UNIT 2 GROUPS

Structure

2.1 INTRODUCTION

In Unit 1 we have discussed some basic properties of sets and functions. In this unit: we are going to discuss certain sets with algebraic structures. We call them groups.

The theory of groups is one of the oldest branches of abstract algebra. It has many applications in mathematics and in the other sciences. Group theory has helped in developing physics, chemistry and computer science. Its own roots go back to the work of the eighteenth century mathematicians Lagrange, Ruffini and Galois.

In this unit we start the study of this theory. We define groups and give some examples. Then we give details of some properties that the elements of a group satisfy. We finally discuss three well known and often used groups. In future units we will be developing group theory further.

Objectives

After reading this unit, you should be able to

- define and give examples of binary operations;
- define and give examples of abelian and non-abelian groups;
- use the cancellation laws and laws of indices for various groups;
- use basic properties of integers modulo n, permutations and complex numbers.

2.2 BINARY OPERATIONS

You are familiar with the usual operations of addition and multiplication in R, Q and C. These operations are examples of binary operations, a term that we will now define.

Definition : Let S be a non-empty set. Any function $* : S \times S \to S$ is called a **binary operation** on S.

So, a binary operation associates a unique element of S to every ordered pair of elements of S.

For a binary operation $*$ on S and $(a,b) \in S \times S$, we denote $*(a,b)$ by $a*b$.

We will use symbols like $+, -, \times, \oplus, \circ, *$ and $\wedge$ to denote binary operations.

Let us look at some examples.

i) + and x are binary operations on $\mathbb{Z}$. In fact. we have +(a,b)= a + b and × (a, b) = a x b $\forall$ a, b $\in \mathbb{Z}$. We will normally denote a x b by ab.

ii) Let $\mathcal{P}(S)$ be the set of all subsets of S. Then the operations $\cup$ and $\cap$ are binary operations on $\mathcal{P}(S)$, since A $\cup$ B and A $\cap$ B are in $\mathcal{P}(S)$ for all subsets A and B of S.

iii) Let X be a non-empty set and $\mathcal{F}(X)$ be the family of all functions f : X $\to$ X. Then the composition of functions is a binary operation on $\mathcal{F}(X)$, since fog $\in \mathcal{F}(X)$ $\forall$ f, g $\in \mathcal{F}(X)$.

We are now in a position to define certain properties that binary operations can have.

Definition : Let * be a binary operation on a set S. We say that

i) * is closed on a subset T of S, if a * b $\in$ T $\forall$ a, b $\in$ T

ii) * is associative if, for all a, b, c $\in$ S, (a * b) * c = a * (b * c).

iii) * is commutative if, for all a, b $\in$ S, a * b = b * a.

For example, the operations of addition and multiplication on R are commutative as well as associative. But, subtraction is neither commutative nor associative on R. Why? Is a–b = b–a or (a–b)–c = a–(b–c) 4) a, b, c $\in$ R ? No, for example, 1–2 $\neq$ 2–1 and (1–2)–3 $\neq$ 1–(2–3). Also subtraction is not closed on $\mathbb{N} \subseteq \mathbb{R}$, because 1 $\in \mathbb{N}$, 2 $\in \mathbb{N}$ but 1–2 $\notin \mathbb{N}$.

Note that a binary operation on S is always closed on S, but may not be closed on a subset of S.

Try the following exercise now.

E 1) For the following binary operations defined on R, determine whether they are commutative or associative. Are they closed on N?

a) $x \oplus y = x + y - 5$

b) $x * y = 2(x + y)$

c) $x \Delta y = \frac{x - y}{2}$

for all x, y $\in$ R.

In calculations you must have often used the fact that a(b+c) = ab + ac and (b+c) a = bc + ba $\forall$ a, b, c $\in$ R. This fact says that multiplication distributes over addition in R. In general, we have the following definition.

Definition : If o and * are two binary operations on a set S, we say that * is distributive over o if $\forall$ a, b, c $\in$ S, we have a * (b o c) = (a * b) o (a * c) and (b o c) * a = (b * a) o (c * a).

For example. let $a * b = \frac{a+b}{2}$ $\forall$ a, b $\in$ R. Then $a(b * c) = a\left(\frac{b+c}{2}\right) = \frac{ab + ac}{2}$

= ab * ac, and

$(b * c)a = \left(\frac{b + c}{2}\right)a = \frac{ba + ca}{2} = ba * ca$ $\forall$ a, b, c $\in$ R.

Hence, multiplication is distributive over *.

For another example go back to E 4 of Unit 1. What does it say ? It says that the intersection of sets distributes over the union of sets and the union of sets distributes over the intersection of sets.

Let us now look deeper at some binary operations. You know that, for any a $\in$ R, a + 0 = a, 0 + a = a and a + (–a) = (–a) + a = 0. We say that 0 is the identity element for addition and (–a) is the negative or additive inverse of a. In general, we have the following definition.

Definition : Let * be a binary operation on a set S. If there is an element e $\in$ S such that $\forall$ a $\in$ S, a * e = a and e * a = a, then e is called an identity element for *.

For $a \in S$, we say that $b \in S$ is an inverse of a, if $a * b = e$ and $b * a = e$. In this case we usually write $b = a^{-1}$.

Before discussing examples of identity elements and inverses consider the following result. In it we will prove the uniqueness of the identity element for $*$, and the uniqueness of the inverse of an element with respect to $*$, if it exists.

Theorem 1 : Let $*$ be a binary operation on a set S. Then

a) if $*$ has an identity element, it must be unique.

b) if $*$ is associative and $s \in S$ has an inverse with respect to $*$, it must be unique.

Proof : a) Suppose e and e' are both identity elements for $*$.

Then $e = e * e'$, since e' is an identity element.
$= e'$, since e is an identity element.
That is, $e = e'$. Hence, the identity element is unique.

b) Suppose there exist $a, b \in S$ such that $s * a = e = a * s$ and $s * b = e = b * s$, e being the identity element for $*$. Then

$a = a * e = a * (s * b)$
$= (a * s) * b$, since $*$ is associative.
$= e * b = b$.

That is, $a = b$.
Hence, the inverse of s is unique.

This uniqueness theorem allows us to say the identity element and the inverse, henceforth.

A binary operation may or may not have an identity element. For example, the operation of addition on N has no identity element.

Similarly, an element may not have an inverse with respect to a binary operation. For example, $2 \in Z$ has no inverse with respect to multiplication on Z, does it?

Let us consider the following examples now.

Example 1 : If the binary operation $\oplus : R \times R \to R$ is defined by $a \oplus b = a + b - 1$, prove that $\oplus$ has an identity. If $x \in R$, determine the inverse of x with respect to $\oplus$, if it exists.

Solution : We are looking for some $e \in R$ such that $a \oplus e = a = e \oplus a \; \forall \; a \in R$. So we want $e \in R$ such that $a + e - 1 = a \; \forall \; a \in R$. Obviously, $e = 1$ will satisfy this. Also, $1 \oplus a = a \; \forall \; a \in R$. Hence, 1 is the identity element of $\oplus$.
For $x \in R$, if b is the inverse of x, we should have $b \oplus x = 1$.
i.e., $b + x - 1 = 1$, i.e., $b = 2 - x$. Indeed, $(2-x) \oplus x = (2 - x) + x - 1 = 1$.
Also, $x \oplus (2 - x) = x + 2 - x - 1 = 1$. So, $x^{-1} = 2 - x$.

Example 2 : Let S be a non-empty set. Consider $\wp(S)$, the set of all subsets of S. Are $\cup$ and $\cap$ commutative or associative operations on $\wp(S)$? Do identity elements and inverses of elements of $\wp(S)$ exist with respect to these operations?

Solution : Since $A \cup B = B \cup A$ and $A \cap B = B \cap A \; \forall \; A, B \in \wp(S)$, the operations of union and intersection are commutative. E 4 of Unit 1 also says that both operations are associative. You can see that the empty set ϕ and the set S are the identities of the operations of union and intersection, respectively. Since $S \neq \phi$, there is no $B \in \wp(S)$ such that $S \cup B = \phi$. In fact, for any $A \in \wp(S)$ such that $A \neq S$, A does not have an inverse with respect to union. Similarly, any proper subset of S does not have an inverse with respect to intersection.

Try the following exercise now.

E 2) a) Obtain the identity element, if it exists, for the operations given in E 1.

b) For $x \in R$, obtain x^{-1} (if it exists) for each of the operations given in E 1.

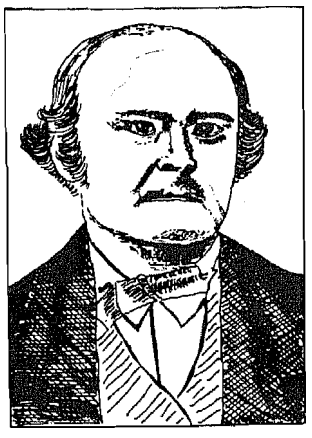

Fig. 1 : Arthur Cayley

When the set S under consideration is small, we can represent the way a binary operation on S acts by a table.

Operation. Table

Let S be a finite set and $*$ be a binary operation on S. We can represent the binary operation by a square table, called an operation table or a Cayley table. The Cayley table is named after the famous mathematician Arthur Cayley (1821-1895).

To write this table, we first list the elements of S vertically as well as horizontally, in the same order. Then we write $a * b$ in the table at the intersection of the row headed by a and the column headed by b.

For example, if $S = (-1, 0, 1)$ and the binary operation is multiplication, denoted by . , then it can be represented by the following table.

.	−1	0	1
−1	(−1).(−1) = 1	(−1) . 0 = 0	(−1) .1 = −1
0	0.(−1) = 0	0.0 = 0	0.1 = 0
1	1.(−1) = −1	1.0 = 0	1.1 = 1

Conversely, if we are given a table, we can define a binary operation on S. For example, we can define the operation $*$ on $S = \{1,2,3\}$ by the following table.

*	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

From this table we see that, for instance, $1 * 2 = 2$ and $2 * 3 = 2$.
Now $2 * 1 = 3$ and $1 * 2 = 2$. $\therefore 2 * 1 \neq 1 * 2$. That is, $*$ is not commutative.
Again, $(2 * 1) * 3 = 3 * 3 = 1$ and $2 * (1 * 3) = 2$.
$\therefore (2 * 1) * 3 \neq 2 * (1 * 3)$. $\therefore$, $*$ is not associative.
See how much information a mere table can give !
The following exercise will give you some practice in drawing Cayley tables.

E 3) Draw the operation table for the set $\mathcal{P}(S)$ (ref. Example 2), where $S = \{0,1\}$ and the operation is $\cap$.

Now consider the following definition.

Definition : Let $*$ be a binary operation on a non-empty set S and let $a_1, \ldots, a_{k+1} \in S$. We define the product $a_1 * \ldots * a_{k+1}$ as follows:

If $k = 1$, $a_1 * a_2$ is a well defined element in S.
If $a_1 * \ldots * a_k$ is defined, then
$a_1 * \ldots * a_{k+1} = (a_1 * \ldots * a_k) * a_{k+1}$

We use this definition in the following result.

Theorem 2 : Let $a_1, \ldots, a_{m+n}$ be elements in a set S with an associative binary operation *. Then

$(a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_{m+n}) = a_1 * \ldots * a_{m+n}$.

Proof : We use induction on n. That is, we will show that the statement is true for n = 1. Then, assuming that it is true for n–1, we will prove it for n.

If n = 1, our definition above gives us

$(a_1 * \ldots * a_m) * a_{m+1} = a_1 * \ldots * a_{m+1}$.

Now, assume that

$(a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_{m+n-1}) = a_1 * \ldots * a_{m+n-1}$

Then

$(a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_{m+n})$

$= (a_1 * \ldots * a_m) * ((a_{m+1} * \ldots * a_{m+n-1}) * a_{m+n})$

$= ((a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_{m+n-1})) * a_{m+n}$ since * is associative

$= (a_1 * \ldots * a_{m+n-1}) * a_{m+n}$, by induction

$= a_1 * \ldots * a_{m+n}$, by definition.

Hence, the result holds for all n.

We will use Theorem 2 quite often in this course, without explicitly referring to it.

Now that we have discussed binary operations let us talk about groups.

2.3 WHAT IS A GROUP ?

In this section we study some basic properties of an algebraic system called a **group. This** algebraic system consists of a set with a binary operation which satisfies certain properties that we have defined in Sec. 2.2. Let us see what this system is.

Definition : Let G be a non-empty set and * be a binary operation on G. We say that the pair (G, *) is a **group** if

G 1) * is associative,

G 2) G contains an identity element e for *, and

G 3) every element in G has an inverse in G with respect to *.

*(G, *) is celled a semigroup if * satisfies the properly G1. Thus, every group is a semigroup.*

We will now give some examples of groups.

Example 3 : Show that (Z, +) is a group, but (Z, .) is not.

Solution : + is an associative binary operation on Z. The identity element with respect to + is 0, and the inverse of any $n \in Z$ is $(-n)$. Thus, (Z, +) satisfies G1, G2 and G3. Therefore, it is a group.

Now, multiplication in Z is associative and $1 \in Z$ is the multiplicative identity. But does every element in Z have a multiplicative inverse? No. For instance, 0 and 2 have no inverses with respect to '.'. Therefore, (Z,.) is not a group.

Note that (Z,.) is a semigroup since it satisfies G1. So, there exist semigroups that aren't groups!

The following exercise gives you two more examples of groups.

E 4) Show that (Q, +) and (R, +) are groups.

Actually, to show that (G, *) is a group it is sufficient to show that * satisfies the following axioms.

G 1') * is associative.

G 2') $\exists\, e \in G$ such that $a * e = a\ \forall\, a \in G$.

G 3') Given $a \in G$, $\exists\, b \in G$ such that $a * b = e$.

What we are saying is that the two sets of axioms are equivalent. The difference between them is the following:

In the first set we need to prove that e is a two-sided identity and that the inverse b of any $a \in G$ satisfies $a * b = e$ and $b * a = e$. In the second set we only need to prove that e is a one-sided identity and that the inverse b of any $a \in G$ only satisfies $a * b = e$.

In fact, these axioms are also equivalent to

G 1") $*$ is associative.

G 2") $\exists\, e \in G$ such that $e * a = a\ \forall\ a \in G$.

G 3") Given $a \in G\ \exists\ b \in G$ such that $b * a = e$.

Clearly, if $*$ satisfies G1, G2 and G3, then it also satisfies G1', G2' and G3'. The following theorem tells us that if $*$ satisfies the second set of axioms, then it satisfies the first set too.

Theorem 3 : Let $(G, *)$ satisfy G1', G2' and G3'. Then $e * a = a\ \forall\ a \in G$. Also, given $a \in G$, if $\exists\ b \in G$ such that $a * b = e$, then $b * a = e$. Thus, $(G, *)$ satisfies G1, G2 and G3.

To prove this theorem, we need the following result.

Lemma 1: Let $(G, *)$ satisfy G1', G2' and G3'. If $\exists\ a \in G$ such that $a * a = a$, then $a = e$.

Proof : By G3' we know that $\exists\ b \in G$ such that $a * b = e$.

Now $(a * a) * b = a * b = e$.

Also. $a * (a * b) = a * e = a$. Therefore, by G1', $a = e$.

Now we will use this lemma to prove Theorem 3.

Proof of Theorem 3 : G1 holds since G1 and G1' are the same axiom. We will next prove that G3 is true. Let $a \in G$. By G3' $\exists\ b \in G$ such that $a * b = e$. We will show that $b * a = e$. Now,

$(b * a) * (b * a) = (b * (a * b)) * a = (b * e) * a = b * a$.

Therefore, by Lemma 1, $b * a = e$. Therefore, G3 is true.

Now we will show that G2 holds. Let $a \in G$. Then by G2', for $a \in G$, $a * e = a$. Since G3 holds, $\exists\ b \in G$ such that $a * b = b * a = e$. Then

$e * a = (a * b) * a = a * (b * a) = a * e = a$.

That is, G2 also holds.
Thus, $(G, *)$ satisfies G1, G2 and G3.

Now consider some more examples of groups.

Example 4 : Let $G = \{\pm 1, \pm i\}$, $i = \sqrt{-1}$. Let the binary operation be multiplication. Show that $(G, \cdot)$ is a group.

Solution : The table of the operation is

	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

This table shows us that $a.1 = a\ \forall\ a \in G$. Therefore, 1 is the identity element. It also shows us that $(G, \cdot)$ satisfies G3'. Therefore, $(G, \cdot)$ is a group.

Note that $G = \{1, x, x^2, x^3\}$, where $x = i$.

From Example 4 you can see how we can use Theorem 3 to decrease the amount of checking we have to do while proving that a system is a group.

Note that the group in Example 4 has only 4 elements, while those in Example 3 and E4 have infinitely many elements. We have the following definitions.

Definition : If (G, ∗) is a group, where G is a finite set consisting of n elements, then we say that (G,∗) is a Finite group of order n. If G is an infinite set, then we say that (G,∗) is an infinite group.

If ∗ is a commutative binary operation we say that (G, ∗) is a commutative group, or an **abelian** group. Abelian groups are named after the gifted young Norwegian mathematician Niels Henrik Abel.

Fig 2 : N.H. Abel (1802-1829)

Thus, the group in Example 4 is a finite abelian group of order 4. The groups in Example 3 and E4 are infinite abelian groups.

Now let us look at an example of a **non-commutative** (or non-abelian) group. Before doing this example recall that an m × n matrix over a set S is a rectangular arrangement of elements of S in m rows and n columns.

Example 5 : Let G be the set of all 2 x 2 matrices with non-zero determinant. That is,

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a,b,c,d \in \mathbf{R},\ ad-bc \neq 0 \right\}$$

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then ad-bc is called the determinant of A. and is written as det A or $|A|$.

Consider G with the usual matrix multiplication, i.e, for

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \text{ in G, } A.P = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$$

Show that (G, ·) is a group.

Solution : First we show that · is a binary operation, that is, A, P ∈ G ⇒ A.P ∈ G. Now,

det (A.P) = det A. det P ≠ 0, since det A ≠ 0, det P ≠ 0.

Hence, A.P ∈ G for all A, P in G.

det (AB) = (det A) (det B)

We also know that matrix multiplication is associative and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity. Now, for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G, the mamx

$$B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \text{ is such that det } B = \frac{}{ad-bc} \neq 0 \text{ and } AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, $B = A^{-1}$. (Note that we have used the axiom G3' here, and not G3.) This shows that the set of all 2 x 2 matrices over R with non-zero determinant forms a group under multiplication. Since

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}, \text{ and}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix},$$

we see that this group is not commutative.

This group is usually denoted by $GL_2(\mathbf{R})$, and is called the general linear group of order 2 over R. We will be using this group for examples throughout Blocks 1 and 2.

And now another example of an abelian group.

Example 6 : Consider the set of all translations of $\mathbf{R}^2$,

$$T = \left\{ f_{a,b} : \mathbf{R}^2 \to \mathbf{R}^2 \;\middle|\; f_{a,b}(x,y) = (x+a, y+b) \text{ for some fixed } a,b \in \mathbf{R} \right\}$$

Note that each element $f_{a,b}$ in T is represented by a point (a,b) in $\mathbf{R}^2$. Show that (T,o) is a group, where o denotes the composition of functions.

Solution : Let us see if o is a binary operation on T.

Now $f_{a,b} \circ f_{c,d}(x,y) = f_{a,b}(x+c, y+d) = (x+c+a, y+d+b)$
$= f_{a+c, b+d}(x,y)$ for any $(x,y) \in \mathbb{R}^2$.

$\therefore f_{a,b} \circ f_{c,d} = f_{a+c, b+d} \in T$.
Thus, o is a binary operation on T.
Now, $f_{a,b} \circ f_{0,0} = f_{a,b}\ \forall\ f_{a,b} \in T$.
Therefore, $f_{0,0}$ is the identity element.
Also, $f_{a,b} \circ f_{-a,-b} = f_{0,0}\ \forall\ f_{a,b} \in T$.
Therefore, $f_{-a,-b}$ is the inverse of $f_{a,b} \in T$.
Thus, (T,o) satisfies G1', G2' and G3', and hence is a group.
Note that $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}\ \forall\ f_{a,b}, f_{c,d} \in T$. Therefore, (T,o) is abelian.
Try the following exercises now.

E 5) Let $\mathbf{Q}^*$, R* and Z* denote the sets of non-zero rationals, reals and integers. Are the following statements true? If not, give reasons.

a) $(Q^*, .)$ is an abelian group.

b) $(\mathbf{R}^*, .)$ is a finite abelian group.

c) $(z^*, .)$ is a group.

d) $(Q^*, .)$, $(R^*, .)$ and $(\mathbf{Z}^*, .)$ are semigroups.

E 6) Show that (G,*) is a non-abelian group,

where $G = \{(a,b) \mid a,b \in R, a \neq 0\}$ and * is defined on G by
$(a,b) * (c,d) = (ac, bc+d)$.

We will now look at some properties that elements of a group satisfy.

2.4 PROPERTIES OF GROUPS

In this section we shall give some elementary results about properties that group elements satisfy. But first let us give some notational conventions.

Convention : Henceforth, for convenience, we will **denote a group (G,*) by** G, if there is no danger of confusion. We will also **denote a * b by ab,** for a, b ∈ G, and say that we are **multiplying** a **and b.** The letter e will continue to denote the group identity.

Now let us prove a simple result.

Theorem 4 : Let G be a group. Then

a) $(a^{-1})^{-1} = a$ for every $a \in G$.

b) $(ab)^{-1} = b^{-1} a^{-1}$ for all a, b ∈ G.

Proof : (a) By the definition of inverse,

$$(a^{-1})^{-1} (a^{-1}) = e = (a^{-1}) (a^{-1})^{-1}.$$

But, $a a^{-1} = a^{-1} a = e$ also, Thus, by Theorem 1 (b), $(a^{-1})^{-1} = a$.

(b) For a, b ∈ G, ab ∈ G. Therefore, $(ab)^{-1} \in G$ and is the unique element satisfying $(ab)(ab)^{-1} = (ab)^{-1}(ab) = e$.

However, $(ab)(b^{-1} a^{-1}) = ((ab) b^{-1}) a^{-1}$
$= (a (b b^{-1}) a^{-1})$
$= (a e) a^{-1}$

$= aa^{-1}$

$= e$

Similarly, $(b^{-1} a^{-1})(ab) = e$.

Thus, by uniqueness of the inverse we get $(ab)^{-1} = b^{-1} a^{-1}$.
Note that, for a group G, $(ab)^{-1} = a^{-1} b^{-1} \forall a, b \in G$ only if G is abelian.

You know that whenever ba = ca or ab = ac for a, b, c in R*,
we can conclude that b = c. That is, we can cancel a. This fact is true for any group.

Theorem 5 : For a, b, c in a group G,

a) $ab = ac \Rightarrow b = c$. (This is known as the **left** cancellation law.)

b) $ba = ca \Rightarrow b = c$. (This is known as the right cancellation **law.)**

Proof : We will prove (a) and leave you to prove (b) (see E 7).

(a) Let ab = ac. Multiplying both sides on the left hand side by $a^{-1} \in G$, we get

$a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1} a) b = (a^{-1} a)c$

$\Rightarrow eb = ec$, e being the identity element.

$\Rightarrow b = c$.

Remember that by multiplying we mean we are performing the operation $*$.

E 7) Prove (b) of Theorem 5.

Now use Theorem 5 to solve the following exercise.

E 8) If in a group ***G,*** there exists an element g such that **gx** = g for all $x \in G$, then show that G = {e}.

We now prove another property of groups.

Theorem ***6*** : For elements a. b in a group G, the equations ax = b and ya = b have unique solutions in G.

Proof : We will first show that these linear equations do have solulions in G, and then we. will show that the solutions are unique.

For a, $b \in G$, consider $a^{-1} b \in G$. We find that $a(a^{-1} b) = (aa^{-1}) b = eb = b$. Thus, $a^{-1} b$ satisfies the equation ax = b, i.e., ax = b has a solution in G.

But is this the only solution ? Suppose x_1, x_2 are two solutions of ax = b in G. Then $ax_1 = b = ax_2$. By the left cancellation law, we gel $x_1 = x_2$. Thus, $a^{-1} b$ is the unique solution in G.

Similarly, using the right cancellation law, we can show that ba^{-1} is the unique solution of ya = b in G.

Now we will illustrate the property given in Theorem ***6***.

Example 7 : onsier $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in GL, (**R**) (see Example 5).

Find the solution of AX = B.

Solution : From Theorem ***6,*** we know that $X = A^{-1} B$. Now,

$A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$ (see Example 5).

$\therefore A^{-1} B = \begin{bmatrix} 2 & -2 \\ -1 & 3 \end{bmatrix} = X.$

In the next example we consider an important group.

Example 8 : Let S be a non-empty set. Consider $\wp(S)$ (see Example 2) with the binary operation of symmetric difference A, given by
$A \Delta B = (A \setminus B) \cup (B \setminus A) \quad \forall A, B \in \wp(S)$.
Show that $(\wp(S), A)$ is an abelian group. What is the unique solution for the equation $Y \Delta A = B$?

Solution : A is an associative binary operation. This can be seen by using the facts that

$A \setminus B = A \cap B^c$, $(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$

and that $\cup$ and $\cap$ are commutative and associative. A is also commutative since $A \Delta B = B \Delta A \; \forall A, B \in \wp(S)$.

Also, ϕ is the identity element since $A \Delta \phi = A \; \forall A \in \wp(S)$.

Further, any element is its own inverse, since $A \Delta A = \phi \; \forall A \in \wp(S)$.
Thus, $(\wp(S), A)$ is an abelian group.

For A, B in $(\wp(S), A)$ we want to solve $Y \Delta A = B$. But we know that A is its own inverse. So, by Theorem 6, $Y = B \Delta A^{-1} = B \Delta A$ is the unique solution. What we have also proved is that $(B \Delta A) \Delta A = B$ for any A, B in $\wp(S)$.

Try the following exercise now.

E 9) Consider Z with subtraction as a binary operation. Is $(Z, -)$ a group ? Can you obtain a solution for $a - x = b \; \forall a, b \in Z$?

And now let us discuss repeated multiplication of an element by itself.

Definition : Let G be a group. For $a \in G$, we define

i) $a^0 = e$.

ii) $a^n = a^{n-1}.a$, if $n > 0$

iii) $a^{-n} = (a^{-1})^n$, if $n > 0$.

n is called the **exponent** (or index) of the integral power a^n of a.
Thus, by definition $a^1 = a$, $a^2 = a.a$, $a^3 = a^2.a$, and so on.

Note : When the notation used fur the binary operation is addition, a^n becomes na. For example, f a any $a \in Z$,
$na = 0$ if $a = 0$,
$na = a + a + \ldots + a$ (n times) if $n > 0$;
$na = (-a) + (-a) + \ldots + (-a)$ ($-n$ times) if $n < 0$.

Let us now prove some laws of indices for group elements.

Theorem 7 : Let G be a group. For $a \in G$ and $m, n \in Z$,

a) $(a^n)^{-1} = a^{-n} = (a^{-1})^n$, **b)** $a^m . a^n = a^{m+n}$, **c)** $(a^m)^n = a^{mn}$.

Proof : We prove **(a) and (b),** and leave the proof of (c) to you (see E 10).

(a) If $n = 0$, clearly $(a^n)^{-1} = a^{-n} = (a^{-1})^n$.
Now suppose $n > 0$. Since $aa^{-1} = e$, we see that
$e = e^n = (aa^{-1})^n$
$= (aa^{-1})(aa^{-1}) \ldots\ldots (aa^{-1})$ (n times)
$= a^n (a^{-1})^n$, since a and a^{-1} commute.
$\therefore (a^n)^{-1} = (a^{-1})^n$.
Also, $(a^{-1})^n = a^{-n}$, by definition.
$\therefore (a^n)^{-1} = (a^{-1})^n = a^{-n}$ when $n > 0$.
If $n < 0$, then $(-n) > 0$ and
$(a^n)^{-1} = [a^{-(-n)}]^{-1}$
$= [(a^{-n})^{-1}]^{-1}$, by the case $n > 0$
$= ad$

Also, $(a^{-1})^n = (a^{-1})^{-(-n)}$
$= [(a^{-1})^{-1}]^{-n}$, by the case $n > 0$
$= a^n$.

So, in this case too,
$(a^n)^{-1} = a^{-n} = (a^{-1})^n$.

(b) If $m = 0$ or $n = 0$, then $a^{m+n} = a^m.a^n$. Suppose $m \neq 0$ and $n \neq 0$.
We will consider 4 situations.

Case 1 ($m > 0$ and $n > 0$) : We prove the proposition by induction on n.
If $n = 1$, then $a^m.\ a = a^{m+1}$, by definition.
Now **assume** that $a^m.\ a^{n-1} = a^{m+n-1}$
Then, $a^m.\ a^n = a^m(a^{n-1}.\ a) = (a^m\ .\ a^{n-1})\ a = a^{m+n-1}.\ a = a^{m+n}$. Thus, by the principle of induction, (a) holds for all $m > 0$ and $n > 0$.

Case 2 ($m < 0$ and $n < 0$) : Then $(-m) > 0$ and $(-n) > 0$. Thus, by Case 1, $a^{-n}.\ a^{-m} = a^{-(n+m)} = ad^{wn})$. Taking inverses of both the sides and using (a), we get,
$a^{m+n} = (a^{-n}.\ a^{-m})^{-1} = (a^{-m})^{-1}.\ (a^{-n})^{-1} = a^m.a^n$.

Case 3 ($m > 0, n < 0$ such that $m + n \geq 0$) : Then, by Case 1, $a^{m+n}.\ a^{-n} = a^m$. Multiplying both sides on the right by $a^n = (a^{-n})^{-1}$, we get $a^{m+n} = a^m.\ a^n$.

Case 4 ($m > 0, n < 0$ such that $m+n < 0$): By Case 2, $a^{-m}\ .\ a^{m+n} = a^n$. Multiplying both sides on the left by $a^m = (a^{-m})^{-1}$, we get $a^{m+n} = a^m\ .\ a^n$.

The cases when $m < 0$ and $n > 0$ are **similar** to Cases 3 and 4. Hence, $a^{wn} = a^m.a^n$ for all $a \in G$ and $m, n \in Z$.

To finish the proof of this theorem, try E 10.

E 10) Now you can prove (c) of **Theorem 7.**

(Hint : Prove, by induction on n, for the case $n > 0$. Then prove for $n < 0$.)

We will now study three. important groups.

2.5 THREE GROUPS

In this section we shall look at three **groups** that we will use as **examples** very often throughout this course — the group of **integers** modulo n, the symmetric group and the set of complex numbers.

2.5.1 Integers Modulo n

Consider the set of integers, Z, and $n \in N$. Let us define the relation of congruence on Z by : a is congruent to b modulo n if n divides a–b. We write this as $a \equiv b \pmod n$. For **example,** $4 \equiv 1 \pmod 3$, since $3 \mid (4-1)$.

Similarly, $(-5) \equiv 2 \pmod 7$ and $30 \equiv 0 \pmod 6$.

$\equiv$ is an equivalence relation (see **Sec.1.4.),** and hence partitions Z into disjoint equivalence classes called congruence **classes** modulo n. We denote the class containing r by $\bar{r}$.

Thus, $\bar{r} = \{ m \in Z \mid m \equiv r \pmod n \}$.

So an integer m belongs to $\bar{r}$ for some r, $0 \leq r < n$, iff $n \mid (r-m)$, **i.e.,** iff $r-m = kn$, for some $k \in Z$..

$\therefore\ \bar{r} = \{ r+kn \mid k \in Z \}$.

Now, if $m \geq n$, then the division **algorithm** says that $m = nq+r$ for some q, $r \in Z$, $0 \leq r < n$. That is, $m \equiv r \pmod n$, for **some** $r = 0, \ldots, n-1$. Therefore, all the congruence classes modulo n are $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Let $Z_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$. We define the operation + on Z_n by $\bar{a} + \bar{b} = \overline{a+b}$.

Is this operation well defined? To check this, we have to see that if $\bar{a} = \bar{b}$ and $\bar{c} = \bar{d}$ in $\mathbf{Z}_n$, then $\overline{a+b} = \overline{c+d}$.

Now, $a \equiv b \pmod n$ and $c \equiv d \pmod n$. Hence, there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $c - d = k_2 n$. But then $(a+c)-(b+d) = (a-b) + (c-d) = (k_1 + k_2)n$.

$\therefore \overline{a+c} = \overline{b+d}$.

Thus, + is a binary operation on Z, .

For example, $\bar{2} + \bar{2} = \bar{0}$ in $\mathbf{Z}_4$ since $2 + 2 = 4$ and $4 \equiv 0 \pmod 4$.

To understand addition in $\mathbf{Z}_n$, try the following exercise.

E 11) Fill up the following operation table for + on $\mathbf{Z}_4$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

Now, let us show that $(\mathbf{Z}_n, +)$ is a commutative group.

i) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ $\forall\, \bar{a}, \bar{b} \in \mathbf{Z}_n$, i.e., addition is commutative in Z_n.

ii) $\bar{a} + (\bar{b} + \bar{c}) = + (\overline{b+c}) = \overline{a + (b+c)}$

$= \overline{(a+b)+c} = (\overline{a+b}) + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$ $\forall\ \bar{a}, \bar{b}, \bar{c} \in Z_n$,

i.e., addition is associative in $\mathbf{Z}_n$.

iii) $\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}$ $\forall\, \bar{a} \in Z_n$, i.e., $\bar{0}$ is the identity for addition,

iv) $\sim$ o r ; $\in \mathbf{Z}_n$, $\exists\ \overline{n-}$ $\mathbf{Z}_n$ such that $\bar{a} + \overline{n - a} = n = 0 = n - a + a$.

Thus, every element $\bar{a}$ in $\mathbf{Z}_n$ has an inverse with respect to addition.

The properties (i) to (iv) show that $(\mathbf{Z}_n, +)$ is an abelian group.

Try the following exercise now.

E 12) Describe the partition of $\mathbf{Z}$ determined by the relation 'congruence modulo 5'.

Actually we can also define multiplication on $\mathbf{Z}_n$ by $\bar{a} \cdot \bar{b} = \overline{ab}$. Then, $\bar{b} = \bar{b}\ \bar{a}$ $\forall\, \bar{a}, \bar{b} \in \mathbf{Z}_n$. Also, $(\bar{a}\ \bar{b})\ \bar{c} = \bar{a}\ (\bar{b}\ \bar{c})$ $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_n$. Thus, multiplication in $\mathbf{Z}_n$ is a commutative and associative binary operation.

$\mathbf{Z}_n$ also has a multiplicative identity, namely, $\bar{1}$.

But $(Z_n, .)$ is not a group. This is because every element of $\mathbf{Z}_n$, for example $\bar{0}$, does not have a multiplicative inverse.

But, suppose we consider the non-zero elements of $\mathbf{Z}_n$, that is, $(\mathbf{Z}_n^*, .)$. Is this a group? For example $\mathbf{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is not a group because . is not even a binary operation on $\mathbf{Z}_4^*$, since $\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbf{Z}_4^*$. But $(Z_p^*, .)$ is an abelian group for any prime p.

E 13) Show that $(Z_5^*, .)$ is an abelian group.
(Hint : Draw the operation table.)

Let us now discuss the symmetric group.

2.5.2 The Symmetric Group

We will now discuss the symmetric group briefly. In Unit 7 we will discuss this group in more detail.

Let X be a non-empty set. We have seen that the composition of functions defines a binary operation on the set $\mathcal{F}(X)$ of all functions from X to X. This binary operation is associative. I_X, the identity map, is the identity in $\mathcal{F}(X)$.

Now consider the subset $S(X)$ of $\mathcal{F}(X)$ given by

$S(X) = \{f \in \mathcal{F}(X) \mid f \text{ is bijective}\}$.

So $f \in S(X)$ iff $f^{-1}: X \to X$ exists. Remember that $f \circ f^{-1} = f^{-1} \circ f = I_X$. This also shows that $f^{-1} \in S(X)$.

Now, for all f, g in $S(X)$,

$(g \circ f) \circ (f^{-1} \circ g^{-1}) = I_X = (f^{-1} \circ g^{-1}) \circ (g \circ f)$, i.e., $g \circ f \in S(X)$.

Thus, $\circ$ is a binary operation on $S(X)$.

Let us check that $(S(X), \circ)$ is a group.

i) $\circ$ is associative since $(f \circ g) \circ h = f \circ (g \circ h)$ $\forall$ f, g, h $\in$ S(X).

ii) I_X is the identity element because $f \circ I_X = I_X \circ f \ \forall f \in S(X)$.

iii) f^{-1} is the inverse of f, for any $f \in S(X)$.

Thus, $(S(X), \circ)$ is a group. It is called the symmetric group on X.

If the set X is finite, say X = (1, 2, 3,.....,n), then we denote $S(X)$ by S_n and each $f \in S_n$ is called a permutation on n symbols.

Suppose we want to construct an element f in S_n. We can start by choosing f(1). Now, f(1) can be any one of the n symbols 1, 2, ... n. Having chosen f(1), we can choose f(2) from the set $\{1,2,.....,n\} \setminus \{f(1)\}$, i.e., in (n–1) ways. This is because f is 1-1. Inductively, after choosing f(i), we can choose f(i+1) in (n–i) ways. Thus, f can be chosen in $(1 \times 2 \times ....\times n) = n!$ ways, i.e., S_n contains n! elements.

For our convenience, we represent $f \in S_n$ by

$$\begin{pmatrix} 1 & 2 & \ldots\ldots\ldots & n \\ f(1) & f(2) & \ldots\ldots\ldots & f(n) \end{pmatrix}$$

For example. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ represents the function f : (1, 2, 3, 4} → {1, 2, 3, 4} : f (1) = 2, f(2) = 4, f (3) = 3, f (4) = 1. The elements in the top row can be placed in any order as long as the order of the elements in the bottom row is changed accordingly.

Thus, $\begin{pmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ also represents the same function f.

Try this exercise now.

E 14) Consider S_3, the set of all permutations on 3 symbols. This has 3! (= 6) elements. One is the identity function. I, Another is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Can you list the other four?

Now, while solving E 14 one of the elements you must have obtained is $f = \begin{pmatrix} 1 & 2 & 3. \\ 2 & 3 & 1 \end{pmatrix}$

Here $f(1) = 2$, $f(2) = 3$ and $f(3) = 1$. Such a permutation is called a cycle. In general we have the following definition.

Definition : We say that $f \in S_n$ is a cycle of length r if there are $x_1, \ldots, x_r$ in $X = \{1, 2, \ldots, n\}$ such that $f(x_i) = x_{i+1}$ for $1 \le i \le r-1$, $f(x_r) = x_1$ and $f(t) = t$ for $t \neq x_1, \ldots, x_r$. In this case f is written as $(x_1 \ldots x_r)$.

For example, by $f = (2\ 4\ 5\ 10) \in S_{10}$, we mean $f(2) = 4$, $f(4) = 5$, $f(5) = 10$, $f(10) = 2$ and $f(j) = j$ for $j \neq 2, 4, 5, 10$.

i.e., $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$

$f \in S_n$ fires an element x if $f(x) = x$.

Note that, in the notation of a cycle, we don't mention the elements that are left fixed by the permutation. Similarly, the permutation

$\begin{pmatrix} 2 & & 5 \\ & & 3 \\ 5 & & \end{pmatrix}$ is the cycle $(1\ 2\ 5\ 3\ 4)$ in S_5.

Now let us see how we calculate the composition of two permutations. Consider the following example in S_5.

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$$

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

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

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

since 1, 3 and 4 are left fixed.

The following exercises will give you some practice in computing the product of elements in S_n.

E 15) Calculate $(1\ 3) \circ (1\ 2)$ in S_3.

E 16) Write the Inverses of the following in S_3 :

a) $(1\ 2)$

b) $(1\ 3\ 2)$

Show that $[(1\ 2) \circ (1\ 3\ 2)]^{-1} \neq (1\ 2)^{-1} \circ (1\ 3\ 2)^{-1}$. (This shows that in Theorem 4(b) we can't write $(ab)^{-1} = a^{-1} b^{-1}$.)

And now let us talk of a group that you may be familiar with, without knowing that it is a group.

2.5.3 Complex Numbers

In this sub-section we will show that the set of complex numbers forms a group with respect to addition. Some of you may not be acquainted with some basic properties of complex numbers. We have placed these properties in the appendix to this unit.

Consider the set C of all ordered pairs (x, y) of real numbers, i.e., we take $C = R \times R$. Define addition (+) and multiplication (.) in C as follows:

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and

$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$

for (x_1, y_1) and (x_2, y_2) in C.

This gives us an algebraic system (C, +, .) called the system of complex numbers. We must remember that two complex numbers (x_1, y_1) and (x_2, y_2) are equal iff $x_1 = x_2$ and $y_1 = y_2$.

In Block 3 you will see that $(\mathbb{C}, +, \cdot)$ is also a ring and a **field.**

You can verify that + and . are commutative and associative.

Moreover,

i) $(0, 0)$ is the additive identity.

ii) for (x, y) in C, $(-x, -y)$ is its additive inverse.

iii) $(1, 0)$ is the multiplicative identity.

iv) if $(x, y) \neq (0, 0)$ in $\mathbb{C}$, then either $x^2 > 0$ or $y^2 > 0$.

Hence, $x^2 + y^2 > 0$. Then

$$(x, y) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$$

$$= \left(x \cdot \frac{x}{x^2 + y^2} - y \cdot \frac{(-y)}{x^2 + y^2}, \; x \cdot \frac{-y}{x^2 + y^2} + y \frac{x}{x^2 + y^2}\right)$$

$$= (1, 0)$$

Thus, $\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$ is the multiplicative inverse of (x, y) in C.

Thus, (C, +) is a group and $(\mathbb{C}^*, .)$ is a group. (As usual, $\mathbb{C}^*$ denotes the set of non-zero complex numbers.)

Now let us see what we have covered in this unit.

2.6 SUMMARY

In this unit we have

1) discussed various types of binary operations.
2) defined and given examples of groups.
3) proved and used the cancellation laws and laws of indices for group elements.
4) discussed the group of integers modulo n, the symmetric group and the group of complex numbers.

We have also provided an appendix in which we list certain basic facts about complex numbers.

2.7 SOLUTIONS/ANSWERS

E 1) a) $x \oplus y = y \oplus x \; \forall \; x, y \in R$.

Therefore, $\oplus$ is commutative.

$$(x \oplus y) \oplus z = (x+y-5) \oplus z = (x+y-5)+z-5$$
$$= x+y+z-10$$
$$= x \oplus (y \oplus z)$$

Therefore, $\oplus$ is associative.

$\oplus$ is not closed on N since $1 \oplus 1 \notin N$.

b) $*$ is commutative, not associative, closed on N.

c) A is not commutative, associative or closed on N.

E 2) a) The identity element with respect to $\oplus$ is 5.

Suppose e is the identity element for $*$.

Then $x * e = x \Rightarrow 2(x + e) = x \Rightarrow e = -\frac{x}{2}$, which depends on x. Therefore, there is no fixed element e in R for which $x * e = e * x = x \; \forall \; x \in R$. Therefore, $*$ has no identity element.

Similarly, **A** has no identity element.

b) The inverse of x with respect to $\oplus$ is 10–x. Since there is no identity for the other operations, there is no question of obtaining x^{-1}.

E 3) $\wp(S) = \{\phi, \{0\}, \{1\}, \{0,1\}\}$.

So, the table is

$\cap$	ϕ	{0}	{1}	S
ϕ	ϕ	ϕ	ϕ	ϕ
{0}	ϕ	{0}	ϕ	{0}
{1}	ϕ	ϕ	{1}	{1}
S	ϕ	{0}	{1}	S

E 4) Check that both of them satisfy G1, *G2* and G3.

E 5) (a) and (d) are true.

(b) R* is an infinite abelian group.

(c) (Z*,.) satisfies G1 and G2, but not *G3*. No integer, apart from ± 1, has a multiplicative inverse.

E 6) $((a,b) * (c,d)) * (e, f)$
$= (ac, bc+d) * (e, f)$
$= (ace, (bc+d)e + f)$
$= (a, b) * ((c, d) * (e, f))$

Thus, $*$ satisfies G1'.
$(a, b) * (1, 0) = (a, b) \; \forall \; (a, b) \in G$.

Therefore, G3' holds.

Therefore, (G,$*$) is a group.

E 7) $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1} \Rightarrow b = c$.

E 8) Let $x \in G$. Then $gx = g = ge$. So, by Theorem 5, $x = e$.
$\therefore \; G = \{e\}$.

E 9) (Z, –) is not a group since G1 is not satisfied.
For any a, $b \in Z$, $a - (a - b) = b$. So, $a - x = b$ has a solution for any a, $b \in Z$.

E 10) When $n = 0$, the statement is clearly true.

Now, let $n > 0$. We will apply induction on n. For $n = 1$, the statement is true.
Now, assume that it is true for n–1, that is, $(a^m)^{n-1} = a^{m(n-1)}$.
Then, $(a^m)^n = (a^m)^{n-1+1} = (a^m)^{n-1}. a^m$, by (b)

$= a^{m(n-1)}. a^m$

$= a^{m(n-1+1)}$, by (b)

$= a^{mn}$.

So, *(c)* is true $\forall \; n > 0$ and $\forall \; m \in Z$.

Now, let $n < 0$. Then $(-n) > 0$.

$\therefore$ $(a^m)^n = [(a^m)^{-n}]^{-1}$, by (a)

$= [a^{m(-n)}]^{-1}$, by the case $n > 0$

$= [a^{-mn}]^{-1}$

$= a^{mn}$, by (a).

Thus, $\forall$ m, n $\in$ Z, (c) holds.

E 11)

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

E 12) Z is the disjoint union of the following 5 equivalence classes.

$\bar{0}$ = { ....., –10, –5, 0, 5, 10, 15,.....}

$\bar{1}$ = { ....., –9, – 4, 1, 6, 11, ...}

$\bar{2}$ = { ....., –8, –3, 2, 7, 12, ...}

$\bar{3}$ = { ....., –7, –2, 3, 8, 13, ...}

$\bar{4}$ = { ....., –6, –1, 4, 9, 14, ...}.

E 13) The operation table for. on $\mathbf{Z}_5^*$ is

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

It shows that. is an associative and commutative binary operation on $\mathbf{Z}_5^*$, $\bar{1}$ is the multiplicative identity and every element has an inverse.

Thus, $(\mathbf{Z}_5^*, .)$ is an abelian group.

E 14) $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$.

E 15) f = (1 3), g = (1 2).

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

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

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

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

E 16) a) Let $f = (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. $\therefore f^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$,

just interchanging the rows.

$\therefore$ $f^{-1} = (1\ 2)$.

b) $(1\ 3\ 2)^{-1} = (2\ 3\ 1)$.

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

Its inverse is $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = (1\ 3)$.

On the other hand,

$(1\ 2)^{-1} \circ (1\ 3\ 2)^{-1} = (1\ 2) \circ (1\ 2\ 3) = (2\ 3) \# (1\ 3)$.

APPENDIX : COMPLEX NUMBERS

Any complex number can be denoted by an ordered pair of real numbers (x, y). In fact, the set of complex numbers is

$\mathbf{C} = \{ (x, y) \mid x, y \in \mathbf{R} \}$.

Another way of representing $(x, y) \in C$ is $x + iy$, where $i = \sqrt{-1}$.

We call x the **real part** and y the imaginary **part** of $x + iy$.

The two representations agree if we denote $(x, 0)$ by x and $(0, 1)$ by **i**. On doing so we can write

$x + iy = (x, 0) + (0, 1)(v, 0)$

$= (x, 0) + (0, y)$

$= (x, y)$,

and $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$.

While working with complex numbers, we will sometimes use the notation $x+iy$, and sometimes the fact that the elements of C can be represented by points in R^2.

You can see that

$$\begin{aligned}(x_1 + iy_1) + (x_2 + iy_2) &= (x_1, y_1) + (x_2, y_2) \\ &= (x_1 + x_2, y_1 + y_2) \\ &= (x_1 + x_2) + i(y_1 + y_2), \text{ and}\end{aligned}$$

$$\begin{aligned}(x_1 + iy_1)(x_2 + iy_2) &= (x_1, y_1)(x_2, y_2) \\ &= (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \\ &= (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1).\end{aligned}$$

Now, given a complex number, we will define its conjugate.

Definition : For a complex number $z = x + iy$, the complex number $x + i(-y)$ is called the **conjugate** of **z.** It is also written as $x - iy$ and is denoted by $\bar{z}$.

For $z = x + iy$, we list the following properties.

i) $z + \bar{z}$ is a real number. In fact, $z + \bar{z} = 2x$.

ii) $z \cdot \bar{z} = x^2 + y^2$, a non-negative real number.

iii) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$, for any $z_1, z_2 \in C$. This is because

$$\begin{aligned}\overline{(x_1 + x_2) + i(y_1 + y_2)} &= (x_1 + x_2) - i(y_1 + y_2) \\ &= (x_1 - iy_1) + (x_2 - iy_2) \\ &= \bar{z}_1 + \bar{z}_2.\end{aligned}$$

iv) $\overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2$, for any $z_1, z_2 \in \mathbf{C}$.

Let us now see another way of representing complex numbers.

Geometric Representation of Complex Numbers

We have seen that a complex number $z = x + iy$ is represented by the point (x, y) in the plane. If O is the point (0,0) and P is (x, y) (see Fig.3), then we know that the distance $OP = \sqrt{x^2 + y^2}$. This is called the **modulus (or the absolute value)** of the complex number z and is denoted by $|z|$. Note that $\sqrt{x^2 + y^2} = 0$ iff $x = 0$ **and** $y = 0$.

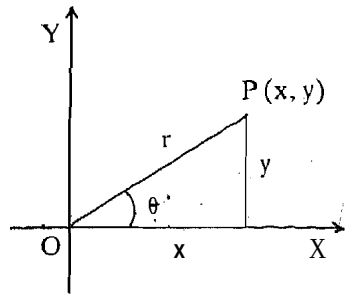

Fig. 3 : Geometric representation of x + iy

Now, let us denote $|z|$ by r and the angle made by OP with the positive x-axis by **θ.** Then **θ** is called **an argument** of the non-zero complex number z. If **θ** is an argument of z, then $\theta + 2n\pi$ is also an argument of z for all $n \in \mathbb{Z}$. However, there is a unique value of these arguments which lies in the interval $[-\pi, \pi]$. It is called the **principal argument** of **x+iy,** and is denoted by **Arg (x + iy).**

From Fig.3 you can see that $x = r\cos\theta$, $y = r\sin\theta$. That is,
$z = (r\cos\theta, r\sin\theta) = r(\cos\theta + i\sin\theta) = re^{i\theta}$.

This is called the **polar form** of the complex number (x+iy).
Now, if $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, then
$z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}$.

Thus, **an argument of $z_1 z_2$ = an argument of z_1 + an argument of z_2.**

We can similarly show that if $z_2 \neq 0$,
an argument of $\frac{z_1}{z_2}$ = an argument of z_1 − an argument of z_2.

In particular, if θ is an argument of z ($\neq 0$), then $(-\theta)$ is an argument of z^{-1}.

We end by stating one of the important theorems that deals with complex numbers.

De Moivre's Theorem : If $z = r(\cos\theta + i\sin\theta)$ and $n \in \mathbb{N}$, then
$z^n = r^n (\cos n\theta + i \sin n\theta)$.