cyclic. This subgroup will have $\phi(c)$ distinct generators, where ϕ is the Euler-phi function.

So, as in Example 6, there will be $\phi(c)$ distinct homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$, for each $c \mid (m, n)$.

So, the total number of group homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$ is $\sum_{c \mid (m, n)} \phi(c) = (m, n).$

iii) This follows immediately from (ii).

E11) For any $\sigma \in S_n$, $\bar{\sigma} \in S_n / A_n$, and $o(S_n / A_n) = 2$, since $|S_n : A_n| = 2$.

$\therefore \bar{\sigma}^2 = \text{Id}$ in S_n / A_n, i.e., $\sigma^2 \in A_n$.

E12) Suppose $K \not\leq H$. Then $HK \neq H$.

Also $HK \leq G$ s.t. $H \leq HK \leq G$.

$\therefore |G : H| = |G : HK||HK : H|$.

Since $|G : H|$ is a prime, either $|G : HK| = 1$ and $|HK : H| = p$, or $|G : HK| = p$ and $|HK : H| = 1$.

Since $HK \neq H$, the second case is not possible.

Hence, $|G : HK| = 1$, i.e., $G = HK$.

Further, if $G = HK$, then $\left(HK/H\right) \simeq \left(K/H \cap K\right)$, by the 2nd isomorphism theorem.

Hence, $|K : H \cap K| = |HK : H| = p$.

E13) (i) and (iv) are isomorphic, both being cyclic of order 4.

(ii) and (v) are isomorphic, since $\text{Aut } \mathbb{Z}_6 = \{I, \phi\}$, where

$\phi : \mathbb{Z}_6 \to \mathbb{Z}_6 : \phi(\bar{1}) = \bar{5}.$

(vi) and (viii) are isomorphic, since ${S_3}\big/{Z(S_3)} \simeq \text{Inn } S_3$ and $Z(S_3)=\{I\}.$

$Q_8 \not\simeq D_8,$ as every non-trrivial element of Q_8 is of order $2,$ but D_8 has elements of order 4 also.

E14) Let ϕ be an epimorphism from $\mathbb{Z}_{11}$ to $\mathbb{Z}_8.$

Then ${\mathbb{Z}_{11}}\big/{\text{Ker } \phi} \simeq \mathbb{Z}_8.$

Since $\mathbb{Z}_{11}$ is simple, $\text{Ker } \phi = \{\bar{0}\}$ or $\text{Ker } \phi = \mathbb{Z}_{11}.$

Accordingly, $o\left({\mathbb{Z}_{11}}\big/{\text{Ker } \phi}\right)$ is 11 or $1.$

$\therefore o(\mathbb{Z}_8)$ is 11 or $1,$ which is a contradiction.

$\therefore$ There is no epimorphism from $\mathbb{Z}_{11}$ to $\mathbb{Z}_8.$

E15) Suppose $D_8 = H \times K,\ H \lhd D_8,\ K \lhd D_8,\ H \cap K = \{e\}.$

Since $o(H) \mid 8,\ o(H) = 2$ or $4.$ And then, $o(K) = 4$ or $2.$

Take the first case, viz., $o(H) = 2,\ o(K) = 4.$

If $D_8 = <\{x,\ y \mid x^4 = e,\ y^2 = e,\ yx = x^{-1}y\}>,$ then $K = <x>.$

Since $o(H) = 2,\ H$ is abelian.

Also, in a direct product of H and $K,$ elements of H and K commute.

So D_8 is abelian, a contradiction.

Similarly, if we take the case $o(H) = 4,\ o(K) = 2,$ we reach a contradiction.

$\therefore D_8 \neq H \times K.$