MODULE 1

UNIT 1 SETS AND FUNCTIONS

CONTENTS

1.0 INTRODUCTION

In this unit we first discuss some ideas concerning sets and functions. These concepts are fundamental to the study of any branch of mathematics, in particular, algebra.

In MTH 131, we discuss some elementary number theory. The primary aims of this section, is to discuss some few facts that we will need in the rest of the course. We also hope to:

Give you a glimpse of the elegance of number theory. It is this elegance that led the mathematician Gauss to call number theory the 'queen of mathematics'.

We would like to repeat that this unit consists of very basic ideas that will be used throughout the course. So go through it carefully.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- use various operations on sets
- define Cartesian products of sets
- check if a relation is an equivalence relation or not, and find equivalence classes
- define and use different kinds of functions
- state the principle of induction
- use the division algorithm and unique prime factorisation theorem.

3.0 MAIN CONTENT

3.1 Sets

You must have used the word 'set' off and on in your conversations to describe any collection. In mathematics the term set is used to describe any **well defined** collection of objects, that is, every set should be so described that given any object it should be clear whether the given object belongs to the set or not.

For instance, the collection N of all natural numbers is well defined, and hence is a set. But the collection of all rich people is not a set, because there is no way of deciding whether a human is rich or not.

If S is set, an object **a** in the collection S is called an **element** of S. This fact is expressed in symbols as $\mathbf{a} \in S$ (read as "**a** is in S" or "**a** belongs to S"). If **a** is not in S, we write $\mathbf{a} \in S$. For example, $3 \in \mathbf{R}$ the set of real numbers. But. $\sqrt{-1} \notin \mathbf{R}$.

Elementary Group Theory

A set with no element in it is called the **empty** set, and is denoted by the Greek ϕ (phi). For example, the set of all natural numbers less than 1 is ϕ.

There are usually two way of describing a non-empty set:

(1) Roster method, and (2) set builder method.

Roster Method

In this method, we list all the elements of the set: within braces. For instance, the collection of all positive divisors of 48 contains 1, 2, 3, 4, 6, 8, 12, 16, 24 and 48 as its elements. So this set may be written as '{1, 2, 3, 4, 6, 8, 12, 16, 24, 48}.

In this description of a set, the following two conventions are followed:

Convection 1

The order in which the elements of the set are listed is not important.

Convention 2

No element is written more than once, that is, every element must be written exactly once.

For example, consider the set S of all integers between $\frac{1}{2}$ and $4\frac{1}{4}$. Obviously, these integers are 2, 3 and 4. So we may write S = (2, 3, 4}.

We may also write S = (3, 2, 4}, but we must not write S = (2, 3, 2, 4}. Why? Isn't this what Convention 2 says?

The roster method is sometimes used to list the elements of a large set also. In this case we may not want to list all the elements of the set. We list a few, enough to give an indication of the rest of the elements. For example, the set of integers lying between 0 and 100 is {0, 1, 2… 100}, and the set of all integers is
Z = {0, $\pm 1, \pm 2, \ldots\ldots$}.

Another method that we can use for describing a set is the

Set Builder Method

In this method we first try to find a property which characterises, the elements of the set, that is, a property P which all the elements of the set possess. Then we describe the set as:

{x | x has property P}, or as

{x: x has property P}.

This is to be read as "the set all x such that x has property P". For example, the set of all integers can also be written as
Z = {x | x is an integer}.

Some other sets that you may be familiar with are

Q, the set of rational numbers = $\left\{ \frac{a}{b} \;\middle|\; a, b \in Z, b \notin 0 \right\}$.

R, the set of real numbers

C, the set of complex numbers = {a+ib | a, b $\in$ R}. (Here i = $\sqrt{-1}$.)

Let us now see what subsets are.

Subsets

Consider the sets A = {1, 3, 4} and B = {1, 4}. Here every element of B is also all element of A. in such a case, that is, when every element of a set B is an element of a set A, we say that **B is a subset of A,** and we write this as **B $\subseteq$ A**.

for every set A, **A $\subseteq$ A.**

Also, for any set A, $\phi \subseteq$ **A**.

Now consider the set S = {1, 3, 5, 15} and T = (2, 3, 5, 7}. Is S $\subseteq$T? No, because not every element of S is in T; for example, 1 $\in$ S but 1$\notin$ T. In this case we say that S is not a subset of T, and denote it by S $\not\subseteq$ T.

'$\exists$' denotes 'there exists', Note that if B is not a subset of A, there must be an element of B which is not an element of A. In mathematical notation this can be written as '$\exists$' x ə B such that x $\notin$ A'.

We can now say that two sets **A and B are equal** (i.e., have precisely the same elements) **if and only if A $\subseteq$B and B $\subseteq$ A.**

Sets and Functions

Try the following exercise now.

SELF ASSESSMENT EXERCISE 1

Which of the following statements are true?

(a) N $\subseteq$ Z, (b) Z $\subseteq$ N, (c) {0} $\subseteq$ {1, 2, 3}, (d) {2, 4, 6} $\not\subseteq$ {2, 4, 8}.

Let us now look at some operations on sets. We will briefly discuss the operations of union, intersection and complementation on sets.

Union

If A and B are subsets of a set S, we can collect the elements of both to get a new set. This is called their union. Formally, we define the **union of A and B** to be the set of those elements of S which are in A or in B.

We denote the union of A and B by:

A U B. Thus,
$A \cup B = \{x \in S \mid x \in A \text{ or } x \in B\}$

For example, if A = {1, 2} and B = {4, 6, 7}, then A U B = {1, 2, 4, 6, 7}.

Again, if A = (1, 2, 3, 4] and B= (2, 4, 6, 8), A U B= (1, 2, 3, 4, 6, 8). Observe that 2 and 4 are in both A and B, but when we write A U B, we write these elements only once, in accordance with Convention 2 given earlier.

Can you see that, for any set A, $A \cup A = A$?

Try the following exercise now. While trying it remember that to show that $A \not\subset B$ you need to show that $x \in A \Rightarrow x \notin B$

SELF ASSESSMENT EXERCISE 2

Let A, B, C, be subsets of a set Such that $A \not\subset C$ and $B \not\subset C$.

Then show that:

a. $A \cup B \not\subset C$
b. $A \cup B = B \cup A$
c. $A \cup \phi = A$

Now will extend the definition of union to define the union of more than two sets.

If $A_1, A_2, A_3 \ldots\ldots A_k$ are k subsets of a set S, then their union $A_1 \cup A_2 \cup \ldots.. \cup A_k$ is the set of elements which belong to at least one of these sets. That is,
$A_1 \cup A_2 \cup \ldots\ldots \cup A_k = \{x \in \$ \quad x \in A_i \text{ for some } i = 1, 2 \ldots\ldots k)$.

The expression $A_1 \cup A_2 \cup \ldots.. \cup A_k$ is often abbreviated to $\bigcup_{i=1}^{k} A_i$.

If $\wp$ is a collection of subsets of a set S, then we can define the union of all members of $\wp$ by $\bigcup_{A \in \wp} A = \{x \in A \text{ for some } A \in \wp\}$

Now let us look at another way of obtaining a new set from two or more given sets.

Intersection

If A and B are two subsets of a set S, we can collect the elements that are common to both A and B. We call this set the **intersection** of **A and B** (denoted by $A \cap B$, So,

$A \cap B = \{x \in S \mid x \in A \text{ and } x \in B\}$

Thus, if P= {1, 2, 3, 4} and Q= {2, 4, 6, 8}, then $P \cap Q$= {2, 4}.

Can you see that, for any set A, $A \cap A = A$?

Now suppose A = {1, 2} and B = (4, 6, 7). Then what is $A \cap B$? We observe that, in this case A and B have no common elements, and so $A \cap B = \phi$, the empty set.

When the intersection of two sets is ϕ , we say that the two sets are **disjoint** (or **mutually disjoint**). For example, the sets {1, 4} and {0, 5, 7, 14} are disjoint.

Try this exercise now.

SELF ASSESSMENT EXERCISE 3

Let A and B be subsets of a set S. Show that

a. $A \cap B = B \cap A$
b. $A \subseteq B \Rightarrow A \cap B = A$
c. $A \cap \phi = \phi$

Elementary Group Theory

The definition of intersection can be extended to any number of sets.

Thus, the intersection of k subsets $A_1, A_2 \ldots\ldots A_k$ of a set S is
$A_1 \cap A_2 \cap \ldots\ldots A_k = \{x \mid \in S \quad x \in A_i \text{ for each } i = 1, 2, \ldots\ldots k\}$.

We can shorten the expression $A_1 \cap A_2 \cap \ldots\ldots A_k$ to $\bigcap_{i=1}^{k} A_i$.

In general, if $\wp$ is a collection of subsets of a set S, then we can define the intersection of all the members of $\wp$ by $\bigcap_{A \in \wp} A = \{x \in S \mid x \in A \forall A \in \wp\}$

In the following exercise we give important properties of unions and intersections of sets.

SELF ASSESSMENT EXERCISE 4

For any subsets, A, B, C of a set S, show that

a. $(A \cup B) \cup C = A \cup (B \cup C)$

b. $(A \cap B) \cap C = A \cap (B \cap C)$
c. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
d. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

SELF ASSESSMENT EXERCISE 5

State whether the following are true or false. If false, give a counter-example.

a. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$
b. If $A \not\subseteq B$ and $B \not\subseteq A$, then A and B are disjoint
c. $A \not\subseteq A \cup B$
d. If $A \cup B = \phi$, then $A = B = \phi$.

Apart from the operations of unions and intersections, there is another operation on sets, namely, the operation of taking differences.

Differences

Consider the sets A = {1, 2, 3} and B = {2, 3, 4}. Now the set of all elements of A that are not in B is {1}. We call this set the **difference A\B**. Similarly, the difference **B \ A** is the set of elements of B that are not in A, that is, {4}. Thus, for any two subsets ‘A and B of a set S, $\{x \in X \quad x \in A \text{ and } x \in B\}$.

When we are working with elements and subsets of a single set X, we say that the set X is the **universal set**. Suppose X is the universal set and $A \subseteq X$. Then the set of all elements of X which are not in A is called the complement of A and is denoted by A' A^c or X \ A.
Thus,

$A^c = \{x \in X \mid x \notin A\}$.

For example, if X = {a, b, p, q, r} and A = {a. p, q}, then $A^c = \{b, r\}$.

Try the following exercise now.

SELF ASSESSMENT EXERCISE 6

Why are the following statements true?

a. A and A^c are disjoint, i.e., $A \cap A^c = \phi$
b. $A \cup A^c = X$, where X is the universal set.
c. $(A^c)^c = A$.

And now we discuss one of the most important constructions in set theory.

3.2 Cartesian Products

An interesting set that can be formed from two given sets is their **Cartesian product**, named after a French philosopher and mathematician Rene Descartes (1596 -1650). He also invented the Cartesian coordinate system.

Let A and B be two sets. Consider the pair (a, b), in which the first element is from A and the second from B. Then (a, b) is called an **ordered pair**. In an ordered pair in order in which the two elements are written is important. Thus, **(a, b)** and **(b, a) are different ordered pairs**. Two ordered pairs **(a, b)** and **(c, d) are called equal, or the same, if a = c and b = d**.

Definition

The Cartesian product A x B, of the sets A and B, is the set of all possible ordered pairs (a, b), where $a \in A, b \in B$.

For example, if A = {1, 2,2 3} and B = {4, 6}, then A X B = { (1, 4), (1, 6), (2, 4), (2, 6), (3, 4), (3, 6)}.

Also note that
B x A = {(4, 1), (4, 2), (4, 3), (6, 1), (6, 2), (6, 3)} and A x B $\neq$ B x A.

Let us make some remarks about the **Cartesian product** here.
Remarks:

i. A x B = ϕ if A = ϕ or B = ϕ.

ii. If A has m elements and B has n elements, then A x B has mn elements. B x A also has mn elements. But the elements of B x A need not be the same as the elements of A x B, as you have just seen.

We can also define the Cartesian product of more than two sets in a similar way. Thus, if A_1, A_2, A_3 …..... A_n are n sets, we can define their **Cartesian product** as

$A_1 \times A_2 \times \ldots\ldots \times A_n = \{(a_1, a_2 \ldots\ldots a_n) \mid a_1 \in A_1 \ldots\ldots a_n \in A_n\}$.

For example, if **R** is the set of all real numbers, then

$\mathbf{R} \times \mathbf{R} = \{(a_1, a_2) \mid a_1, \in \mathbf{R}, a_2 \in \mathbf{R}\}$
$\mathbf{R} \times \mathbf{R} \times \mathbf{R} = \{(a_1, a_2, a_3) \mid ai, \in \mathbf{R}; i = 1, 2, 3\}$, and so on. It is customary to write $\mathbf{R}^2$ for **R** x **R** and $\mathbf{R}^n$ for **R** x …… x **R** (in n times).

Now, you know that every point in a plane has two coordinates, x and y. Also, every ordered pair (x, y) of real numbers defines the coordinates of a point in the plane. So, we can say that $\mathbf{R}^2$ represents a plane. In fact, $\mathbf{R}^2$ is the Cartesian product of the x-axis

and the y-axis. In the same way $\mathbf{R}^3$ represents three-dimensional space, and $\mathbf{R}^n$ represents n-dimensional space, for any $n \geq 1$. Note that **R** represents a line.

Try the following exercises now.

SELF ASSESSMENT EXERCISE 7

If A = {2, 5} B = {2, 3}, find A x B, B x A and A x A.

SELF ASSESSMENT EXERCISE 8

If A x B = {(7, 2), (7, 3), (7, 4), (2, 2), (2, 4)}, determine A and B.

SELF ASSESSMENT EXERCISE 9

Prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$ and $(A \cap B) \times C == (A \times C) \cap (B \times C)$.

Let us now look at certain subsets of Cartesian products.

3.3 Relations

You are already familiar with the concept of a relationship between people. For example, a parent-child relationship exists between A and B if and only if A is a parent of B or B is a parent of A.

In mathematics, relation **R** on a set S is a relationship between the elements of S. If $a \in S$ is related to $b \in S$ by means of relation, we write a **R** b or $(a, b) \in \mathbf{R} \subseteq S \times S$. And this is exactly how we define a relation on a set.

Definition

A **relation** R defined on a set S is a subset of S x S.

For example, if **N** is the set of natural and R is the relation' is a multiple of' then 15 R 5, but not 5 R 15. That is, $(15, 5) \in R$ but $(5, 15) \notin R$. Here $R \subseteq \mathbf{N} \times N$.

Again, if **Q** is the set of all rational numbers and R is the relation 'is greater than', then 3 R 2 (because 3> 2).

The following exercise deals with relations.

SELF ASSESSMENT EXERCISE 10

Let N be the set of all natural numbers and R the relation $\{(a, a^2)\ a \in N\}$. State whether the following are true or false:

a. 2 R 3, b. 3 R 9, c. 9 R 3.

We now look at some particular kinds of relations.

Definition

A relation R defined on a set S is said to be

i. **reflexive** if we have aRa $\forall$ a $\in$ S.
ii. **symmetric** if aRb $\Rightarrow$ bRa $\forall$a , b $\in$ S.
iii. **transitive** if aRb and bRc $\Rightarrow$ aRc $\forall$a, b, c $\in$ S.

To get used to these concepts, consider the following examples.

Example 1

Consider the relation **R** on **Z** given by 'aRb iff and only if a> b'. Determine whether R is reflexive, symmetric and transitive.

Solution

Since a > a is not true, aRa is not true. Hence, **R** is not reflexive.

If a > b, then certainly b > a is not true. That is, aRb does not imply bRa. Hence, it is symmetric,

Since a > b and b > c implies a > c, we find that aRb, bRc implies aRc. Thus, R is transitive.

Example 2

Let S be a non-empty set. Let $\wp$ (S) denote the set of all S, i.e., $\wp$ (S) = {A : A $\subseteq$ S}. We call $\wp$ (S) **the power set of S**.

Define the relation R on $\wp$ (S) by
R= {(A, B) | A, B $\in$ $\wp$(S) and A $\subseteq$ B}.

Check whether R is reflexive, symmetric or transitive.

Solution

Since $A \subseteq A \forall A \in \wp(S)$, R is reflexive.

If $A \subseteq B$, B need not be contained in A. (In fact, $A \subseteq$ Band $B \subseteq A \Leftrightarrow A = B$.) Thus, R is not symmetric.

If $A \subseteq$Band $B \subseteq C$, then $A \subseteq C \forall A, B, C \in \wp(S)$. Thus, R is transitive.

You may like to try the following exercises now.

SELF ASSESSMENT EXERCISE 11

The relation $R \subseteq N \times N$ is defined by $(a, b) \in$, R if 5 divides (a -b). Is R Reflexive? Symmetric? Transitive? ,

SELF ASSESSMENT EXERCISE 12

Give examples to show why the relation in **Self-Assessment Exercise l0** is not reflexive, symmetric or transitive.

The relationship in **Self-Assessment Exercise 11** is reflexive, symmetric and transitive. Such a relation is called an **equivalence relation**.

A very important property of an equivalence relation on a set S is that it divides S into a number of mutually disjoint subsets, that is, it **partitions** S. Let us see how this happens.

Let R be an equivalence relation on the set S. Let $a \in S$. Then the set $\{b \in S \ aRb\}$ is called the equivalence class of a in S. It is just the set of elements in S which are related to a. We denote it by [a].

For instance, what is the equivalence class of 1 for R given in **Self- Assessment Exercise** 11?

This is

[1] $= \{n \mid 1Rn, n \in \mathbf{N}\}$
$= \{ n \mid n \in N$ and 5 divides 1-n$\}$
$= \{ n \mid n \in N$ and 5 divides n-1$\}$
$= \{1, 6, 11, 16, 21 ...\}$,

Similarly,

[2] $= \{ n \mid n \in N \text{ and } 5 \text{ divides } n-2\}$
$= \{2, 7, 12, 17, 22,\},$
[3] $= \{3, 8, 13, 18, 23 ...\},$
[4] $= \{4, 9, 14, 19, 24,\},$
[5] $= \{5, 10, 15, 20, 25 ...\},$
[6] $= \{1, 6, 11, 16, 21 ...\},$
[7] $= \{2, 7, 12, 17, 22 ...\},$

Note that

i. [1] and [6] are not disjoint. In fact, [1] = [6]. Similarly, [2] = [7], and so on.
ii N = [1] $\cup$[2] $\cup$ [3] $\cup$ [4] $\cup$ [5], and the sets on the right hand side are mutually disjoint.

We will prove these observations in general in the following theorem.

Theorem 1

Let R be an equivalence relation on a set S. For $a \subseteq S$, let [a] denote the equivalence class of a. then

a. $a \in [a]$,
b. $b \in [a] \Leftrightarrow [a] = [b]$,
c. $S = \bigcup_{a \in S} [a]$
d. if $a, b \in S$, then $[a] \cap [b] = \phi$ or $[a] = [b]$.

Proof: a. Since **R** is an equivalence relation, it is reflexive.

$\therefore$ aRa $\forall$ $a \in S$, $\therefore$ $a \in [a]$.

b. Firstly, assume that $b \in [a]$. We will show that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. For this, let $x \in [a]$. Then xRa.

We also know that aRb. Thus, by transitivity of **R**, we have xRb, i.e., $x \in [b]$. $\therefore$ $[a] \subseteq [b]$.

We can similarly show that $[b] \subseteq [a]$.
$\therefore$ [a] = [b].

Conversely, assume that [a] = [b]. Then $b \in [b]$. $\therefore$ $b \in [a]$.

c. Since $[a] \subseteq S$ $\forall$ $a \in S$, $\bigcup_{a \in S} [a] \subseteq S$ (see **Self Assessment Exercise 2**).

Conversely, let $x \in S$. Then $\lambda \in [x]$, $x \subseteq [x]$ by (a) above. [x] is one of the sets in the collection whose union is $\bigcup_{a \in S} [a]$.

Hence, $x = \bigcup_{a \in S} [a]$. So, $S \subseteq \bigcup_{a \in S} [a]$.

Thus, $S \subseteq \bigcup_{a \in S} [a]$ and $\bigcup_{a \in S} [a] \subseteq S$, proving (c).

d. Suppose $[a] \cap [b] \neq \phi$. Let $x \in [a] \cap [b]$.

Then $x \in [a]$ and $x \in [b]$
$\Rightarrow [x] = [a]$ and $[x] = [b]$, by (b) above
$\Rightarrow [a] = [b]$.

Note that in **Theorem 1**, distinct sets on the right hand side of (c) are mutually disjoint because of (d). Therefore, (c) expresses S as a union of mutually disjoint subsets of S; that is we have a partition of S into equivalence classes.

Let us look at some more examples of partitioning a set into equivalence classes.

Examples 3

Let S be the set of straight lines in **R** x **R**. Consider the relation on S given by 'L_1 R L_2 if $L_1 = L_2$ or L_1 is parallel to L_2'. Show that R is an equivalence relation. What are the equivalence classes in S?

Solution

R is reflexive, symmetric and transitive. Thus, **R** is an equivalence relation.

Now, take any line L_1 (see Fig. 1).

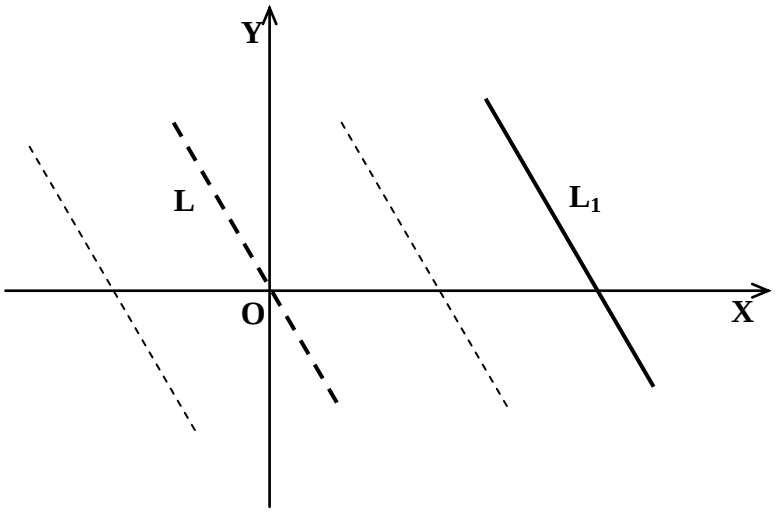

Fig. 1: The equivalence class of L_1

Let L be the line through (0, 0) and parallel to L_1. Then $L \in [L_1]$. Thus, $[L] = [L_1]$. In this way the distinct through (0, 0) give distinct equivalence classes into which S is partitioned. Each equivalence class [L] consists of all the lines in the planes that are parallel to L.

Now for a nice self assessment exercise!

SELF ASSESSMENT EXERCISE 13

Show that 'aRb if and only if |a| = |b|' is an equivalence relation on Z. what are [0] and [1]?

In the next section we will briefly discuss a concept that you may be familiar with namely, functions.

3.4 Functions

Recall that a function f from a non-empty set A to a non-empty set B is a rule which associates with every element of A exactly on element of B. This is written as f: A $\rightarrow$ B. If f associates with a $\in$ A, the element b of B, we write f(a) = b. A is called the domain of f, and the set f(A) = {f(a) | a $\in$ A} is called the **range** of f. The range of f is a subset of B, i.e., f(A) $\subseteq$ B. B is called the **codomain** of f.

Note that

i. For **each** element of A, we associate some element of B.

ii. For each element of A, we associate **only one** element of B.

iii Two or more elements of A could be associated with the same element of B.

For example, let A = {1, 2, 3}, B = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Define f: A $\rightarrow$ B by f(1) = 1, f(2) = 4, f(3) = 9. Then f is a function with domain A and range {1, 4, 9}. In this case we can also write $f(x) = x^2$ fro each x $\in$ A or f: A $\rightarrow$ B: $f(x) = x^2$. We will often use this notation for defining any function.

If we define g: A $\rightarrow$ B by g(1) = 1, g(2) = 1, g(3) = 4, then g is also a function. The domain of g remains the same, namely, A. but the range of g is {1, 4}.

Remark

We can also consider a function f: A $\rightarrow$ B to be the subset {(a, f(a)) | a $\in$ A} of A x B.

Now let us look at functions with special properties.

Definition

A function f: A $\rightarrow$ B is called **one-to-one** (or **injective**) if f associates different elements of **A** with different elements of **B**, i.e., if a_1, $a_2 \in$ A and $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. In other words, f is 1 - 1 if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.

In the examples given above, the function f is one-to-one. The function g is not one-one because 1 and 2 are distinct elements of A, but g(1) = g(2).

Now consider another example of sets and functions.

Let A = {1, 2, 3}, B = {p, q, r}. Let f: A $\rightarrow$ B be defined by f(1) = q, f(2) = r, f(3) = p. then f is a function. Here the range of f = B = codomain of f. This is an example of an onto function, as you shall see.

Definition

A function f: A $\rightarrow$ B is called **onto** (or **surjective**) if the range of f is B, i.e., if, for each b $\in$ B, there is an a $\in$ A such that f (a) = b. In other words, f is onto if f(A) = B.

For another important example of a surjective function, consider two non-empty sets A and B. we define the function π_1: A x B $\rightarrow$ A: π_1 ((a, b)) = a. π_1 is called the **projection** of A x B onto A. You can see that the range of π_1 is the whole of A. Therefore, π_1 is onto. Similarly, π_2: A x B $\rightarrow$ B: π_2 ((a, b)) = b, the projection of A x B onto B, is a surjective function.

If a function is both one-to-one and onto, it is called **bijective**, or a **bijection**. You will be using this type of function heavily in Block 2 of this course.

Consider the following example that you will use again and again.

Example 4

Let A be any set. The function I_A: A $\rightarrow$ A: $I_A(a) = a$ is called the **identity function** on A. Show that I_A is bijective.

Solution

For any a $\in$ A, $I_A(a) = a$. Thus, the range of I_A is the whole of A. That is, I_A is onto.

I_A is also: because if a_1, a_2, $\in$ A such that $a_1 \neq a_2$, then $I_A(a_1) \neq I_A(a_2)$.

Thus, I_A is bijective.

If f: A $\rightarrow$ B is a bijection, then we also say that the **sets A and B are equivalent**. Any set which is equivalent to the set {1, 2, 3…….. n}, for some n $\in$ N, is called a **finite** set. A set that is not finite is called an **infinite** set.

Convention

The empty set f is assumed to be finite.
Try the following self assessment exercise now.

SELF ASSESSMENT EXERCISE 14

Let f: N $\rightarrow$ N be defined by f(n) = n + 5. Prove that f is one-to-one but not onto.

SELF ASSESSMENT EXERCISE 15

Let f: Z $\rightarrow$ Z be defined by f(n) = n + 5. Prove that f is both one-one and onto.

The next exercise deals with a function that you will often come across, namely, the constant function f: A $\rightarrow$ B: f(a) = c, where c is a fixed element of B.

SELF ASSESSMENT EXERCISE 16

What must X be like for the constant function f: X $\rightarrow$ {c} to be injective? Is f surjective?

Let us now see what the inverse image of a function is.

Definition

Let A and B be two sets and f: A $\rightarrow$ B be a function. Then, for any subset S of B, the **inverse image** of S **under f** is the set.

$f^{-1}(S) = \{a \in A \mid f(a) \in S\}$.

For example, $I_A^{-1}(A) = \{a \in A \mid I_A(a) \in A\} = A$.

Again, for the function f in **Self-Assessment Exercise 14**,

$f^{-1}(\{1, 2, 3\}) = \{n \in \mathbf{N} \mid f(n) \in \{1, 2, 3\}\}$
$= \{n \in \mathbf{N} \mid n+5 \in \{1, 2, 3\}\}$
$= \phi$, the empty set.

But $f^{-1}(N) = \{6, 7, 8, ...\}$.

We now give some nice theorems involving the inverse image of a function.

Theorem 2

Let $f : A \to B$ be a function. Then,
a) for any subset S of B, $f(f^{-1}(S)) \subseteq S$.
b) for any subset X of A, $X \subseteq f^{-1}(f(X))$.

Proof

We will prove (a) and you can prove (b) (**see Self Assessment Exercise 17**). Let $b \in f(f^{-1}(S))$. Then, by definition, $\exists\ a \in f^{-1}(S)$ such that $b = f(a)$. But $a \in f^{-1}(S) \Rightarrow f(a) \in S$. That is, $b \in S$. Thus, $f(f^{-1}(S) \subseteq S$.

The theorem will be proved once you solve **Self Assessment Exercise 17.**

SELF ASSESSMENT EXERCISE 17

Prove (b) of Theorem 2.

SELF ASSESSMENT EXERCISE 18

Given $f: A \to B$ and $S, T \subseteq B$, show that

a. if $S \subseteq T$, then $f^{-1}(S) \subseteq f^{-1}(T)$.
b. $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$
c. $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

Now let us look at the most important way of producing new functions from given ones.

Composition of Functions

If $f : A \to B$ and $g: C \to D$ are functions and if the range of f is a subset of C, there is a natural way of combining g and f to yield a new function
$h: A \to D$. Let us see how.

For each $x \in A$, h(x) is defined by the formula $h(x) = g(f(x))$.

Note that f(x) is in the range of f, so that $f(x) \in C$. Therefore, g(f(x)) is defined and is an element of D. This function h is called the **composition of g and f** and is written as $\mathbf{g \circ f}$**.** The domain of $g \circ f$ is A and its codomain is D. In most cases that we will be dealing with we will have B = C. Let us look at some examples.

Example 5

Let f: $\mathbf{R} \rightarrow \mathbf{R}$ and g: $\mathbf{R} \rightarrow \mathbf{R}$ be defined by $f(x) = x^2$ and $g(x) = x + 1$. What is $g \circ f$? What is $f \circ g$?

Solution

We observe that the range of f is a subset of R, the domain of g. Therefore, $g \circ f$ is defined. By definition, $\forall x \in \mathbf{R}, g \circ f(x) = g(f(x)) = f(x) + 1 = x^2 + 1$.

Now, let us find $f \circ g$. Again, it is easy to see that $f \circ g$ is defined. $\forall x \in R, f \circ g(x) = f(g(x)) = (g(x))^2 = (x + 1)^2$.

So $f \circ g$ and $g \circ f$ are both defined. But $g \circ f \neq f \circ g$.

Example 6

Let A = {1, 2, 3}, B = {p, q, r} and C = {x, y}. Let f: $A \rightarrow B$ be defined by f(1) = p, f(2) = p, f(3) = r. Let g: $B \rightarrow C$ be defined by g(p) = x, g(q) = y, g(r) = y. determine if $f \circ g$ and $g \circ f$ can be defined.

Solution

For $f \circ g$ to be defined, it is necessary that the range of g should be a subset of the domain of f. In this case the range of g is C and the domain of f is A. As C is not a subset of A, $f \circ g$ cannot be defined.

Since the range of f, which is {p, r}, is a subset of B, the domain of g, we see that $g \circ f$ is defined. Also $g \circ f$: $A \rightarrow C$ is such that

$g \circ f(1) = g(f(1)) = g(p) = x$,
$g \circ f(2) = g(f(2)) = g(p) = x$,
$g \circ f(3) = g(f(3)) = g(r) = y$.

In this example note that g is surjective, and so is $g \circ f$.

Now for an exercise on the composition of functions.

SELF ASSESSMENT EXERCISE 19

In each of the following questions, both f and g are functions from $R \rightarrow R$. Define $f \circ g$ and $g \circ f$.

a. $f(x) = 5x$, $g(x) = x + 5$
b. $f(x) = 5x$, $g(x) = x/5$
c. $f(x) = |x|$, $g(x) = x^2$.

We now come to a theorem which shows us that the identity function behaves like the number $1 \in \mathbf{R}$ does for multiplication. That is, if we take the composition of any function f with a suitable identity function, we get the same function f.

Theorem 3

Let A be a set. For every function f: A $\rightarrow$ A, we have $f \circ I_A = I_A \circ f = f$.

Proof

Since both f and I_A are defined from A to A, both the compositions $f \circ I_A$ and $I_A \circ f$ are defined. Moreover, $\forall x \in$ A.,
$f \circ I_A(x) = f(I_A(x)) = f(x)$, so $f \circ I_A = f$.
Also, $\forall x \in$ A, $I_A \circ f(x) = I_A(f(x)) = f(x)$, so $I_A \circ f = f$.

You can try the next self assessment exercise on the lines of this theorem.

SELF ASSESSMENT EXERCISE 20

If A and B are sets and g: B $\rightarrow$ A, prove that $I_A \circ g = g$ and $g \circ I_B = g$.

In the case of real numbers, you know that given any real number $x \neq 0$, $\exists y \neq 0$ such that xy = 1. y is called the inverse of x. Similarly, we can define an inverse function for a given function.

Definition

Let f: A $\rightarrow$ B be a given function. If there exists a function g: B $\rightarrow$ A such that $f \circ g = I_B$ and $g \circ f = I_A$, then we say that g is the **inverse** of f, and we write $g = f^{-1}$.

For example, consider f: R $\rightarrow$ R defined by f(x) = x + 3. If we define g: R$\rightarrow$ R by g(x) = x – 3, then $f \circ g(x) = f(g(x)) = g(x) + 3 = (x - 3) + 3 = x$ $\forall x \in \mathbf{R}$. Hence, $f \circ g = I_R$. You can also verify that $g \circ f = I_R$. So $g = f^{-1}$.

Note that in this example f adds 3 to x and g does the opposite – it subtracts 3 from x. Thus, the key to filling the inverse of a given function is: try to retrieve x from f(x).

For example, let f: $\mathbf{R} \rightarrow \mathbf{R}$ be defined by f(x) = 3x + 5. How can we retrieve x from 3x + 5? The answer is "first subtract 5 and then divide by 3". So, we try $g(x) = \frac{x - 5}{3}$. And we find $g \circ f(x) = g(f(x)) = \frac{f(x) - 5}{3} = \frac{(3x + 5) - 5}{3} = x$.

Also, $f \circ g(x) = 3(g(x)) = 3\left[\frac{(x-5)}{3}\right] + 5 = x$.

Let's see if you've understood the process of extracting the inverse of a function.

SELF ASSESSMENT EXERCISE 21

What is the inverse of f: $\mathbf{R} \rightarrow \mathbf{R}$: $f(x) = \frac{x}{3}$?

Do all functions have an inverse? No, as the following example shows.

Example 7

Let f: $\mathbf{R} \rightarrow \mathbf{R}$, be the constant function given by $f(x) = 1$ $\forall x \in \mathbf{R}$. What is the inverse.

Solution

If f has an inverse g: $\mathbf{R} \rightarrow \mathbf{R}$, we have $f \circ g = I_g$, i.e. $\forall\, x \in \mathbf{R}$, $f \circ g(x) = x$.

Now take x = 5. We should have $f \circ g\,(5) = 5$, i.e., $f(g(5)) = 5$. But $f(g(5)) = 1$,

Since $f(x) = 1$ $\forall\, x \in \mathbf{R}$. So we reach a contradiction. Therefore, f has no inverse.

In view of this example, we naturally ask for necessary and sufficient conditions for f to have an inverse. The answer is given by the following theorem.

Theorem 4

A function f: $A \rightarrow B$ has an inverse if and only if f is bijective.

Proof

Firstly, suppose f is bijective. We shall define a function g: $B \rightarrow A$ and prove that $g = f^{-1}$.

Let $b \in B$. Since f is onto, there is some $a \in A$ such that $f(a) = b$. Since f is one-one, there is only one such $a \in A$. We take this unique element a of A as g(b). That is, given $b \in B$, we define $g(b) = a$, where $f(a) = b$.

Note that, since f is onto, $B = \{f(a) \mid a \in A\}$. Then, we are simply defining g: $B \rightarrow A$ by $g(f(a)) = a$. This automatically ensures that $g \circ f = I_A$.

Now, let $b \in B$ and $g(b) = a$. Then $f(a) = b$, by definition of g. Therefore, $f \circ g(b) = f(g(b)) = f(a) = b$. Hence, $f \circ g = I_B$.

So, $f \circ g = I_B$ and $g \circ f = I_A$. This proves that $g = f^{-1}$.

Conversely, suppose f has an inverse and that $g = f^{-1}$. We must prove that f is one-one and onto.

Suppose $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$.
$\Rightarrow g \circ f(a_1) = g \circ f(a_2)$
$\Rightarrow a_1 = a_2$, because $g \circ f = I_A$.
So, f is one-one.

Next, given $b \in B$, we have $fog = I_B$, so that $f \circ g(b) = I_B(b) = b$,
i.e., $f(g(b)) = b$. That is, f is onto.

Hence, the theorem is proved.

Try the following self assessment exercise now.

SELF ASSESSMENT EXERCISE 22

Consider the following functions from R to R. For each determine whether it has an inverse and, when the inverse exists, find it.

a. $f(x) = x^2$ **∀** $x \in \mathbf{R}$.
b. $f(x) = 0$ **∀** $x \in \mathbf{R}$.
c. $f(x) = 11x + 7$ **∀** $x \in \mathbf{R}$.

Let us now discuss some elementary number theory.

3.5 Some Number Theory

In this section we will spell out certain factorization properties of integers that we will use throughout the course. For this we first need to present the principle of finite induction.

3.5.1 Principle of Induction

We will first state an axiom of the integers that we will often use implicitly, namely, the well-ordering principle. We start with a definition.

Definition

Let S be a non-empty subset of **Z**. An element $a \in S$ is called a **least element** (or a **minimum element**) of S if $a \leq b$ **∀** $b \in S$. For example, n has a least element, namely, 1. But **Z** has no least element. In fact, many subsets of Z, like 2Z, {-1, -2, -3, ...}, etc., don't have least elements.

The following axiom tells us of some sets that have a least element.

Well-ordering Principle: Every non-empty subset of N has a least element.

You may be surprised to know that this principle is actually equivalent to the principle of **finite induction**, which we now state.

Theorem 5

Let $S \subseteq \in N$ such that

i. $1 \in S$, and
ii. Whenever $k \in S$, then $k + 1 \in S$
Then $S = N$

This theorem is further equivalent to:

Theorem 6

Let $S \subseteq N$ such that

i. $1 \in S$, and
ii. if $m \in S$ ∀ $m < k$, then $k \in S$.
then $S = N$

We will not prove the equivalence of the well-ordering principle and Theorems 5 and 6 in this course, since the proof is slightly technical.

Let us rewrite Theorem 5 and 6 in the forms that we will normally use.

Theorem 5': Let P(n) be a statement about a positive integer n such that

i. P(1) is true, and
ii. if P(k) is true for some $k \in N$, then P(k + 1) is true.
Then, P(n) is true for all $n \in N$.

Theorem 6': Let P(n) be a statement about a positive integer n such that

i. P(1) is true, and
ii. if P(m) is true for all positive integers $m < k$, then P(k) is true.
Then P(n) is true for all $n \in N$.

The equivalence statements given above are very useful for proving a lot of results in algebra. As we go along, we will often use the principle of induction in whichever form is convenient. Let us look at an example.

Example 8

Prove that $1^3 + 2^3 + \ldots\ldots\ldots\ldots + n^3 = \frac{n^2 (n+1)^2}{4}$ for every $n \in N$.

Solution

Let $S_n = 1^3 + \ldots\ldots\ldots\ldots + n^3$, and let P(n) be the statement that

$$S = \frac{n^2 (n+1)^2}{4}.$$

Since $S_1 = \frac{1^2 x 2^2}{4}$, P(1) is true.

Now, suppose P(n – 1) is true, i.e., $S_{n-1} = \frac{(n-1)^2 n^2}{4}$

Then $S_n = 1^3 + \ldots\ldots\ldots\ldots + (n-1)^3 + n^3$

$= S_{n-1} + n^3$

$= \frac{(n-1)^2 n^2}{4} + n^3$, since P(n – 1) is true.

$= \frac{n^2 [(n-1)^2 + 4n]}{4}$

$= \frac{n^2 (n+1)^2}{4}$

Thus, P(n) is true.

Therefore, by the principle of induction, P(n) is true for all n in **N**.

Now, use the principle of induction to prove the following property of numbers that you must have used time and again.

SELF ASSESSMENT EXERCISE 23

For a, b $\in$ R and n $\in$ N, prove that $(ab)^n = a^n b^n$.

Let us now look at some factorization properties of integers.

3.5.2 Divisibility in Z

One of the fundamental ideas of number theory is the divisibility of integers.

Definition

Let a, b $\in$ Z, a $\neq$ 0. Then, we say that a **divides b** if there exists an integer c such that b = ac. We write this as **a** | **b** and say that **a is a divisor** (or **factor**) **of b, or b is divisible by a, or b is a multiple of a**.

If a does not divide b we write $a \not| b$.

We give some properties of divisibility of integers in the following exercise. You can prove them very easily.

SELF ASSESSMENT EXERCISE 24

Let a, b, c be non-zero integers. Then

a. $a \mid 0, \pm 1 \mid a, \pm a \mid a$.
b. $a \mid b \Rightarrow ac \mid bc$.
c. $a \mid b$ and $b \mid c \Rightarrow a \mid c$.
d. $a \mid b$ and $b \mid a \Leftrightarrow a = \pm b$.
e. $c \mid a$ and $c \mid b \Rightarrow c \mid (ax + by)$ $\forall$ $x, y \in Z$.

We will now give a result, to prove which we use Theorem 5'.

Theorem 7

(Division Algorithm): Let $a, b \in Z$, $b > 0$. Then there exists unique integers q, r such that $a = qb + r$, where $0 \leq r < b$.

Proof

We will first prove that q and r exist. Then we will show that they are unique. To prove their existence, we will consider three different situations: $a = 0$, $a > 0$, $a < 0$.

Case 1 $(a = 0)$: Take $q = 0$, $r = 0$. Then $a = qb + r$.

Case 2 $(a > 0)$: Let P(n) be the statement that $n = qb + r$ for some $q, r \in Z$, $0 \leq r < b$.

Now let us see if P(1) is true.

If $b = 1$, we can take $q = 1$, $r = 0$, and thus, $1 = 1.1 + 0$.

If $b \neq 1$, then take $q = 0$, $r = 1$, i.e., $1 = 0.b + 1$.

So, P(1) is true.

Now suppose P(n - 1) is true, i.e., $(n - 1) = q_1 b + r_1$ for some $q_1, r_1 \in Z$, $0 \leq r_1 < b$. But then $r_1 \leq b - 1$, i.e., $r_1 + 1 \leq b$. Therefore,

$$n = \begin{cases} q_1 b + (r_1 + 1), \text{if } (r_1 + 1) < b \\ (q_1 + 1)b + 0, \text{if } r_1 + 1 = b \end{cases}$$

This shows that P (n) is true. Hence, by theorem 5', P(n) is true, for any $n \in N$. That is, for $a > 0$, $a = qb + r$, $q, r \in Z$, $0 \leq r < b$.

Case 3 ($a < 0$): Here $(-a) > 0$. Therefore, by Case 2, we can write

$(-a) = qb + r'$, $0 \leq r' < b$

$$\text{i.e., } a = \begin{cases} (-q)b, \text{if } r' = 0 \\ (-q-1)b + (b - r'), \text{if } 0 < r' < b \end{cases}$$

This proves the existence of the integers q, r with the required properties.

Now let q', r' be in **Z** such that $a = qb + r$ and $a = q'b + r'$, where $0 \leq r, r' < b$. Then $r - r' = b(q' - q)$. Thus, $b \mid (r - r')$. But $|r - r'| < b$. Hence, $r - r' = 0$, i.e., $r = r'$ and $q = q'$. So we have proved the uniqueness of q and r.

In the expression, $a = qb + r$, $0 \leq r < b$, r is called the **remainder** obtained when a is divided by b.

Let us go back to discussing factors.

Definition

Let $a, b \in \mathbf{Z}$. $c \in \mathbf{Z}$ is called a **common divisor** of a and b if $c \mid a$ and $c \mid b$.

For example, 2 is a common divisor of 2 and 4. From **Self Assessment Exercise 24**(a) you know that 1 and -1 are common divisors of a and b, for any $a, b \in Z$. Thus, a pair of integers does have more than one common divisor. This fact leads us to the following definition.

Definition

An integer d is said to be **a greatest common divisor** (**g.c.d** in short) of two non-zero integers a and b if

i. $d \mid a$ and $d \mid b$, and
ii. if $c \mid a$ and $c \mid b$, then $c \mid d$.

Note that if d and d' are two g.c.d s of a and b, then (ii) says that d | d' and d' | d. Thus, d = ± d' (**see Self-Assessment Exercise 24**). But then only one of them is positive. This **unique positive g.c.d. is denoted by (a, b).**

We will now show that (a, b) exists for any non-zero integers a and b. You will also see how useful the well-ordering principle is.

Theorem 8
Any two non-zero integers a and b have a g.c.d, and (a, b) = ma + nb, for some m, n $\in$ Z.

Proof

Let S = {xa + yb | x, y $\in$ Z, (xa + yb) > 0}.

Since $a^2 + b^2 > 0$, $a^2 + b^2 \in$ S, i.e., S $\neq$ f . But then, by the well-ordering principle, S has a least d $\in$ S. Therefore, d > 0. So by the division algorithm we can write
a = qd + r, 0 $\leq$ r < d. Thus,
r = a – qd = a – q(ma + nb) = (1 – qm)a + (-q)b.

Now, if r $\neq$ 0, then r $\in$ S, which contradicts the minimality of d in S. Thus, r = 0, i.e., a = qd, i.e., d | a. We can similarly show that d | b. Thus, d is a common divisor of a and b.

Now, let c be an integer such that c | a and c | b.

Then $a = a_1c$, $b = b_1c$ for some $a_1, b_1 \in$ Z.

But then $d = ma + nb = ma_1c + nb_1c$. Thus, c | d. So we have shown that d is a g.c.d. In fact, it is the unique positive g.c.d. (a, b).

For example, the g.c.d. is 2 and 10 is 2 = 1.2 + 0.10, and the g.c.d. of 2 and 3 is 1 = (-1) 2+ 1(3).

Pair of integers whose g.c.d. is 1 have a special name.

Definition

If (a, b) = 1, then the two integers a and b are said to be **relatively prime (or co prime)** to each other.

Using Theorem 8, we can say that **a and b are co prime to each other iff there exists m, a $\in$ Z such that 1 = ma + nb**.

The next theorem shows us a nice property of relatively prime numbers.

Theorem 9

If a, b $\in$ **Z**, such that (a, b) = 1 and b | ac, then b | c.

Proof

We know that $\exists$ m, n $\in$ Z such that 1 = ma + nb. Then c = c.1 = c(ma +nb) = mac + nbc.

Now, b | ac and b | bc. $\therefore$ b | (mac + nbc) (by **Self-Assessment Exercise 24(c)).** Thus, b | c.

Let us now discuss prime factorization.

Definition

A natural number p ($\neq$ 1) is called a **prime** if its only divisors are 1 and p. If a natural number n ($\neq$ 1) is not a prime, then it is called a **composite number.**

For example, 2 and 3 are prime numbers, while 4 is a composite number.

Note that, if p is a prime number and a $\in$ Z such that p $\not|$ a, then (p, a) = 1.

Try the following self assessment exercise now.

SELF ASSESSMENT EXERCISE 25

If p is a prime and p | ab, then show that p | a or p | b.

SELF ASSESSMENT EXERCISE 26

If p is a prime and p| a_1a_2 ..... a_n, then show that p\ai for some i = 1, ..., n.

Now consider the number 50. We can write 50 = 2 x 5 x 5 as a product of primes. In fact we can always express any natural number as a product of primes. This is what the unique prime factorization theorem says.

Theorem 10

(Unique Prime Factorisation): Every integer n > 1 can be written as n p_1, p_2 ..... p_n, where p_1, ..., p_n are prime numbers. This representation is unique, except for the order in which the prime factors occur.

Proof

We will first prove the existence of such a factorization. Let P (n) be the statement that n + 1 is a product of primes. P (1) is true, because 2 is a prime number itself.

Now let us assume that P (m) is true for all positive integers m < k. We want to show that P (k) is true. If (k + 1) is a prime, P (k) is true. If k + 1 is not a prime, then we can write $k + 1 = m_1m_2$, where $1 < m_1 < k + 1$ and $1 < m_2 < k + 1$. But then P (m_1 - 1) and P(m_2 – 1) are both true. Thus, $m_1 = p_1p_2.....p_r$, $m_2 = q_1 q_2$ ..... q_s, where p_1, p_2... p_r, q_1, q_2, ……, q_s are primes. Thus,
$k + 1 = p_1p_2 \ldots p_r q_1 q_2 \ldots q_s$, i.e., P(k) is true. Hence, by Theorem 6', P(n) is true for every $n \in N$.

Now let us show that the factorisation is unique.
Let $n = p_1p_2 \ldots p_t = q_1 q_2 \ldots q_s$, where

$p_1, p_2 \ldots p_t, q_1, q_2 \ldots q_s$, are primes. We will use induction on t.

If t = 1, then $p_1 = q_1 q_2 \ldots\ldots, q_s$. But p_1 is a prime. Thus, its only factors are 1 and itself. Thus, s = 1 and $p_1 = q_1$.

Now suppose t > 1 and the uniqueness holds for a product of t – 1 primes. Now $p_1 \mid q_1q_2 \ldots\ldots q_s$ and hence, by **Self-Assessment Exercise 26,** $p_1 \mid q_1$ for some i. By re-ordering $q_1, \ldots.., q_s$ we can assume that $p_1 \mid q_1$. But both p_1 and q_1 are primes. Therefore, $p_1 = q_1$ are primes.

Therefore, $p_1 = q_1$. But then $p_2 \ldots\ldots p_t = q_2 \ldots\ldots q_s$. So, by induction, t – 1 = s – 1 and $p_2, \ldots\ldots., p_t$ are the same as $q_2, \ldots\ldots q_s$ in some order.

Hence, we have proved the uniqueness of the factorisation.

The primes that occur in the factorisation of a number may be repeated in the factorisation 50 = 2 x 5 x 5. By collecting the same primes together we can give the following corollary to Theorem 10.

Corollary: Any natural number n can be uniquely written as $n = p_1^{m_1} p_2^{m_2} ..... p_r^{m_r}$, where for i = 1, 2, ..., r, each $m_i \in N$ and each p_i is a prime with $1 < p_1 < p_2 < \ldots < p_r$.

As an application of Theorem 10, we give the following important theorem, due to the ancient Greek mathematician Euclid.

Theorem 11

There are infinitely many primes.

Proof

Assume that the set **P** of prime numbers is finite, say
$P = \{p_1, p_2, \ldots, p_n\}$. Consider the natural number
$n = (p_1p_2, \ldots\ldots, p_n) + 1$

Now, suppose some $p_i \mid n$. Then $p_i \mid (n - p_1p_2 \ldots\ldots In.. p_n)$, i.e., $p_i \mid 1$, a contradiction. Therefore, no p_i divides n. But since $n > 1$, Theorem 10 says that n must have a prime factor. We reach a contradiction. Therefore, the set of primes must be infinite.
Try the following self assessment exercise now.

SELF ASSESSMENT EXERCISE 27

Prove that $\sqrt{p}$ is rational for any prime p.

(**Hint**: Suppose $\sqrt{p}$ is rational. Then $\sqrt{p} = \frac{a}{b}$, where $a, b \in Z$ and we can assume that $(a, b) = 1$. Now use the properties of prime numbers that we have just discussed.)

Let us now summarise what we have done inn this unit.

4.0 CONCLUSION

In this unit, we have placed emphasis on some properties of sets and subsets. We have also defined relations in general and equivalence relations in particular. The definitions of functions were also considered. The summary of what we have considered in this unit are given below, Please read carefully and master every bit of it in order for you to follow the subsequent units.

5.0 SUMMARY

In this unit we have covered the following points.

- Some properties of sets and subsets.
- The union, intersection, difference and complements of sets.
- The Cartesian product of sets.
- Relation in general and equivalence relations in particular.
- The definition of a function, a 1-1 function, an onto function and a bijective function.
- The composition of functions.
- The well-ordering principle, which states that every subset of **N** has a least element.
- The principle of finite induction, which states that : If P(n) is a statement about some $n \in N$ such that:

- P(1) is true, and
- if P(k) is true for some $k \in N$, then P(k + 1) is true,
  then P(n) is true for every $n \in N$.

- The principle of finite induction can also be stated as:
  If P(n) is a statement about some $n \in \mathbf{N}$ such that
  - P(1) is true, and

- if P(m) is true for every positive integer $m < k$, then P(k) is true,
  then P(n) is true for every $n \in N$,

Note that well-ordering principle is equivalent to the principle of finite induction.

- Properties pf divisibility in **Z**, like the division algorithm and unique prime factorisation.

ANSWER TO SELF ASSESSMENT EXERCISE 1

a) T b) F c) F d) T

ANSWER TO SELF ASSESSMENT EXERCISE 2

a. $x \in A \cup B \Rightarrow x \in A$ or $x \in B \Rightarrow x \in C$, since $A \subseteq C$ and $B \subseteq C$.

b. $x \in A \cup B \Leftrightarrow x \in A$ or $x \in B \Leftrightarrow x \in B$ or $x \in A \; x \Rightarrow \in B \cup A$. $\therefore A \cup B = B \cup A$.

c. $x \in A \cup \phi \Rightarrow x \in A$ or $x \in \phi \Rightarrow x \in A$, since ϕ has no element.
$\therefore A \cup \phi \subseteq A$.
Also, $A \in A \cup \phi$, since $x \in A \Rightarrow x \in A \cup \phi$.
$\therefore A = A \cup \phi$

ANSWER TO SELF ASSESSMENT EXERCISE 3

a. You can do it on the lines of Self Assessment Exercise 2(b).

b. $x \in A \cap B \Rightarrow x \in A$ and $x \in B \Rightarrow x \in A$, since $A \subseteq B$.
$\therefore A \cap B \subseteq A$.

Conversely, $x \in A \Rightarrow x \in A$ and $x \in B$ since $A \subseteq B$.
$\Rightarrow x \in A \cap B$.
$\therefore A \subseteq A \cap B$.
$\therefore A \cap B = A$.

c. Use the fact that $\phi \subseteq A$.

ANSWER TO SELF ASSESSMENT EXERCISE 4

a. $x \in (A \cup B) \cup C \Leftrightarrow x \in A \cup B$ or $x \in C$
$\Leftrightarrow x \in A$ or $x \in B$ or $x \in C$.
$\Leftrightarrow x \in A$ or $x \in B \cup C$
$\Leftrightarrow x \in A \cup (B \cup C)$
$\therefore (A \cup B) \cup C = A \cup (B \cup C)$

b. Try it on the same lines as (a).

c. $B \cap C \subseteq B \Rightarrow A \cup (B \cap C) \subseteq A \cup B$.

Similarly, $A \cup (B \cap C) \subseteq A \cup C$.
$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Conversely, $x \in (A \cup B) \cap (A \cup C)$
$\Rightarrow x \in A \cup B$ and $x \in A \cup C$
$\Rightarrow x \in A$ or $x \in B$ and $x \in A$ or $x \in C$.
$\Rightarrow x \in A$ or $x \in B \cap C$
$\Rightarrow x \in A \cup (B \cap C)$
$\therefore (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Thus, (c) is proved

d. Try it on the same lines as (c).

ANSWER TO SELF ASSESSMENT EXERCISE 5

a. T
b. F. For example, if A = [0, 1] and B = [0, 2], then $A \not\subset B$, $B \not\subset$ and $A \cap B = (0) \neq \phi$.
c. F, In fact, for any set A, $A \subset B$.
d. T.
e. T.

ANSWER TO SELF ASSESSMENT EXERCISE 6

a. $x \in A$ iff $x \notin A^c$.

b. Since A and A^c are subsets of X, $A \cup A^c \subseteq X$.
Conversely, if $x \in X$ and $x \notin A$, then $x \in A^c$.
$\therefore X \subseteq A \cup A^c$.
$\therefore X = A \cup A^c$.

c. $x \in A \Leftrightarrow x \notin A^c \Leftrightarrow x \in (A^c)^c$. $\therefore A = (A^c)^c$.

ANSWER TO SELF ASSESSMENT EXERCISE 7

A x B = {(2, 2), (2, 3), (5, 2), (5, 3)}
B x A = {(2, 2), (3, 2), (2, 5), (3, 5)}
A x A = {(2, 2), (2, 5), (5, 2), (5, 5)}

ANSWER TO SELF ASSESSMENT EXERCISE 8

The set of the first coordinates is A. $\therefore A = \{7, 2\}$.
The set of the second coordinates is B. $\therefore B = \{2, 3, 4\}$.

ANSWER TO SELF ASSESSMENT EXERCISE 9

$(x, y) \in (A \cup B) \times C \Leftrightarrow x \in A \cup B$ and $y \in C$
$\Leftrightarrow x \in A$ or $x \in B$ and $y \in C$
$\Leftrightarrow x \in A$ and $y \in C$ or $x \in B$ and $y \in C$
$\Leftrightarrow (x, y) \in A \times C$ or $(x, y) \in B \times C$
$\Leftrightarrow (x, y) \in (A \times C) \cup (B \times C)$.

You can similarly show that

$(A \cap B) \times C = (A \times C) \cap (B \times C)$.

ANSWER TO SELF ASSESSMENT EXERCISE 10

a. F b. T c. F

ANSWER TO SELF ASSESSMENT EXERCISE 11

Since 5 divides $(a - a) = 0$ $\forall$ $a \in$ **N, R** is reflexive.
If $5 \mid (a - b)$, then $5 \mid (b - a)$. $\therefore$, R is symmetric.
If $5 \mid (a - b)$, then $5 \mid (b - c)$, then $5 \mid \{(a - b) + (b - c)\}$, i.e.
$5 \mid (a - c)$. $\therefore$, R is transitive.

ANSWER TO SELF ASSESSMENT EXERCISE 12

2 R 2 is false
$(2, 4) \in R$, but $(4, 2) \notin R$.
$(2, 4) \in R$, $(4, 16) \in R$, but $(2, 16) \notin R$.

ANSWER TO SELF ASSESSMENT EXERCISE 13

$|a| = |a|$ $\forall$ $a \in Z$ $\therefore$, R is reflexive.
$|a| = |b| \Rightarrow |b| = |a|$ $\therefore$, R is symmetric.
$|a| = |b|$ and $|b| = |c| \Rightarrow |a| = |c|$. $\therefore$, R is transitive.

$\therefore$, R is an equivalence relation.

$[0] = \{a \in Z \mid aR0\} = \{a \in Z \mid |a| = 0\} = \{0\}$.
$[1] = \{1, -1\}$.

ANSWER TO SELF ASSESSMENT EXERCISE 14

For $n, m \in N$, $f(n) = f(m) \Rightarrow n + 5 = m + 5 \Rightarrow n = m$.
$\therefore$, f is $1 - 1$.
Since $1 \notin f(N)$, $f(N) \neq N$. $\therefore$, f is not surjective.

ANSWER TO SELF ASSESSMENT EXERCISE 15

f is $1 - 1$ (as in **Self Assessment Exercise 14**).
For any $z \in Z$, $f(z - 5) = z$. $\therefore$, f is surjective, and hence, bijective.

ANSWER TO SELF ASSESSMENT EXERCISE 16

$f(x) = c \ \forall \ x \in X$.

Suppose X has at least two elements, say x and y. Then $f(x) = c = f(y)$, but $x \neq y$. That is, f is not $1 - 1$. Therefore, if f is $1 - 1$, then X consists of only one element.

Since $f(X) = \{c\}$, f is surjective.

ANSWER TO SELF ASSESSMENT EXERCISE 17

$x \in X \Rightarrow f(x) \in f(X) \Rightarrow x \in f^{-1}(f(X))$. $\therefore$, $X \subseteq f^{-1} f(X))$.

ANSWER TO SELF ASSESSMENT EXERCISE 18

a. $x \in f^{-1}(S) \Leftrightarrow f(x) \in S \cup T$.
$\Leftrightarrow f(x) \in S$ or $f(x) \in T$
$\Leftrightarrow x \in f^{-1}(S)$ or $x \in f^{-1}(T)$
$\therefore f^{-1}(S) \subseteq f^{-1}(T)$.

b. $x \in f^{-1}(S \cup T) \Leftrightarrow f(x) \in S \cup T$
$\Leftrightarrow f(x) \in S$ or $f(x) \in T$
$\Leftrightarrow x \in f^{-1}(S)$ or $x \in f^{-1}(T)$
$\Leftrightarrow x \in f^{-1}(S) \cup f^{-1}(T)$

c.) Do it on the lines of (b).

ANSWER TO SELF ASSESSMENT EXERCISE 19

$f \circ g$ and $g \circ f$ are functions from **R** to **R** in all cases.

a. $f \circ g\ (x) = f(x + 5) = 5(x + 5)$ $\forall\ x \in R$
$g \circ f\ (x) = g(5x) = 5x + 5$ $\forall\ x \in R$.

b. $f \circ g\ (x) = g \circ f\ (x) = x$ $\forall\ x \in R$.

c. $f \circ g\ (x) = x^2 = g \circ f\ (x)$ $\forall\ x \in R$.

ANSWER TO SELF ASSESSMENT EXERCISE 20

Show that $I_A \circ g(b) = g(b)$ and $g \circ I_B(b) = g(b)$ $\forall\ b \in B$.

ANSWER TO SELF ASSESSMENT EXERCISE 21

$g : R \rightarrow R : g(x) = 3x$.

ANSWER TO SELF ASSESSMENT EXERCISE 22

a. f is not 1 – 1, since f(1) = f(-1).
$\therefore$, f^{-1} doesn't exist.

b. f is not surjective, since $f\mathbf{(R)} \neq \mathbf{R}$.
$\therefore$, f^{-1} doesn't exist.

c. f is bijective, $\therefore$, f^{-1} exists.
$f^{-1}: \mathbf{R} \rightarrow \mathbf{R} : f^{-1}(x) = \frac{x - 7}{11}$.

ANSWER TO SELF ASSESSMENT EXERCISE 23

Let P(n) be the statement that $(ab)^n = a^n b^n$.
P(1) is true. Assume that P(n – 1) is true. Then
$(ab)^n = (ab)^{n-1}\ (ab) = (a^{n-1}\ b^{n-1})ab$, since P(n -1) is true.
$= a^{n-1}\ (b^{n-1}a)b$
$= a^{n-1}\ (ab^{n-1})b$
$= a^n b^n$.
$\therefore$, P(n) is true
$\therefore$, P(n) is true $\forall\ n \in N$.

ANSWER TO SELF ASSESSMENT EXERCISE 24

a. Since $a.0 = 0$, $a \mid 0$.
$(\pm 1)(\pm a) = a$. $\therefore \pm 1 \mid a$ and $\pm a \mid a$.

b. $a \mid b \Rightarrow b = ad$, for some $d \in Z$
$\Rightarrow bc = (ac)d$,
$\Rightarrow ac \mid bc$

c. $b = ad$, $c = be$, for some $d, e \in \mathbf{Z}$.
$\therefore, c = ade$. $\therefore, a \mid c$.

d. $a \mid b \Rightarrow b = ad$, for some $d \in Z$
$b \mid a \Rightarrow a = be$, for some $e \in Z$.
$\therefore, a = ade \Rightarrow de = 1$, since $a \neq 0$.
$\therefore, e = \pm 1$. $\therefore, a = \pm b$.

e. $c \mid a$ and $c \mid b \Rightarrow a = cd$, $b = ce$ for some $d, e \in Z$.
$\therefore$, for any $x, y \in Z$, $ax + by = c(dx + ey)$.
$\therefore$, $c \mid (ax + by)$.

ANSWER TO SELF ASSESSMENT EXERCISE 25

Suppose $p \nmid a$. Then $(p, a) = 1$. $\therefore$, by Theorem 9, $p \mid b$.

ANSWER TO SELF ASSESSMENT EXERCISE 26

Let P(n) be the statement that $p \mid a_1 a_2 \ldots\ldots\ldots a_n$
$\Rightarrow p \mid a_i$ for some $i = 1, 2, \ldots\ldots\ldots, n$.
P(1) is true.

Suppose P (m – 1) is true.

Now, let $p \mid a_1 a_2 \ldots\ldots\ldots a_m$. Then $p \mid (a_1 \ldots\ldots\ldots A_{m-1})a_m$.
By Self Assessment Exercise 25, $p \mid (a_1 a_2 \ldots\ldots\ldots a_{m-1})$ or $p \mid a_m$.
$\therefore, p \mid a_i$ for some $i = 1, \ldots\ldots, m$ (since P(m – 1) is true).
$\therefore$, P(m) is true.
$\therefore$, P(n) is true $\forall\, n \in N$.

ANSWER TO SELF ASSESSMENT EXERCISE 27

$\sqrt{p} = \frac{a}{b} \Rightarrow a^2 = pb^2 \Rightarrow p \mid a^2 \Rightarrow p \mid a$, since p is a prime.

Let a = pc. Then $a^2 = pb^2 \Rightarrow p^2c^2 = pb^2 \Rightarrow pc^2 = b^2$
$\Rightarrow p \mid b^2 \Rightarrow p \mid b.$
$\therefore$, $p \mid (a, b) = 1$, a contradiction.
$\therefore$, $\sqrt{p}$ is irrational.

7.0 REFERENCES/FURTHER READINGS

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

UNIT 2 GROUPS

CONTENTS

1.0 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.

2.0 OBJECTIVES

At the end of 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.

3.0 MAIN CONTENT

3.1 Binary Operations

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

Definition

Let S be an 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 Δ to denote binary operations.

Let us look at some examples.

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

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

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

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 I 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) $\forall$ 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 **N** $\subseteq$ **R**, because 1 $\in$ N, 2 $\in$ N but 1 – 2 $\notin$ 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 self assessment exercise now.

SELF ASSESSMENT EXERCISE 1

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

1. $x \oplus y = x + y - 5$
2. $x * y = 2(x + y)$
3. $x \Delta y = \frac{x - y}{2}$
   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 = ba + ca $\forall$ a, b, c $\in$ **R**. This fact says that multiplication distributes over addition in R. In general, we have the following definition.

Definition

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

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 Self Assessment Exercise 4 of Unit 1. What does it say? It says that the intersection of sets distributes over the union distributes over the intersection of sets.

Let us now look deeper at some binary operations. You know that, for any $a \in \mathbf{R}$, $a + 0 = a$, $0 + a = a$ 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 a and e' are both identity elements for $*$.

Then $e = e * e'$, since e' is an identity element.
$e = e'$, 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
$a = a * c = a * (s * b)$
$= (a * s) * b$, since $*$ is associative.
$= e * b = b$.

That is, $a = b$.

Hence, the inverse of s is unique.

This uniqueness theorem allows us to say **th**e 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 or are associative operations on $\wp(S)$. Self Assessment Exercise of Unit 1 also says that both operations are associative. You can see that the empty set ϕ and the set are S 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 $A \neq \phi$, 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 self assessment exercise now.

SELF ASSESSMENT EXERCISE 2

1. Obtain the identity element, if it exists, for the operations given in Self Assessment Exercise 1.
2. For $x \in \mathbf{R}$, obtain x^{-1} (if it exists) for each of the operations given in Self Assessment Exercise 1.

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 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	(-1).1 =0
1	1.(-1) =-1	1.0 =0	1.1 =1

Fig. 1 : Arthur Cayley

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.

SELF ASSESSMENT EXERCISE 3

Draw the operation table for the set $\wp(S)$ (ref. Example 2), where $S = \{0, 1\}$ and the operation in $\cap$.

Now consider the following definition.

Definition

Let $*$ be a binary operation on a non-empty set S and let $a_1, .., a_{k+1} \in S$.

We define the product $a_1 * \ldots\ldots * a_{k+1}$ as follows:

If $k = 1$, $a_1 * a_2$ is a well defined element in S.
If $a_1 * \ldots\ldots * a_k$ is defined, then
$a_1 * \ldots\ldots * a_{k+1} = (a_1 * \ldots\ldots * a_k) * a_{k+1}$
We use this definition in the following result.

Theorem 2

Let $a_1, \ldots\ldots, a_{m+n}$ be elements in a set S with an associative binary operation $*$. Then
$(a_1 * \ldots\ldots * a_m) * (a_{m+1} * \ldots\ldots * a_{m+n}) = a_1 * \ldots\ldots * a_{m+n}$.

Proof

We use induction on n. That is, we will show that the statement is true for $n = 1$.

Then, assuming that is true for $n - 1$, we will prove it for n.

If $n = 1$, our definition above gives us

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

Now, assume that

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

Then

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

3.2 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

G1) $*$ is associative,
G2) G contains an identity element e for $*$, and
G3) every element in G has an inverse in G with respect to $*$.

We will now give some examples of groups.

Example 3

Show that $(\mathbf{Z}, +)$ is a group, but $(\mathbf{Z},)$ is not.

Solution

$+$ is an associative binary operation on $\mathbf{Z}$. the identity element with respect to $+$ is 0, and the inverse of any $n \in \mathbf{Z}$ is $\mathbf{(-n)}$. Thus, $(\mathbf{Z}, +)$ 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? No. For instance, 0 and 2 have no inverses with respect to **'.'**. Therefore, (Z,.) is not a group.

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

The following self assessment exercise gives you two more examples of groups.

SELF ASSESSMENT EXERCISE 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.

G1') $*$ is associative.
G2') $\exists e \in G$ such that $a * e = a$ **∀** $a \in G$.
G3') 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

G1") $*$ is associative.
G2") $\exists\ e \in G$ such that $e * a = a$ **∀** $a \in G$.
G3") 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 $e * a = a$ " $a \in G$. 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 to Theorem 3

G1 holds since G1 and G1' are the same axioms. We will next prove that G3 is true. Let $a \in G$ 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 $(G, \times)$ 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,·) satisfies G3'. Therefore, (G,·) 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 Self Assessment Exercise 4 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**.


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

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.

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

Now let us look at an example of a non-commutative (or non-abelian) group. Before doing this example recalls that an m by 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,

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

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, $P \in G \Rightarrow A.P \in G$.

Now,

det(A. P) = det A. det P $\neq 0$, since det A $\neq 0$, det P $\neq 0$.

Hence, A.P $\in$ G for all A, P in G.

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 matrix

B = $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ is such that det B = $\frac{1}{ad - bc} \neq 0$ 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 act set of all 2 x 2 matrices over **R** with non-zero determinant forms a group under multiplication. Since

$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$ 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 $\mathbf{GL_2(R)}$, 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 translation of R^2,

$T = \{f_{a,b} : R^2 \to R^2 \mid f_{a,b}(x,y) = (x + a, y + b)$ *for some* fixed $a,b \in R\}$

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

Solution

Let us see if $\circ$ is a binary operation on T.

Now $f_{a,b} \circ f_{c,b}(x, y) = f_{a,b}(x + c, y + d) = (x + c + a, y + d + b)$
$= f_{a+c, b+d}(x, y)$ for any $(x, y) \in \mathbf{R}^2$.
$\therefore f_{a,b} \circ f_{c,d} = f_{a+c, b+d} \in T$.
Thus, $\circ$ 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, $f_{a,b} \circ f_{-a,-b}$ is the inverse of $f_{0,0} \forall f_{a,b} \in T$.

Thus, $(T, \circ)$ satisfies G1', G2' and G3', and hence is a group.

Note that $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} \forall f_{a,b} \circ f_{c,d} \in T$. Therefore, $(T, \circ)$ is abelian.

Try the following self assessment exercises now.

SELF ASSESSMENT EXERCISE 5

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

1. $(\mathbf{Q}^*, .)$ is an abelian group.
2. $(\mathbf{R}^*, .)$ is a finite abelian group.
3. $(\mathbf{Z}^*, .)$ is a group.
4. $(\mathbf{Q}^*, .)$, $(\mathbf{R}^*, .)$ and $(\mathbf{Z}^*, .)$ are semigroups.

SELF ASSESSMENT EXERCISE 6

Show that $(G, *)$ is a non-abelian group,
where $G = \{(a,b) | a, b \in R, a \neq 0\}$ 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.

3.3 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$\in$ 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 $a, b \in G$.

Proof

a. By the definition of inverse,
$(a^{-1})^{-1} (a^{-1}) = e = (a^{-1}) (a^{-1})^{-1}$.

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

b. For a, b$\in$G, ab$\in$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 is abelian.

You know that whenever ba = ca or ab = ac for a, b, c in $\mathbf{R}^*$,
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 Self Assessment 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 can mean we are performing the operation $*$.

SELF ASSESSMENT EXERCISE 7

Prove (b) of Theorem 5.

Now use Theorem 5 to solve the following self assessment exercise.

SELF ASSESSMENT EXERCISE 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 solutions 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 get $x_1 = x_2$. 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

Consider $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ in GL_2 (**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** Δ, given by
$A \Delta B = (A \setminus B) \cup (B \setminus A)$ $\forall$ A, B $\in \wp(S)$.

Show that $(\wp(S), \Delta)$ is an abelian group. What is the unique solution for the equation $Y \Delta A = B$?

Solution

Δ is an associative binary operation. This can be seen by using the fact 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. Δ 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, $(\wp(S), \Delta)$ is an abelian group.

For A, B in $(\wp(S), \Delta)$ 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 self assessment exercise now.

SELF ASSESSMENT EXERCISE 9

Consider **Z** with subtraction as a binary operation. Is (**Z**, -) a group? Can you obtain a solution for $a - x = b$ ∀$a, b \in \mathbf{Z}$?

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

iii $a^{-a} = (a^{-1})^n$, 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 for the binary operation is addition, a^n becomes na. For example, for any $a \in Z$,

na = 0 if a = 0,
na = a + a + … + a (n times) if n > 0;
na = (-a) + (-a) + … + (-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 Self Assessment Exercise 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

$e = e^n = (aa^{-1})^n$
$= (aa^{-1})\ (aa^{-1})$ ..... (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 $n > 0$
$= a^{-n}$
Also, $(a^{-1})^n = (a^{-1})^{-(-n)}$
$= [(a^{-1})^{-1}]^{-n}$, y 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 $a^m.a^{n-1} = a$
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, $a^{-n}.a^{-m} = a^{-(n+m)} = a^{-(m+n)}$. 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 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 Case 3 and 4. Hence, $a^{m+n} = a^m.a^n$ for all $a \in G$ and $m, n \in Z$.

To finish the proof of this theorem try self assessment exercise 10.

SELF ASSESSMENT EXERCISE 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.

3.4 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.

3.4.1 Integers Modulo n

Consider the set of integers, Z, and $n \in Z$ 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 | (4 -1).

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

≡ is an equivalent relation (see Sec. 3.3 of Unit 1), 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, $0 \leq r <$, iff n | (r – m), i.e., iff r – m = kn, for some $k \in Z$.

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

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

Now, if $m \geq a$, then the division algorithm says that m = nq + r for some q, $r \in Z$, $0 \leq r < q$. That is, $m \equiv r \pmod n$, for some r 0, …., n – 1.

Therefore, all the congruence classes modulo n are $\bar{0}, \bar{1}, \ldots\ldots, \overline{n-1}$.

Let $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots, \overline{n-1}\}$. 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 Z_n, then $\overline{a+b} = \overline{c+d}$.

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

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 $\mathbf{Z}_n$.

For example, $\bar{2} + \bar{2} = \bar{0}$ in Z_4 since $2 + 2 = 4 \equiv 0 \pmod 4$.

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

SELF ASSESSMENT EXERCISE 11

Fill up the following operation table for + on Z_4.

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

i. $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ ∀ $\bar{a}, \bar{b} \in Z_n$, i.e., addition is commutative in Z_n.

ii. $\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + (\overline{b+c}) = \overline{a+(b+c)}$
$= \overline{(a+b)+c} = (\overline{a+b}) + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$ ∀ $\bar{a}, \bar{b}, \bar{c} \in Z_n$,
i.e., addition is associative in $\mathbf{Z}_n$.

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

iv. For $\in Z_n, \exists\ \overline{n-a} \in Z_n$ such that $\bar{a} + \overline{n-a} = \bar{n} = \bar{0} = \overline{n-a} + \bar{a}$.

Thus, every element $\bar{a}$ in Z_n has an inverse with respect to addition.
The properties (i) to (iv) show that $(Z_n, +)$ is an abelian group.

Try the following self assessment exercise now.

SELF ASSESSMENT EXERCISE 12

Describe the partition of Z determined by the relation ‘congruence modulo 5’.

Actually we can also define multiplication on $\mathbf{Z}_n$ by $\bar{a}.\bar{b} = \overline{ab}$. Then, $\bar{a}\,\bar{b} = \bar{b}\,\bar{a}$ $\forall$ $\bar{a}$, $\bar{b} \in \mathbf{Z}_n$. Also $(\bar{a}\,\bar{b})\bar{c} = \bar{a}(\bar{b}\,\bar{c})$ $\forall$ $\bar{a}$, $\bar{b}$, $\bar{c} \in Z_n$. 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 $(\mathbf{Z}_n,.)$ 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, $(Z_n^*, .)$ Is this a group? For example $Z_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is not a group because . is not even a binary operation on Z_4^*, since $\bar{2}.\bar{2} = \bar{0} \notin Z_4^*$. But $(Z_p^*,.)$. is an abelian group for any prime p.

SELF ASSESSMENT EXERCISE 13

Show that $(Z_5^*,.)$ is an abelian group.

(**Hint**: Draw the operation table.)

Let us now discuss the symmetric group.

3.4.2 The Symmetric Group

We will now discuss the symmetric group briefly. In MTH 312 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 $F(X)$ of all functions from X to X. This binary operation is associative. I_X, the identity map, is the identity in $F(X)$.

Now consider the subset S(X) of $F(X)$ given by

$S(X) = \{f \in F(X) \mid f \text{ is bijective}\}$.
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 $f^{-1} \in S(X)$.

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

Let us check that $(S(X), _o)$ is a group

i. $_o$ is associative since $(f\ _o\ g)\ _o\ h = f(g\ _o\ h)$ $\forall$ f, g, h $\in$S(X).
ii. I_x is the identity element because $f\ _o\ I_x = I_x\ _o\ f$ $\forall$ $f \in S(X)$.
iii. f^{-1} is the inverse of f, for any $f \in S(X)$.

Thus, $(S(X), {}_o)$ 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 Sn 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}\{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 x 2 x….x_n) n 1 ways, i.e., S_n contains an! Elements.

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

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

For example, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ represents the function f:

{1, 2, 3, 4} $\rightarrow$ {1, 2, 3, 4}: f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1. the elements in the top row can be laced 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.

SELF ASSESSMENT EXERCISE 14

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

Now, while solving **Self Assessment Exercise** 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 $x_1 \ldots\ldots, x_r$ in X = { 1, 2, ….., n} such that $f(x_i) = x_i + 1$ for $1 \leq i \leq r - 1$, (fx_r) and f(t) = t for t x_i, …..x_r. In this case f is written as $(x_i \ldots x_r)$,
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 fixes 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.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$ 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 S_3,

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

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

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

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

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.

SELF ASSESSMENT EXERCISE 15

Calculate (1 3) ∘ (1 2) in S_3.

SELF ASSESSMENT EXERCISE 16

Write the inverses of the following in S3:

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. j

3.4.3 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 x 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
$(x_1, y_1) . (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 - x_2 y_1)$
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 $y_1 = y_2$.

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

Moreover,

i. (0,)) is the additive identity.
ii. For (x, y) in **C,** (-x, -y) s its additive inverse.
iii. (1, 0) is the multiplicative identity.
iv. If (x, y) (0, 0) in **C**, then either $x^2 > 0$ or $y^2 > 0$.

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

(x, y). $\dfrac{x}{x^2 + y^2}, \dfrac{-y}{x^2 + y^2}$

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

$$= (1, 0)$$

Thus, (**C**, +) is a group and (**C***,.) is a group, (as usual, **C*** denotes the set of non-zero complex numbers).

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

4.0 CONCLUSION

The study of groups in algebra is a fundamental requirement for any students who want to major in pure mathematics. You are required to pay attention to all the details in this unit.

5.0 SUMMARY

In this unit we have

1. discussed various types of binary operations.
2. defined and give 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 fact about complex numbers.

ANSWER TO SELF ASSESSMENT EXERCISE 1

1. a. $x \oplus y = y \oplus x, \forall x, y \in Z$
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. Δ is not commutative, associative or closed on **N**.

ANSWER TO SELF ASSESSMENT EXERCISE 2

a. The identity element with respect to $\oplus$ is 5.
Suppose e is the identity element for *

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

ANSWER TO SELF ASSESSMENT EXERCISE 3

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

So, the table is

N	ϕ	{0}	{1}	S
ϕ	ϕ	ϕ	ϕ	{1}
{0}	ϕ	{0}	ϕ	{0}
{1}	ϕ	ϕ	{1}	{1}
S	ϕ	{0}	{1}	S

ANSWER TO SELF ASSESSMENT EXERCISE 4

Check that both of then satisfy G1, G2 and G3

ANSWER TO SELF ASSESSMENT EXERCISE 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.

ANSWER TO SELF ASSESSMENT EXERCISE 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.

ANSWER TO SELF ASSESSMENT EXERCISE 7

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

ANSWER TO SELF ASSESSMENT EXERCISE 8

Let $x \in G$. Then $gx = g = ge$. So, by Theorem 5, $x = e$.

$\therefore G = \{e\}$,

ANSWER TO SELF ASSESSMENT EXERCISE 9

(Z,-) is not a group since G1 is not satisfied.

For any $a, b \in \mathbf{Z}$, $a - (a - b) = b$. So, $a - x$ has a solution for any $a, b \in \mathbf{Z}$.

ANSWER TO SELF ASSESSMENT EXERCISE 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 , 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, $(a^m)^{(n-1)\cdot} = a^{m(n-1)}$.

Then, $(a^m)^n = (a^m)^{n-1} + 1 = (a^m)^{(n-1)\cdot} = a^m$, by (b)
$= a^{m(n-1)\cdot} a^m$
$= a^{m(n+1+1)}$, by (b)
$= a^{mn}$.

So, (c) is true $\forall$ $n > m \in \mathbf{Z}$.

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 ∈ Z, (c) holds.

ANSWER TO SELF ASSESSMENT EXERCISE 11

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

ANSWER TO SELF ASSESSMENT EXERCISE 12

Z is the disjoint union of the following 5 equivalence classes.

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

ANSWER TO SELF ASSESSMENT EXERCISE 13

The operation table for on $\mathbf{Z}_5$ is

·	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

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

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

ANSWER TO SELF ASSESSMENT EXERCISE 14

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

ANSWER TO SELF ASSESSMENT EXERCISE 15

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

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

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

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

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

ANSWER TO SELF ASSESSMENT EXERCISE 16

a. Let $f = (1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. $\therefore f^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$,
just interchanging the rows.
$\therefore\ f^{-1} = (1\ 2)$.

b. $(1\ 3\ 2)^{-1} = (2\ 3\ 1)$.
Now, $(1\ 2)\ _o\ (1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Its inverse is $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = (1\ 3)$.
On other hand,
$(1\ 2)^{-1}\ _o\ (1\ 3\ 2)^{-1}\ _o = (1\ 2)\ _o\ (1\ 2\ 3) = (2\ 3) \neq (1\ 3)$.

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 $(x, y) \in \mathbf{C}$ is $x + iy$, where $i = \sqrt{-i.}$.

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

$x + iy = (x, 0) + (0, 1)\ (y, 0)$
$= (x, 0), + (0, y),$
$= (x, y),$
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 $\mathbf{R}^2$**.**

You can see that

$(x + iy_1) + (x_2 + iy_2) = (x_1, y_1) + (x_2, y_2)$
$= (x_1 + x_2, x_2 + y_2)$
$= (x_1 + x_2) + i(y_1 + y_2)$, and

$(x_1 + iy_1)(x_2 + iy_2) = (x_1, y_1) + (x_2, y_2)$
$= (x_1x_2 - y_1y_2, x_1y_2)$
$= (x_1x_2) - y_1y_2) + i(x_1y_2 + x_2y_1).)$, and

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 $z_1, z_2 \in \mathbf{C}$. This is because

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

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

Let us now see another way of representing complex numbers.

Geometric Representation of Complex Numbers Y

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 y number z and is denoted by | z |. Note that $\sqrt{x^2 + y^2}$ = 0 iff x = 0 **and** y = 0.

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 $0 + 2n\pi$ is also an argument of z for all $n \in \mathbf{Z}$,. 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 cosθ, y = r sinθ that is, z = (rcosθ, rsinθ) = **r(cosθ + i sinθ)** = re^{10}.

This is called the **polar form** of the complex number (x + iy).

Now, if $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$, then
$z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$.

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 (≠ 0), then (-θ) is an argument of z^-
We end by stating one of the important theorems that deals with complex numbers.

De Moivre's Theorem: If z = r(cosθ + i sinθ) and n ∈ N, then $z^n = 1^n$ (cos nθ + i sin nθ).

7.0 REFERENCES/FURTHER READINGS

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

UNIT 3 SUBGROUPS

CONTENTS

1.0 INTRODUCTION

You have studied the algebraic structures of integers, rational numbers, real numbers and, finally, complex numbers. You have noticed that, not only is $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$. but the operations of addition and multiplication coincide in these sets.

In this unit you will study more examples of subsets of groups which are groups in their own right. Such structures are rightfully named subgroups. In Sec. 3.3 we will discuss some of their properties also.

In Sec. 3.4 we will see some cases in which we obtain a group from a few elements of the group. In particular, we will study cases of groups that can be built up by a single element of the group.

Do study this unit carefully because it consists of basic concepts which will be used again and again in the rest of the course.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- define subgroups and check if a subset of a given group is a subgroup or not
- check if the intersection. union and product of two subgroups is ;I subgroup
- describe the structure and properties of cyclic groups.

3.0 MAIN CONTENT

3.1 Subgroups

You may have already noted that the groups (**Z**,+), (**Q**,+) and (**R**,+) are contained in the bigger group (**C**,+) of complex numbers, not just as subsets but as groups. All these are examples of subgroups, as you will see.

Definition

Let (G,*) be a group. A non-empty subset H of G is called a subgroup of G if

i. $a * b \in H \forall a. b \in H$. i.e.. * is a binary operation on H.
ii. (H,*) is itself a group.

So, by definition, (**Z**,+) is a subgroup of (**Q**,+), (**R**,+) and (**C**,+).

Now, if (H, *) is a subgroup of (G,*), can the identity element in (H,*) be different from the identify element in (G,*)? Let us see. If h is the identity of (H,*), then for any $a \in H$.

$b * a = a * h = a$. However, $a \in H \subseteq G$. Thus. $a * e = e * a = a$. where e is the identity in G.

Therefore $h * a = e * a$.
By right cancellation in (G,*). We get $h = e$.
Thus, whenever (H, *) is a subgroup of (G,*). $e \in H$.

Now you may like to try the following exercise.

SELF ASSESSMENT EXERCISE 1

If (H, *) is a subgroup of (G,*), does $a^{-1} \in H$ for every $a \in H$.,

Self Assessment Exercise 1 and the discussion before it allows us to make the following remark.

Remark 1

(H,*) is a subgroup of (G, *) if and only if

i. $e \in H$.
ii. $a, b \in H \Rightarrow a * b \in H$
iii. $a \in H \Rightarrow a^{-1} \in H$.

We would also like to make an important remark about notation here.

Remark 2

If (H,*) is a subgroup of (G,*), **we shall just say that H is a subgroup of G**, provided that there is no confusion about the binary operations. We will also denote this fact by $H \leq G$.

Now we discuss an important necessary and sufficient condition for a subset to be a subgroup.

Theorem 1

Let **H be a non-empty** subset of a group G. Then H is a subgroup of G iff
$a, b \in H, ab^{-1} \in H$.

Proof

Firstly, let us assume that $H \leq G$. Then, by Remark 1, $a, b \in H \Rightarrow a, b^{-1} \in H$.

Conversely, since $H \neq \phi \ \exists \ a \in H$. But then, $aa^{-1} = e \in H$.

Again, for any a e H, $ea^{-1} = a^{-1} \in H$.

Finally, if: $a, b \in H$, then $a, b^{-1} \in H$. Thus, $a (b^{-1})^{-1} = ab \in H$, i.e.,
H is closed under the binary operation of the group.

Therefore by Remark 1, H is a group.

Let us look at some examples of subgroups now. While going through these you may realise the fact that a **subgroup of an abelian group is abelian.**

Example 1

Consider the group (C*,.). Show that

$S = \{z \in C \mid |z| = 1\}$ is a subgroup of **C***

Solution

$S \neq \phi$, since $1 \in S$. Also, for any $z_1, z_2 \in S$,

$|z_1 z_2^{-1}| = |z1| \ |z_2^{-1}| = |z_1| \ \frac{1}{|z_2|} = 1.$

Hence, $z_1 z_2^{-1} \in S$. Therefore, by Theorem 1, $S \leq C^*$.

Example 2

Consider $G = \mathbf{M_{2x3}}(\mathbf{C})$, the set of all 2 x 3 matrices over **C**. Check that
(G,+) is an abelian group. Show that

$S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \middle| \; a, \; b, \; c \in C \right\}$ is a subgroup of G.

Solution

We define addition on G by

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} p & q & r \\ s & t & u \end{bmatrix} = \begin{bmatrix} a + p & b + q & c + r \\ d + s & e + t & f + u \end{bmatrix}.$$

You can see that + is binary operation on G. O = is the additive identity and

$\begin{bmatrix} -a & -b & -c \\ -d & -e & -f \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \in$ G.

Since, a + b = b + a. $\forall$ a, b $\in$ **C**, + is also abelian.

Therefore, (G,+) is an abelian group.

Now, since O $\in$ S, S $\neq \phi$. Also, for

$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in$ S, we see that

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} - \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \in S.$$

H ≤ (G, +) ⇔ H ≠ ϕ and a – b ∈ H.

$\therefore$ S ≤ G.

Example 3

Consider the set of all invertible 3 x 3 matrices over R, GL_3 (**R**). That is,
A $\in$ GL_3(**R**) iff det (A) $\neq$ 0. Show that SL_3 (**R**) = (A E GL_3(**R**) det(A) 1} is a subgroup of (GL_3(**R**),.).

Solution

The 3x3 identity matrix is in SL_3(**R**). Therefore, SL3(**R**) $\neq \phi$.

Now, for A, B $\in$ SL_3(**R**).

det (AB^{-1}) = det (A) det(B^{-1}) = det (A) $\frac{1}{\det(B)}$ = 1, since det (A) =1and det (B) =l.

$\therefore AB^{-1} \in SL_3(\mathbf{R})$
:. SL_3(**R**) ≤ GL_3(**R**).

Try the following exercise now.

SELF ASSESSMENT EXERCISE 2

Show that for any group G, {e} arid G are subgroups of G.
({e} is called the **trivial subgroup**.)

The next example is very important, and you may use it quite often.

Example 4

Any non-trivial subgroup of (**Z**, +) is of the form m**Z**; where $m \in N$ and
$mZ = \{ mt \mid t \in Z\} = \{ 0, \pm m, \pm 2m, \pm 3m, \}$.

Solution

We will first show that m**Z** is a subgroup of Z. Then we will show that if H is a subgroup of Z, $H \neq \{0\}$, then H = mZ, for some $m \in N$.

Now, $0 \in m\mathbf{Z}$. Therefore, $m\mathbf{Z} \neq \phi$. Also, for mr, ms $\in m\mathbf{Z}$, $mr-ms = m(r-s) \in m\mathbf{Z}$.

Therefore, m**Z** is a subgroup of **Z**.

Note that m is the **least positive integer in m**Z.

Now, let $H \neq \{0\}$ be a subgroup of Z and $S=\{i \mid i> 0, i \in \mathbf{H}\}$.

Since $H \neq \{0\}$, there is a non-zero integer k in **H**. If k > 0, then $k \in S$. If k < 0, then $(-k) \in S$, since $(-k) \in H$ and (-k) > 0.

Hence, $S \neq \phi$.

Clearly, $S \subseteq N$. Thus, by the well-ordering principle (Sec. 16.1) S has a least element, say s. That is, s is the least positive integer that belongs to **H**.

Now $s\mathbf{Z} \subseteq H$. Why? Well, consider any element $st \in s\mathbf{Z}$.

If t = 0, then $st = 0 \in H$.
If t > 0, then st = s +s +….. + s (t times) $\in$ H.
If t < 0, then st = (-s) + (-s) + …...+ (-s) (-t times) $\in$ H.

Therefore, $st \in H \forall t \in Z$. That is, $sZ \subseteq H$.

Now, let $m \in H$. By the division algorithm (see Sec. 1.6.2), $m = ns + r$ for some $n, r \in Z$, $0 \leq r < s$. Thus, r = m -ns. But **H** is a subgroup of Z and $m, ns \in \mathbf{H}$. Thus, $r \in H$. By minimality of $S \in S$, we must have r = 0, i.e., m = ns. Thus, $H \subseteq s\mathbf{Z}$.

So we have proved that **H** = s**Z**.

Before going to the next example, let us see what the nth roots of unity are, that is; for which complex numbers z is $z^n = 1$.

From Unit 2, you know that the polar form of a non-zero complex number $z \in \mathbf{C}$ **is z** $= r(\cos\theta + i \sin\theta)$, where $r = |z|$ and θ ia an argument of z. Moreover, if θ_1 is an argument of z_1 and θ_2 that of z_2, then $\theta_1 + \theta_2$ is an argument of $z_1 z_2$. Using this we will try to find the nth roots of 1, where $n \in N$.

Thus, by De Moivre's theorem,

$1 = 2^n = 1^n (\cos n\theta + i \sin n\theta)$, that is,
$\cos(\theta) + i \sin(\theta) = r^n (\cos n\theta) + i \sin n\theta)$. …….. (1)

Equating the modulus of both the sides of (1), we get rn = 1, i.e., r = 1. On comparing the arguments of both sides of (1), we see that $0 + 2\pi k$ ($k \in \mathbf{Z}$) and $n\theta$ are arguments of the same complex number. Thus, $n\theta$ can take any one of the values $2\pi k$, $k \in \mathbf{Z}$. Does this mean that as k ranges over Z and θ ranges over $Cos\ \frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} = \cos\frac{2\pi m}{n} + i \sin\frac{2\pi m}{n}$ if and only if $\frac{2\pi k}{n} - \frac{2\pi m}{n} = 2\pi t$ for some $t \in$ Z. This will happen if k = m + nt, i.e., k = m (mod n). Thus, corresponding to every $\bar{r}$ in Z_n we get an nth root of unity, $z = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$, $0 \le r < n$; and these are all the nth roots of unity.

For example, if n = 6, we get the 6^{th} roots of 1 as z_0, z_1, z_2, z_3, z_4, and z_5, where z_j, $\frac{2\pi j}{6} + i \sin\frac{2\pi j}{6}$, $j = 1,\ 2,\ 3,\ 4,\ 5,\ 6$. In Fig. 1 you can see that all these lie on the unit circle (i.1., the circle of radius one with centre (0, 0)). They form the vertices of a regular hexagon.

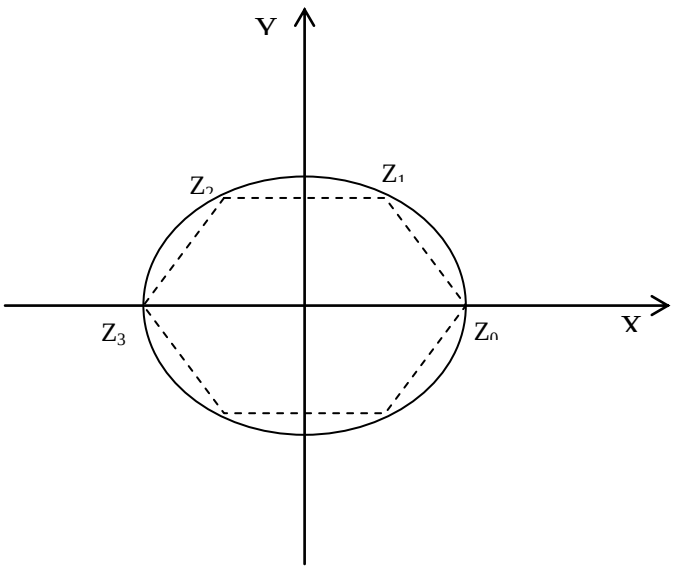

Fig. 1: 6^{th} Roots of Unity

Now, let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then all the nth roots of 1 are 1, ω, ω^2, ……., ω^{n-1}, since $\omega^j = \cos\frac{2\pi j}{n} + i\sin\frac{2\pi j}{n}$ for $0 \leq j \leq n-1$ (using De Moivre's theorem).

Let $\bigcup_n = \{1, \omega, \omega^2, \ldots\ldots, \omega^{n-1}\}$. The following exercise shows you an interesting property of the elements of $\bigcup_n$.

SELF ASSESSMENT EXERCISE 3

If $n > 1$ and $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, then show that $1 + \omega + \omega^2 + \omega^3 + \ldots + \omega^{n-1} = 0$.

Now we are in a position to obtain a finite subgroup of C*.

Example 5

Show that $\bigcup_n \leq (\mathbf{C}^*, .)$.

Solution

Clearly, $\bigcup_n \neq \phi$. Now, let $\omega^i, \omega^j \in \bigcup_n$.

Then, by the division algorithm, we can write $i + j = q_n + r$ for $q, r \in Z$, $0 \leq r \leq n-1$. But then $\omega^i . \omega^j = \omega^{i+j} = \omega^{qn+r} = (\omega^n)^q, \omega^r = \omega^r \in \bigcup_n$, since $\omega^n = 1$, i.e, ω^{n-1}. Thus, $\bigcup_n$ is closed under multiplication.

Finally, if $\omega^1 \in \bigcup_n$, then $0 \leq i \leq n-1$ and $\omega^i, \omega^{n-1} = \omega^n = 1$, i.e., ω^{n-1} is the inverse of ω^1 for all $1 \leq i < n$. Hence, $\bigcup_n$ is a subgroup of **C***.

Note that $\bigcup_n$ **is a finites group of order n and is a subgroup of an infinite group, C*.** So, for every natural number n we have a finite subgroup of order n of C*.

Before ending this section we will introduces you a subgroup that you will use off and on.

Definition

The centre of a group G, denoted by **Z(G) =G,** denoted by **Z(G)**, is the set $Z(G) = \{g \in G \quad xg = gx \; \forall \; x \in G\}$.

Thus, Z(G) is the set of some elements of G that commute with every element of G.

For example, if G is abelian, then Z(G) = G.

We will now show that $Z(G) \leq G$.

Theorem 2

The centre of any group G is a subgroup of G.

Proof

Since $e \in Z(G)$, $Z(G) \neq \phi$. Now,

$a \in Z(G) \quad \Rightarrow ax = xa \ \forall \ x \in G.$
$\Rightarrow x = a^{-1} xa \ \forall \ x \in G$, pre-multiplying by a^{-1}.
$\Rightarrow x = a^{-1} = a^{-1} x \ \forall \ x \in G$, post-multiplying by a^{-1}.
$\Rightarrow a^{-1} \in Z(G)$.

Also, for any $a, b \in Z(G)$ and for any $x \in G$.
$(ab) x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.
$\therefore ab \in Z(G)$.

Thus, Z(G) is a subgroup of G.

The following exercise will give you some practice in obtaining the centre of a group.

SELF ASSESSMENT EXERCISE 4

Show that $Z(S_{3)}) = (\mathbf{I})$.

(**Hint**: write the operation table for S_3)

Let us now discuss some properties of subgroups.

3.2 Properties of Subgroups

Let us start with showing that the relation 'is a subgroup of' is transitive. The proof is very simple.

Theorem 3

Let G be a group, H be a subgroup of G and K be a subgroup of H. Then k is a subgroup of G.

Proof

Since $K \leq H$, $K \neq \phi$ and $ab^{-1} \in K \ \forall \ a, b \in K$. Therefore, $K \leq G$.

Let us look at subgroups of Z, in the context of Theorem 3.

Example 6

In Example 4 we have seen that any subgroup of Z is of the form m**Z** for some m $\in$ N. Let m**Z** and k**Z** be two subgrougs of **Z**. Show that m**Z** is a subgroup of k**Z** iff k | m.

Solution

We need to show that m**Z** $\subseteq$ k**Z** $\Leftrightarrow$ k | m. Now m**Z** $\subseteq$ k**Z** $\Leftrightarrow$ m $\in$ m**Z** $\subseteq$ k**Z** $\Rightarrow$ m $\in$ k**Z** $\Rightarrow$ m = kr for some r $\in$ **Z** k |m.

Conversely, suppose k | m.

Then, m = kr for some r $\in$ **Z**. Now consider any n $\in$ m**Z** such that n = mt.

Then n = mt = (kr) t = k (rt) $\in$ k**Z**.

Hence, m**Z** $\subseteq$ k**Z**

Thus, m**Z** $\leq$ k**Z** iff k | m.

Now, you may like to try the next exercise.

SELF ASSESSMENT EXERCISE 5

Which subgroups of **Z** is 9**Z** a subgroup of?

We will now discuss the behaviour of subgroups under the operations of intersection and union.

Theorem 4

If H and K are two subgroups of a group G, then H$\cap$K is also a subgroup of G.

Proof

Since e $\in$ H and e $\in$ K, where e is the identity of **G**, **e** $\in$ H$\cap$K.

Thus, H$\cap$K $\neq \phi$.

Now, let a, b $\in$ H$\cap$K. By Theorem 1, it is enough to show that $ab^{-1} \in$ H$\cap$K. Now, since a, b $\in$ H, $ab^{-1} \in$ H. Similarly, since a, b $\in$ K, $ab^{-1} \in$ K. Thus, $ab^{-4} \in$ H$\cap$K. Hence, H$\cap$K is a subgroup of G.

The whole argument of Theorem 4 remains valid if we take a family of subgroups instead of just two subgroups. Hence, we have the following result.

Theorem 4': if $\{H_i\}_{i \in 1}$ is a family of subgroups of a group G, then $\bigcap_{i \in 1} H_i$ is also a subgroup of G.

Now, do you think the union of two (or more) subgroups is again a subgroup? Consider the two subgroups $2\mathbf{Z}$ and $3\mathbf{Z}$ of $\mathbf{Z}$. Let $S = 2\mathbf{Z} \cup 3\mathbf{Z}$. Now, $3 \in 3\mathbf{Z} \subseteq S$, $2 \in 2Z \subseteq S$, but $1 = 3 - 2$ is neither in $2\mathbf{Z}$ nor in $3\mathbf{Z}$. Hence, S is not a subgroup of (Z,+). Thus, if A and B are subgroups of G, $A \cup B$ need not be a subgroup of G. But, if $A \subseteq B$ is a subgroup of G. The next exercise says that this is the only situation in which $A \cup B$ is a subgroup of G.

SELF ASSESSMENT EXERCISE 6

Let A and B be two subgroups of a group G. Prove that $A \cup B$ is a subgroup of G iff $A \subseteq B$ or $B \subseteq A$.

(**Hint**: Suppose $A \subseteq B$ and $B \subseteq A$. Take $a \in A \backslash B$ and $b \in B \backslash A$. Then show that $ab \notin A \cup B$. Hence, $A \cup B \leq G$. Note that proving this amounts to proving that $A \cup B \leq G \Rightarrow A \subseteq B$ or $B \subseteq A$.

Let us now see what we mean by the product of two subsets of a group G.

Definition

Let G be a group and A, B be non-empty subsets of G.

The **product of A and B** is the set $\mathbf{AB} = \{ab \mid a \in A, b \in B\}$.

For example, $(2\mathbf{Z})(3\mathbf{Z}) = \{(2m)(3m) \mid m, n \in \mathbf{Z}\}$
$= \{6mn \mid m, n \in \mathbf{Z}\}$
$= 6\mathbf{Z}$.

In this example we find that the product of two subgroups is a subgroup. But is that always so? Consider the group

$S_1 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, and its subgroups $H = \{1, (1\ 2)\}$ and $K = \{1, (1\ 3)\}$.

Remember, (1 2) is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $(1\ 2\ 3)$ is the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Now HK = {I ∘ I, I ∘ (1 3), (1 2) ∘I, (1 2) ∘ (1 3)}
= {I, (1 3), (1 2), (1 3 2)}

HK is not a subgroup of G, since it is not even closed under composition. (Note that (1 3) ∘ (1 2) = (1. 2 3) ∉ HK.)

So, when will the product of two subgroups be a subgroup? The following result answers this question.

Theorem 5

Let H and K be subgroups of a group G. Then HK is a subgroups of G if HK = KH.

Proof

Firstly, assume that HK ≤ G. We will show that HK = KH. Let hk ∈ HK. Then $(hk)^{-1} = k^{-1} h^{-1} \in$ HK, since HK ≤ G.

Therefore, $k^{-1} h^{-1} = k_1 h_1$ for some $h_1 \in$ H, $k_1 \in$ K. But then $hk = (k^{-1} h^{-1})^{-1} = k_1^{-1} h_1^{-1} \in$ KH. Thus, HK ⊆ KH.

Now, we will show that KH ⊆ HK. Let kh ∈ KH. Then $(kh)^{-1} = h^{-1} k^{-1} \in$ HK. But HK ≤ G. Therefore, $(kh)^{-1})^{-1} \in$ HK, that is, kh ∈ HK. Thus, KH ⊆ HK.

Hence, we have shown that HK = KH.

Conversely, assume that HK = KH. We have to prove that HK ≤ G. Since $e = e^2 \in$ HK, HK ≠ ϕ.
Now, let a, b∈ HK. Then a = hk and $b = h_1 k_l$ for some h, $h_1 \in$ Hand k, $k_l \in$ K.

Then $ab^{-1} = (hk)(k_1^{-1} h_1^{-1}) = h[(kk, {}_1^{-1}) h_1^{-1}]$.

Now $(kk_1^{-1}) h_1^{-1} \in$ KH = HK. Therefore, ∃ $h_2k_2 \in$ HK such that $(kk_1^{-1}) h_1^{-1} = h_2k_2$.
+Then, $ab^{-1} = h(h_2k_2) = (hh_2)k_2 \in$ HK.
Thus, by Theorem 1, HK ≤ G.

The following result is a nice corollary to Theorem 5.

Corollary: If H and K are subgroups or abelian group G, then HK.

Try the following exercise now.

SELF ASSESSMENT EXERCISE 7

Is AB a subgroup of S_4, where A = {I, (1 4)} and B = {I, (1 2)}?

The next topic that we will take up is generating sets.

3.3 Cyclic Groups

In this section we will briefly discuss generating sets, and then talk about cyclic groups in detail.

Let G be any group and S a subset of G. Consider the family *F* of all subgroups of G that contain S, that is,

$F = \{H \mid H \leq G \text{ and } S \subseteq H\}$.

We claim that $F \leq \phi$. Why Doesn't $G \in F$? Now, by Theorem 4′, $\bigcap_{H \in F} H$ is a subgroup of G.

Note that

i $S \subseteq \bigcap_{H \in F} H$.

ii. $\bigcap_{H \in F} H$ is the smallest subgroup of G containing S. (Because if K is a subgroup of G containing S, then $K \in F$.
Therefore, $\bigcap_{H \in F} H \subseteq K$.)

These observations lead us to the following definition.

Definition

If S is a subset of a group G, then the smallest subgroup of G containing S is called **the subgroup generated by the set S**, and is 'written as <S>.

Thus, $\langle S \rangle = \cap \{H \mid H \leq G, S \not\subset H\}$.
If $S = \phi$, then $\langle S \rangle = \{e\}$.
If $\langle S \rangle = G$, then we say that G is **generated by the set S**, and that S is a set of **generators of G**.

If the set **S** is finite, we say that G is **finitely generated**.

Before giving examples, we will give an alternative way of describing <S>. This definition is much easier to work with than the previous one.

Theorem 6

If S is a non-empty subset of a group G, then
$<S> = \{a_1^{n_1} a_2^{n_2} .....a_k^{n_k} \mid a_i \in S for\ 1 \ \ i \ \ k, n_1, ..., n_k \ \ Z.\}$

Proof

Let $A = \{a_1^{n_1} a_2^{n_2} .....a_k^{n_k} \mid a_i \in S for\ 1 \ \ i \ \ k, n_1, ..., n_k \ \ Z.\}$
Since a_1……, $a_k \in S \subseteq <S>$ and <S> is a subgroup of G, $a_1^{n_1} \in <S>$.

Now, let us see why $<S> \subseteq A$. We will show that A is a subgroup containing S. Then, by the definition of <S>, it will follow that $<S> \subseteq A$.

Since any $a \in S$ can be written as $a = a^1$, $S \subseteq A$.
Since $S \neq \phi$ $A \neq \phi$.

Now let $x, y \in A$. Then $x = (a_1^{n_1} a_2^{n_2} .....a_k^{n_k})(b_1^{m_1} b_2^{m_2} .....b_r^{m_r})^{-1}$ l

$= (a_1^{n_1} a_2^{n_2} .....a_k^{n_k})(b_r^{-m_r} .....b_1^{m_1}) \in A.$

Thus, by Theorem 1, A is a subgroup of G. Thus, A is a subgroup of G containing S. And hence, $<S> \subseteq A$.

This shows that <S> = A.

Note that, if (G, +) is a group generated by S, then any element of G is of the form $n_1 a_1 + n_2 a_2 + …….. n_r a_r$, where $a_1, a_2 …., a_r \in S$ and $n_1, n_2 …….. n_r \in Z$.

For example, Z is generated by the set of odd integers $S = \{\pm1, \pm3, \pm5, ….\}$. Let us see why. Let $m \in Z$. Then $m = 2^r_s$ where $r \geq 0$ and $s \in S$. Thus, m e <5>. And hence, <S> = Z.

Try the following exercises now.

SELF ASSESSMENT EXERCISE 8

Show that S = {I} generates **Z**.

SELF ASSESSMENT EXERCISE 9

Show that a subset **S** of **N** generates the group Z of all integers iff there exist
S_1….. , S_k in Sand n_l, ….. n_k in Z such that $n_1 s_1 + …..+ n_k s_k = 1$.

(**Hint**: **Apply Theorem 6**.)

SELF ASSESSMENT EXERCISE 10

Show that if S generates a group G and $S \subseteq T \subseteq G$, then <T> = G.

Self-Assessment Exercise 10 shows that a group can have many generating sets. Self Assessment Exercise 8 gives an example of a group that is generated by only one element. We give such a group a special name.

Definition

A group G is called a **cyclic group** if $G = \langle \{a\} \rangle$ for some $a \in G$. We usually write $\langle \{a\} \rangle$ as $\langle \mathbf{a} \rangle$.

Note that $\langle a \rangle = \{a^n \mid n \in Z\}$.

A subgroup H of a group G is called a **cyclic subgroup** if it is a cyclic group. Thus, $\langle (12) \rangle$ is a cyclic subgroup of S_3 and $2Z = \langle 2 \rangle$ is a cyclic subgroup of **Z**.

We would like to make the following remarks here.

Remark 3

i. If $K \leq G$ and $a \in K$, then $\langle a \rangle \subseteq K$. This is because <a> is the smallest subgroup of G containing

ii. All the elements of $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$ may or may not be a distinct. For example, take $a = (1\ 2) \in S_3$.

Then $\langle (1\ 2) \rangle = \{I, (1\ 2)\}$, since $(1\ 2)^2 = I$, $(1\ 2)3 = (1\ 2)$, and so on.

SELF ASSESSMENT EXERCISE 11

Show that if $G \neq \{e\}$, then $G \neq \langle e \rangle$.

SELF ASSESSMENT EXERCISE 12

Show that $\langle a \rangle = \langle a\text{-}1 \rangle$ for any $a \in G$.

We will now prove a nice property of cyclic groups.

Theorem 7

Every cyclic group is abelian

Proof

Let G = <a> = $\{a^n \mid n \in \mathbf{Z}\}$. Then, for any x, y in G there exist m, n $\in$ **Z** such that x = a^m, y = a^n. But, then xy = $a^{m.} a^a = a^{m+n} = a^n.a^m$ = yx. Thus, xy = yx for all x, y. in G.

That is, G is abelian.

Note that **Theorem 7** says that every cyclic group is abelian. But this does not mean that every abelian group of is cyclic. Consider the following example.

Example 7

Consider the set K_4 = {e, a, b, ab} and the binary operation of K_4 given by the table.

•	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Fig. 2: Felix Klein (1849–1925)

The table shows that (K_4 , .) is a group.

This group is called the **Klein 4-group**, after the pioneering German group theorist Felix Klein.

Show that K_4 is abelian but not cyclic.
Solution

From the table we can see that K_4 is abelian. If it were cyclic, it would have to be generated by e, a,. b or ab. Now, < e > = {e}. Also, a^1 =a,a^2 = e,a^3 = a, and so on.

Therefore, < a > = {e, a}. Similarly, < b > = {e, b} and < ab > = { e, ab}.

Therefore, K_4 can't be generated bye, a, b or ab.
Thus, K_4 is not cyclic.

Use **Theorem 7** to solve the following exercise.

SELF ASSESSMENT EXERCISE 13

Show that S3 is not cyclic.

Now let us look at another nice property of cyclic groups.

Theorem 8

Any subgroup of a cyclic group is cyclic.

Proof

Let $G = < x >$ be a cyclic group and H be a subgroup.

If $H = \{e\}$, then $H = < e >$, and hence, H is cyclic.

Suppose $H \neq \{e\}$. Then 3 $n \in Z$ such that $x^n \in H$, $n \neq 0$. Since H is a subgroup, $(x^{-n})^{-1} = x^{-n} \in H$. Therefore, there exists a positive integer m(i.e., n or-n) such that $x^m \in H$. Thus, the set $S = \{t \in N \mid x^t \mid \in H\}$ is not empty. By the well-ordering principle (see Sec.) 1.6.1.) S has a least element, say k. We will show that $H = < x^k >$.

Now, $<x^k > \subseteq H$, since $x^k \in H$.

Conversely, let x^n be an arbitrary element in H. By the division algorithm $n = mk + r$ where $m, r \in Z$, $0 \leq r \leq k\text{-}l$. But then $x^r = x^r = x^{n-mk} = x^n . x^k)^m \in H$, since $x^n, x^k \in .$ H. But k is the least positive integer such that $x^k \in H$. Therefore, x^r can be in H only if $r = 0$. And then, $n = mk$ and $x^n = (x^k)^m \in < k^k >$. Thus, $H \subseteq < x^k >$. Hence, $H = < x^k ?$, that is, H is cyclic.

Using Theorem 8 we can immediately prove what we did in Example 4. .
Now, Theorem 8 says that every subgroup of a cyclic group is cyclic. But the converse is not true. That is, we can have groups whose proper subgroups are all cyclic, without the group being cyclic. We give such an example now.

Consider the group S_3, of all permutations on 3 symbols. Its proper subgroups are subgroups are all cyclic, without the group being cyclic. We give an example now.

Consider the group S_3, of all permutations on 3 symbols. Its proper subgroups are

$A = < 1 >$
$B = <12>$
$C = < (1\ 3) >$
$D = < (2\ 3) >$
$E = <123>$

As you can see, all these are cyclic. But, by Self Assessment Exercise you know that S_3 itself is not cyclic.

Now we state a corollary to Theorem 8, in which we write down the important point made in the proof of Theorem 8.

Corollary: Let H ≠{e} be a subgroup of < a >. Then H = < a^n >, where n is the least positive integer such that $a^n \in H$.

Try the following exercises now.

SELF ASSESSMENT EXERCISE 14

Show that any non-abelian group must have a proper subgroup other than {e}.

SELF ASSESSMENT EXERCISE 15

Obtain all the subgroups of Z_4, which you know is $< \overline{1} >$.

Let us now see what we have done in this unit.

4.0 CONCLUSION

Subgroups play important roles in group theory. In MTH 312 you will be introduced to another important subgroups called the normal subgroups which has a lot of application in some other sciences such as Molecular Chemistry, You are to read carefully and master all the materials in this unit.

5.0 SUMMARY

I
n this unit we have covered the following points.

1. The definition and examples of subgroups.
2. The intersection of subgroups is a subgroup.
3. The union of two subgroups H and K is a subgroup if and only if H $\subseteq$ K or K $\subseteq$ H.
4. The product of two subgroups H and K is a subgroup if and only if HK = KH.
5. The definition of a generating set.
6. A cyclic group is abelian, but the converse need not be true.
7. Any subgroup of a cyclic group is cyclic, but the converse need not be true.

ANSWER TO SELF ASSESSMENT EXERCISE 1

1. Yes, because H is a group in its own right.

ANSWER TO SELF ASSESSMENT EXERCISE 2

2. {e} ≠ . Also for any e e^{-1} = e ∈ {e} ….., by Theorem 1, {e} ≤ G.
   G ≤ ϕ. Also for any x ∈ G, x^{--1} ∈ G. :., for a, b ∈ G.
   A, b e G ∴ ab^{-1} e G. ∴ G ≤ G.

ANSWER TO SELF ASSESSMENT EXERCISE 3

Since $\omega^n = 1, (1-\omega^n) = 0$ i.e.,
$(1 - \omega)(1+\omega+\omega^2+.....+\omega^{n-1} = 0.$
Since $\omega \neq 1, 1+\omega^2+.....+\omega^{n-1} = 0.$

ANSWER TO SELF ASSESSMENT EXERCISE 4

From Self Assessment Exercise 14 of Unit 2 recall the elements of S_3. On writing the operation table for S_3 you will find that only I commute with every permutation in S_3.

ANSWER TO SELF ASSESSMENT EXERCISE 5

The divisors of 9 are 1, 3 and 9
Thus, 9**Z** is a subgroup of **Z**, 3**Z** and itself only.

ANSWER TO SELF ASSESSMENT EXERCISE 6

We know that if $A \subseteq B$ or $B \subseteq A$, then $A \cup B$ is A or B, and hence, is a subgroup of G.

Conversely, we will assume that $A \subseteq$ Band $B \subseteq A$, and conclude that $A \cup B \nleq G$.
Since $A \subseteq B$, $\exists$ a $\in$ A such that a $\notin$ B.

Since $B \subseteq A$, $\exists$ b $\in$ B such that b $\notin$ A.

Now, if ab $\in$ A, then ab = c, for some c $\in$ A.
Then $b = a^{-1} c \in A$, a contradiction. $\therefore ab \notin A$. Similarly, ab $\notin$ B. ...ab $\notin A \cup B$.

But a $\in A \cup B$ and b $\in A \cup B$. So, $AUB \nleq G$.

ANSWER TO SELF ASSESSMENT EXERCISE 7

AB = {I, (1 4), (1 2), (1 2 4)
But, (1 2) ◦ (14) = (142) $\notin$ AB. $\therefore$ $AB \nleq S_4$

ANSWER TO SELF ASSESSMENT EXERCISE 8

For any n $\in$ Z, n = n. l $\in$ < {1} >. $\therefore$ Z = < {1} >.

ANSWER TO SELF ASSESSMENT EXERCISE 9

Firstly, suppose Z = < S>. Then 1 $\in$ < S >. $\therefore$ $\exists s_1,\ldots,s_k \in S$ and
$n_l, \ldots\ldots, n_k \in Z$ such that $n_1s_1 + \ldots + n_ks_k = 1$.

Conversely, suppose $\exists$, s_1, …….$s_k \in S$ and n_1,…., $n_k \in \mathbf{Z}$ such that $n_1s_1 + n_2s_2 +\ldots.. + n_ks_k = 1$.

Then, for any $n \in Z$, $n = n.1 = nn_1, s_1, + ...:. + nn_ks_k \in <S>$.
$\therefore Z = < S >$.

ANSWER TO SELF ASSESSMENT EXERCISE 10

We know that $G = < S >$. Therefore, for any $g \in G$,
$\exists$ s_1……,$s_k \in S$ and n_1,….., $n_k \in Z$ such that $g = s_1^{n_1}$ .....$s_k^{n_k}$ m
Since $S \subseteq T$, $s_1 \in T$ $\forall_i = 1, \ldots, k$.
$\therefore$ by Theorem 6, we see that $G = < T >$.

ANSWER TO SELF ASSESSMENT EXERCISE 11

Since $G \neq \{e\}$, $\exists a \neq e$ in G. Since $a \neq e$ for any $r \in \mathbf{Z}$. $a \neq < e >$.
$\therefore G \neq < e >$.

ANSWER TO SELF ASSESSMENT EXERCISE 12

We will show that $< a > \subseteq < a^{-1} >$ and $< a^{-1} > \subseteq < a >$.
Now, any element of $< a >$ is $a^n = (a^{-1})^{-n}$, for $n \in \mathbf{Z}$.
$\therefore a^n \in < a^{-1} >$. $\therefore < a > \subseteq <$ a-1 $>$.

Similarly, $< a^{-1} > = < a >$.

$< a > = < a^{-1} >$.

ANSWER TO SELF ASSESSMENT EXERCISE 13

Since S_3 is not abe!ian (e.g., $(1\ 3) \circ (1\ 2) \neq (1\ 2) \circ (1\ 3)$), by .
Theorem 7, S_3 can't be cyclic.

6.0 TUTOR- MARKED ASSIGNMENT

1. Let G be a non-abelian group. Then $G \neq \{e\}$. Therefore, 3 $a \in G$, $a \neq e$. Then $< a > G$. $G \subseteq < a >$, since G is non-abelian. $\therefore < a > \leq G$.
2. Since $\mathbf{Z}_4$ is cyclic, all its Subgroups are cyclic.
   Thus, its Subgroups are $\mathbf{Z}_4$, $< \overline{2} >$, $< \overline{3} >$ and

7.0 REFERENCES/FURTHER READINGS

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.

UNIT 4 LAGRANGE'S THEOREM

CONTENTS

1.0 INTRODUCTION

In the previous unit we have discussed different subgroups. In this unit we will see how a subgroup can partition a group into equivalence classes. To do this we need to define the concept of cosets.

In Sec. 4.3 we use cosets to prove a very useful result about the number of elements in a subgroup. The beginnings of this result were made in a research paper on the solvability of algebraic equations by the famous mathematician Lagrange. Today this elementary theorem is known as Lagrange's theorem, though Lagrange proved it for subgroups of S_n only.

While studying MTH 312 you will be using Lagrange's theorem again and again. So, make sure that you read this unit carefully.

2.0 OBJECTIVES

At the end of this unit, you should be able to::

- form left or right cosets of a subgroup
- partition a group into disjoint cosets of a group
- prove and use Lagrange's theorem.

3.0 MAIN CONTENT

3.1 Cosets

In Sec. 3.3 we defined the product of two subsets of a group. We will now look at the case when one of the subsets consists of a single element only. In fact, we will look at the situation $H\{x) = \{hx \mid h \in H\}$, where H is a subgroup of a group G and $x \in G$. We will denote $H\{x\}$ by Hx.

Definition

Let H be a subgroup of a group G, and let $x \in G$. We call the set,
$\{hx \mid h \in H\}$ a **right coset** of H in G. The element x is a **representative of Hx**.

We can similarly define the left coset

$xH \quad \{xh \mid h \in H\}$

Note that, if the group operation is +, then the right and left cosets of H in (G,+) represented} $x \in G$ are

$H+x = \{h+x \mid h \in H\}$ and $x + H = \{ x + h \mid h \in H\}$, respectively.

Let us look at some examples.

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
$He= \{he \mid h \in H\} = \{h \mid h \in H\} =H$.

Similarly, $eH = H$.

Thus, H is a right as well as left coset of H in G.

Example 2

What are the right cosets of 4Z in Z? '

Solution

Now H = 4Z = {….., -8, -4, 0, 4, 8, 12, ….}

The, right cosets of H are
H + 0 = H, using Example 1.
H +1 = {…… , -11, -7, -3, 1,5,9, 13,….. }
H + 2 = {….., -10, -6, -2, 2, 6, 10, 14, …..}
H+3 = { ….,-9,-5,-1,3,7,11,15,…. }
H + 4 = {….., -8, -4, 0, 4, 8, 12,…..} = H

Similarly, you can 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 co sets are H, H+1, H+2 and H+3.

In general, **the distinct right cosets of H (= nZ) in Z are H, H+l,**

H+ (n-l). Similarly, the distinct left cosets of H (=nZ) in Z are H, 1 +H, 2+H ....., (n-1) + H.

Before giving more examples of cosets, let us discuss some properties of cosets.

Theorem 1

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

Then

a. $x \in Hx$
b. $Hx = H \Leftrightarrow x \in H$.
c. $Hx = H \Leftrightarrow xy^{-1} \in H$.

Proof

a. Since x = ex and e $\in$ H, we find that x $\in$ Hx.
b. Firstly, let us assume that Hx = H. Then, since x $\in$ H x, x $\in$ H.

   Conversely, let us assume that x $\in$ H. We will show that Hx $\subseteq$ H and H $\subseteq$ Hx. Now any element of Hx is of the form hx, where h $\in$ H. This is in H, since h $\in$ H and x $\in$ H. Thus, Hx $\subseteq$ H. Again, let h$\in$ H. Then h = (hx^{-l}) x $\in$ Hx, since $hx^{-1} \in$ H.

   $\therefore$ H $\subseteq$Hx.
   $\therefore$ H = Hx.

c. $Hx = Hy = \Leftrightarrow Hxy^{-1} = Hyy^{-1} = He = H \Leftrightarrow xy^{-1} \in H$, by (b).

   Conversely, $Xy^{-1} \in H \Leftrightarrow Hxy^{-1} = H \Leftrightarrow Hxy^{-1}y = Hy \Leftrightarrow Hx = Hy$.

Thus, we have proved (c).

The properties listed in Theorem 1, are not only true for right cosets. We make the following observations.

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

a. $x \in xH$.
b. $xH = H \Leftrightarrow x \in H$.
c. $xH = yH \Leftrightarrow x^{-1}y \in H$.

Let us look at a few more examples of cosets.

Example 3

Let $G = S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 23), (13\ 2)$ and H be the cyclic subgroup of G generated by (1 2 3). Obtain the left cosets of H in G.

Solution

Two cosets are

$H = \{I, (1\ 23), (1\ 3\ 2)\}$ and
$(1\ 2)H = \{(1\ 2), (1\ 2) \circ (1\ 2\ 3), (1\ 2) \circ (1\ 3\ 2)\}$
$= \{(1\ 2), (2\ 3), (1\ 3))$

For the other cosets you can apply Theorem 1 to see that

$(1\ 2)\ H = (2\ 3)H = (1\ 3)H$ and
$(123)H = (132)H$.

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

Try the following exercise now.

SELF ASSESSMENT EXERCISE 1

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

Let us now look at the cosets of a very important group, the **quaternion group.**

Example 4

Consider the following set of 8 2x2 matrices over **C.**

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

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

You can check that the following relations hold between the elements of Q_8:

$I^2 = I$, $A^2 = B^2 = C^2 = -I$,
$AB = C = -BA$, $BC = A = -CB$, $CA = B = -AC$.

Therefore, Q_8 is non-abelian group under matrix multiplication.

Show that the subgroup $H = < A >$ has only two distinct right cosets in Q_8.

Solution

$H = < A> = \{I, A, A^2, A^3\} = \{I, A, -I, -A\}$,
Since $A^4 = I$, $A^5 = A$, and so on.
Therefore, $HB = \{B, C, -B, -C\}$, using the relations given above.
Using Theorem I (b), we see that
$H= HI = HA = H(-I) = H(-A)$.
Using Theorem I(c), we see that
$HB =HC= H(-B) = H(-C)$.
Therefore, H has only two distinct right co sets in Q_8, H and HB.

The following exercise will help you to understand Q_8.

SELF ASSESSMENT EXERCISE 2

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

We will show that each group can be written as the union of disjoint cosets of any of its subgroups. For this we define a relation on the elements of G.

Definition

Let H be a subgroup of a group G. We define a relation '~' on G by $x \sim y$ iff $xy^{-1} \in H$, where $x, y \in G$. Thus, from Theorem 1 we see that $x \sim y$ iff $Hx = Hy$.

We will prove that this relation is an equivalence relation (see unit 1).

Theorem 2

Let H be a subgroup of a group G. Then the relation ~defined by '$x \sim y$' $xy^{-1} \in H$ is an equivalence relation. The equivalence classes are 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 $xy^{-1} \in H$.

$\therefore$ $xy = xy^{-1-} \in H$, Thus, $y \sim x$. That is, ~ is symmetric.

Finally, fi x, y, z, $\in$ G such that $x \sim y$ and $y \sim z$, then $xy^{-1} \in H$ and $yz^{-1} \in H$.

$\therefore$ $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H$, $\therefore x \sim z$.

That is ~ is transitive.
Thus, ~ is an equivalence relation.
The equivalence class determined by $x \in G$ is $\{x| = \{y \in G \mid y - x\} = \{y \in G \mid xy^{-1} \in H\}$.

Now, we will show that [x] = Hx. So, let $y \in [x]$. Then Hy = Hx, by Theorem 1. And since $y \in Hy$, $y \in Hx$.

Therefore, $[x] \subseteq Hx$.

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, $H \subseteq G$ [x].

Thus, we have shown that [x] = Hx.
Using Theorem 2 and Theorem 1 (d) of Unit l, we can make the following remark.

Remark

If Hx and Hy are two right cosets of a subgroup H in G, then **Hx** = **Hy** or $Hx \cap Hy = \phi$.

Note that what Theorem 2 and the remark above say is that **any subgroup H of a group G partitions G into disjoint right cosets**.

On exactly the same lines as above we can state 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 example, $S_3 = < (1\ 23) > \bigcup (1*2) < (1\ 2\ 3) >$ (using Example 3).

You may like to do the following exercises now.

SELF ASSESSMENT EXERCISE 3

Let H be a subgroup of a group G. Show that there is a one-to-one correspondence between the elements of H and those of any right or left coset of H.

(**Hint**: Show that the mapping $f: H \rightarrow Hx$: $f(h) = hx$ is a bijection.)

SELF ASSESSMENT EXERCISE 4

Write Z as a union of disjoint cosets of 5**Z**.

Using Self-Assessment Exercise 3 we can say 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.**

We will use this fact to prove an elementary theorem about the number of cosets of a subgroup of a finite group 10, the next section.

3.2 LAGRANGE'S THEOREM

In this section we will first define the order of a finite group and then show that the order of any subgroup divides the order of the group.
So let us start with a definition.

Definition

The **order** of a finite group G is the number of elements in G. It is denoted by **o(G)**. For example, $o(S_3) = 6$ and $o(A_3) = 3$. Remember, A3 = {I, (1 23), (1 32)}!

You can also see that $o(Z_n> = n$. And, from Sec. 2.5.2 you know that $o(S_n> = n!$.

Now, let G be a finite group and H be a subgroup of G. We define a function f between the set of right cosets of H in G and the set of left cosets of H in G by

$f: \{Hx \mid x \in G\} \rightarrow \{y H \mid y \in G\}: f(Hx) = x^{-1}H.$

Now try Self-Assessment Exercise 5.

SELF ASSESSMENT EXERCISE 5

Check that f is a bijection.

Self-Assessment Exercise 5 allows us to say that there is a one-to-one correspondence between the right cosets and the left cosets of H in G. Thus, **the number of distinct right cosets of H in G always equals the number of distinct left cosets of H in G**.

Definition

Let H be a subgroup of a finite group G. We call the number of distinct
of H in G the **index** of H in G, and denote it by | **G : H**|.

Thus, from Example 3 we see that $| S_3: A_3| = 2$.

Note that, if we take H = {e}, then | G: {e} | = o(G), since {e}g = {g} ∀ g ∈ G and {e}g ≠ {c}g′ if g ≠g′ .

Now let us look at the order of subgroups. In Sec. 3.4 you saw that the orders of the subgroups of S_3 are 1, 2, 3 and 6. All these divide $o(S_3) = 6$. This fact is part of a fundamental theorem about finite groups. Its beginnings appeared in a paper in 1770, written by the famous French mathematician Lagrange. He proved the result for permutation groups
only. The general result was probably proved by the famous mathematician Evariste Galois in 1839.

Theorem 3 (Lagrange)

Let H be a subgroup of a finite group G. Then o(G) = o(H) | **G: H** |. Thus, o(H) divides o(G), and | **G: H** | divides o(G).

Proof

You know that we can write G as a union of disjoint right cosets of **H** in G. So, if Hx_1, Hx_2, are all the distinct right cosets of if in G, we have

$G = Hx_1 \cup Hx_2 \cup \ldots\ldots \cup Hx_r$ ……. (1)

From **Self Assessment Exercise 3**, we know that $|Hx_1| = |Hx_2| = \ldots = |Hx_r| = o(H)$.

Thus the total number of elements in the union on the right hand side of (l) is element o(H) + o(I I) +….. + o(H) (r times) = r o(H).

Therefore, (1) says that o(G) = r o(H)
= o(H) | **G: H** |.'

You will see the power of Lagrange's theorem when we get down to obtaining all the subgroup of a finite group.

Fig 1: Joseph Louis Lagrange (1736 –1813)

For example, suppose we are asked to find all the subgroups of a group G of order 35. Then the only possible subgroups are those of order 1, 5, 7 and 35. So, for example, we don't need to waste time looking for subgroups of order 2 or 4.

In fact, we can prove quite a few nice results by using Lagrange's theorem. Let us prove some results about the order of an element. But first, let us define this phrase.

Definition

Let G be a group and g ∈ G. Then the **order of g** is the order of the cyclic subgroup < g >, if < g > is finite. We denote this finite number by o(g). If < g > is an infinite subgroup of G, we say that **g is of infinite order**.

Now, let $g \in G$ have finite order. Then the set $\{e, g, g^2, ...\}$ is finite, since G is finite. Therefore, all the powers of g can't be distinct.

Therefore, $g^r = g^S$ for some $r > s$. Then
$g^{r-s} \Rightarrow$,e and $r\text{-}s \in N$. Thus, the set $\{t \in \mathbf{N} \mid gt = e\}$ is non-empty. So, by the well-ordering principle it has a least element Let n be the least positive integer such that $g^n = e$.

Then

$< g > = \{e. g, g^2, g^{n-1}\}$.
Therefore, $o(g) = 0 < g > = n$.

That is, o(g) is the least positive integer n such that $g^n = e$.

(Note that. if $g \in (G, +)$, then o(g) is the **least positive integer n such that $g^n = e$.)**

Now suppose $g \in G$ is of infinite order. Then, for $m \neq n$, $g^m \neq g^n$. (Because, if $g^{m\,n} = e$, which shows that $< g >$ is a finite group.) We will use this fact while proving

Theorem 5

Try the following exercise now.

SELF ASSESSMENT EXERCISE 6

What are the orders of

a) $(1\ 2) \in S_3$, b) $I \in S_4$, c) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in Q_g$,

d) $\overline{3} \in Z_4$, e) $1 \in R$?

Now Jet us prove an important result about the order of an element.

Theorem 4

Let G be a group and $g \in G$ be of order n. Then $g^m = e$ for some $m \in \mathbf{N}$ iff $n \mid m$.

Proof

We will first show that $g^m = e \Rightarrow n \mid m$. For this & consider the set
$S = \{r \in Z \mid g^r = e\}$.

Now, $n \in S$. Also, if $a, b \in S$, then $g^a = e = g^b$. Hence, $g^{a-b} = g^a (g^b)^{-1} = e$. Therefore. $a\text{-}b \in S$. Thus, $S \leq Z$.

So, from Example 4 of Unit 3, we see that S = n**Z**. Remember, n is the least positive integer in S!

Now if $g^m = e$ for some $m \in N$, then $m \in S = n\mathbf{Z}$. Therefore, n | m.

Now let us show that $n \mid m \Rightarrow g^m = e$. Since n | m, m = nt for some $t \in Z$; Then $g^m = g^{nt} = (g^n)^t = e^t = e$. Hence, the theorem is proved.

We will now use Theorem 4 to prove a result about the orders of elements in a cyclic group.

Theorem 5

Let G = < g > be 11 cyclic group.

a. If g is of infinite order then g^m is also of infinite order for every $m \in Z$.

b. If o(g) = n, then $o(g^m) = \frac{n}{(n,m)}$ **V** m = 1, …., n-l.((n, m) is the g.c.d. of n and m.)

Proof

a. An element is of .infinite order iff all its powers are distinct. We know that all the powers of g^m are distinct. We have to show that all the powers of g^m are distinct. If possible, let $(g^m)^t = (g^m)^w$. Then $g^{mt} = g^{mw}$. But then mt = mw, and hence t = w. This shows that the powers of g^m are all distinct, and hence g^m is of infinite order.

b. Since o(g) = n, G= {e, g,….. , g^{n-1}} < gm >, being a subgroup of G, must be of finite order. Thus, g^m is of finite order. Let o(gm) = t. We will show that $t \frac{n}{(n,m)}$.

Now, $g^{mt} = (g^m)^t$ y= e $\Rightarrow$ n | tm, by Theorem 4.

Let d = (n, m). We can then write $n = n_1 d$, $m = m_1 d$, where $(m_l\ n_l) = 1$.

Then $n_1 \frac{n}{d} = \frac{n}{(n,m)}$

Now, $n \mid tm \Rightarrow n \mid tm_l d \Rightarrow n_1 d \mid tm_l d \Rightarrow n \mid tm_1$.

But $(n,m_l) = 1$. Therefore, $n_l \mid t$. ……..…….... (1)

Also, $(g^m)^{n_1} = g^{m_1 dn_1} = g^{m_1 d_1} = g^{m_1 n} = (g^n)^{m_1} = e^{m_1} = e$.

Thus, by definition of $o(g^m)$ and Theorem 4, we have

$t \mid n_l$, …… (2)

(1) and (2) show that

$$t = n_1 \frac{n}{n,m},$$

$$\text{i.e., } o(g^m) = \frac{n}{n,m}$$

Using this result we know that $o(\bar{4})$, in Z_{12} is $\frac{12}{(12,4)} = 3$.

The next exercise will give you some practice in using Theorem 5.

SELF ASSESSMENT EXERCISE 7

Find the orders of= $\bar{2},\bar{4},$ and $5 \in Z_{18}$.

The next exercise is a consequence of Lagrange's theorem.

SELF ASSESSMENT EXERCISE 8

Let G be a finite group and $x \in G$. Then, show that o(x) divides o(G). In particular, show that $x^{o(G)} = e$.

We use the result of Self-Assessment Exercise 8 to prove a simple but important result of finite group theory.

Theorem 6

Every group of prime order is cyclic.

Proof

Let G be a group of prime order p. Since $p \neq 1$, $\exists\ a \in G$ such that $a \neq e$. Now, by Self-Assessment Exercise and Theorem 4, o(a) | p. Therefore, o(a) = 1 or o(a) = p. Since $a \neq e$, $o(a) \geq 2$.

Thus, o(a) = p, i.e., $o(< a >) = p$. So, $< a > \leq G$ such that $o(< a >) = o(G)$. Therefore, $< a> = G$. That is, G is cyclic.

Using Theorem 3 and 6, we can immediately say that all the proper subgroups of a group of order 35 are subgroups.
Now let us look at groups of composite order.

Theorem 7

If G is a finite group such that o(G) is neither 1 nor a prime, then G has non-trivial proper subgroups.

Proof

If G is not cyclic, then any $a \in G$, $a \neq e$, generates a proper non-trivial subgroup $< a >$.

Now suppose G is acyclic, say $G = < x >$, where $o(x) = mn$ $(m, n \neq 1)$.

Then, $(x^m)^n = x^{mn} = e$. Thus, by Theorem 4, $o(x^m) \leq n < o(G)$.

Now, you can see Theorem 7 to solve the following exercise.

SELF ASSESSMENT EXERCISE 9

Obtain two trivial proper subgroups of Z_8.

We will now prove certain important number theoretic results which follow from Lagrange's theorem. Before going further, recall the definition of 'relatively prime' from Sec. 1.6.2.

We first define the Euler phi-function, named after the Swiss mathematician Leonard Euler (1707 – 1783).

Definition

We define the **Euler phi-function** $\phi : \mathbf{N} \rightarrow \mathbf{N}$ as follows:

$\phi(i) = 1$, and
$\phi(u)$ = number of natural numbers < n and relatively prime to n, for
$n \geq 2$.

For example, $\phi(2) = 1$ and $\phi(6) = 2$ (since the only positive integers < 6 and relatively prime to 6 are 1 and 5).

We will now prove a lemma, which will be needed to prove the theorem that follows it. This lemma also gives us examples of subgroups of Z_n, for every
$n \geq 2$.

Lemma1: Let $G = \{ \bar{r} \in Z_n \mid (r, n) = 1 \}$, where $n \geq 2$. Then (G,.) is a group, where $\bar{r}\,\bar{s} = \overline{rs}$ $\forall$ $\bar{r}, \bar{s} \in Z_n$. Further, $o(G) = \phi(n)$.

Proof

We first check that G is closed under multiplication.

Now, $\bar{r}, \bar{s} \in G \Rightarrow (r, n) = 1$ and $(s, n) = 1 \Rightarrow (rs, n) = 1$.

$\Rightarrow \overline{rs} \in G$. Therefore, is a binary operation on G.

$\bar{1} \in G$, and its identity.

Now, for $\bar{r} \in G$, $(r, n) = 1$.
$\Rightarrow$ $ar + bn = 1$ for some a, b, $\in Z$ (by Theorem 8 of Unit 1)
$\Rightarrow n \mid ar$
$\Rightarrow ar = 1 \pmod{n}$
$\Rightarrow \bar{a}\ \bar{r} = \bar{1}$.
$\Rightarrow \bar{a} = \bar{r}^{-1}$

Further, $\bar{a} \in G$, because if a and n have a common factor other than 1, then this factor will divide $ar + bn = 1$. But that is not possible.

Thus, every element in G has an inverse.

Therefore, (G,.) is a group.

In fact, it is the group of the elements of Z_n that have multiplication inverse. Since G consist of all those $\bar{r} \in G$ such that $r < n$ and $(r, n) = 1$, $o(G) = \phi(n)$.

Lemma 1 and Lagrange's theorem immediately give us the following result due to the mathematician Euler and Pierre Fermat.

Theorem 8 (Euler-Fermat)

Let $a \in N$ and $n \geq 2$ such that $(a, n) = 1$.
Then, $a^{\phi(n)} = 1 \pmod{n}$.

Proof

Since $\bar{a} \in Z_n$ and $(a, n) = 1$, $\bar{a} \in G$ (of Lemma 1). Since $o(G) = \phi(n)$, we use Self-Assessment Exercise and find that $a^{-\phi(n)} = \bar{1}$.

Thus, $a^{\phi(n)} = 1 \pmod{n}$.
Now you can use Theorem 8 to solve the following exercises.

SELF ASSESSMENT EXERCISE 10

What is the remainder left on dividing 3^{47} by 23? (Note that $\phi(23) = 22$, since each of the numbers 1, 2, …, 22 are relatively prime to 23.)

SELF ASSESSMENT EXERCISE 11

Let $a \in N$ and p be a prime. Show that = 1 (mod p). (This result is called **Fermat's little theorem**. To prove it you will need to use the fact that $\phi(p) =$ p-1.)

You have seen how important Lagrange's theorem is. Now, is it true that if m | o(G), then G has a subgroup of order m? IF G is cyclic, it is true. (You can prove this on the lines of the proof of Theorem 7.) But, if G is not cyclic, the converse of Lagrange's theorem is not true.

In Unit 7 we will show you that the subgroup
A4 = {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 has no subgroup of order 6, though $6 \mid 12 = o(A_4)$.

Now let us summaries what we have done in this unit.

4.0 CONCLUSION

We have examined in this unit subgroup and cosets of a group. You should read this unit carefully because it will useful in MTH 312 where we shall be considering a class of subgroup called normal subgroup.

5.0 SUMMARY

In this unit we have covered the following points.

1. The definition and examples of right and left cosets of a subgroup.
2. Two left (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 definition of the order of a group and the order of an element of a group
5. The proof of Lagrange's theorem, which states that if H is a group of a finite group G, then o(G) = o(H) | G : H |. But, if m | o(G), then G need not have a subgroup of order m.
6. The following consequences of Lagrange's theorem:

   (i) Every group of prime order is cyclic.
   (ii) $a^{\phi(n)} \equiv 1 \pmod{n}$, where $a, n \in N$, $(a, n) = 1$ and $n \geq 2$.

ANSWER TO SELF ASSESSMENT EXERCISE 1

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

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

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

ANSWER TO SELF ASSESSMENT EXERCISE 2

Since $ab^{-1} \in K$ **∀** a, b $\in$ K, we can apply Theorem 1 of Unit 3 to say that K $\leq Q_8$.
Now, K = KI = K(-I), KA = K(-A) = {A, -A}'
KB – K(-B) = {B, -B}, KC = K(-C) = {C, -C}

ANSWER TO SELF ASSESSMENT EXERCISE 3

Let Hx be a coset of H in G. Consider the function f: H $\rightarrow$ Hx: f(h) = hx.
Now, for h, h′ by cancellation.

Therefore, f is 1 – 1.
F is clearly surjective. 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 f: H $\rightarrow$ Hx: f(h) = xh is a bijection.
Thus, the elements of H and xH are in one-to-one correspondence.

ANSWER TO SELF ASSESSMENT EXERCISE 4

The distinct cosets of 5**Z** in **Z** are 5**Z**, 5**Z** + 1, 5**Z** + 2, 5**Z** + 3, 5**Z** + 4.
$\therefore$ **Z** = 5**Z**$\cup$5**Z** + 1$\cup$5**Z** + 2$\cup$5**Z** + **3**$\cup$5**Z** + 4.

ANSWER TO SELF ASSESSMENT EXERCISE 5

f is well defined because Hx = Hy $\Rightarrow xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H$
$\Rightarrow (y^{-1})^{-1} x^{-1} \in x^{-1}H\, y^{-1}H$
$\Rightarrow$ f(Hx) = f(Hy)

f is 1 – 1 because $f(Hx) = f(Hy) \Rightarrow x^{-1}H = y^{-1}H$
$\Rightarrow yx^{-1} \in H \Rightarrow xy^{-1} \in Hx = Hy.$
F is surjective because any left coset of H in G is $yH = f(Hy^{-1})$.

Therefore, f is a bijection.

ANSWER TO SELF ASSESSMENT EXERCISE 6

i. $(1\ 2) \neq 1, (1\ 2)^2 = (1\ 2) \circ (1\ 2) = I \therefore o((1\ 2)) = 2.$
ii. $1^1 = I. \therefore (I) = 1.$
iii. 2
iv. $\bar{3} \neq \bar{0}, 2, \bar{2} = \bar{6} = \bar{2}, 3, \bar{3} = \bar{9} = \bar{1}, 4, \bar{3} = \overline{12} = \bar{0}, \because o(\bar{3}) = 4.$
v. Since $< 1 >$ **R** is infinite, **1** is of infinite order.

ANSWER TO SELF ASSESSMENT EXERCISE 7

$\mathbf{Z}_{18} = < 1 >$. Thus, using Theorem 5, we see that
$o(\bar{r}) = o(r, \bar{1}) = \dfrac{18}{(18, r)}$, for any $\bar{r} \in \mathbf{Z}_{18}$
$\therefore o(\bar{2}) = 9, o(\bar{4}) = 9, o(\bar{5}) = 18.$

ANSWER TO SELF ASSESSMENT EXERCISE 8

Since $o(x) = o(< x >)$ and $o(< x >) \mid o(G)$, $o(x) \mid o(G)$.
Thus, using Theorem 4, $x^{o(G)} = e$.

ANSWER TO SELF ASSESSMENT EXERCISE 9

$o(Z_8) = 8 = 2 \times 4.$
$\bar{2} \in Z_8$ such that $o(\bar{2}) = 4.$ Then $< \bar{2} > < Z_8.$
Similarly, $\bar{4} \in Z_8$ such that $o(\bar{4}) = 2. \therefore < \bar{4} > < \mathbf{Z}_8.$

ANSWER TO SELF ASSESSMENT EXERCISE 10

We know that in Z_{23}, $(\bar{3})^{\phi(23)} = \bar{1}$,
that is, $3^{22} = \bar{1}. \therefore 3^{44} = \bar{1}$
$\therefore 3^{47} = 3^{-3,}\ 3^{44} = \bar{3}^{-3,} = \overline{27}$
Thus, $3^{47} = 27 \pmod{23}$.

Therefore, on dividing 3^{47} by 23, the remainder we get is 27.

ANSWER TO SELF ASSESSMENT EXERCISE 11

We get the result immediately by using Theorem 8 and the fact that $\phi(p) = p - 1$.

6.0 TUTOR-MARKED ASSIGNMENT

1. State and prove the Lagrange Theorem.
2. Show that every subgroup of a commutative group is normal. Is the converse true? Justify your answer.

7.0 REFERENCES/FURTHER READINGS

Ansa B. E. (2010). Modern Algebra Ethereal Bliss Publisher. Calabar.

Kiku, A. O. (1992). Abtract Algebra Ibadan. Ibadan University, Press

Ilori, S. A. & Akinyele, O. (1986). Elementary Abstract and Linear Algebra. Ibadan University, Press.

Ilori, S. A. & Ajayi D. O. (2000). University Mathematics Series 2. Algebra Books (A Division of Ass Book Markers Nig. Ltd Ibadan).

Lipschuty, S. (2004). Schaum's Outlines Series on Set Theory and Related Topics. MAcGraw – Hill, NY.

Osisiogu, U. A. (1998). An Introduction to Real Analysis with Special Topic on Functions of Several Variables and Method of Languages Multipliers, Bestsoft Educational Books Nigeria.