
# NATIONAL OPEN UNIVERSITY OF NIGERIA

## COURSE CODE : MTH 211

## COURSE TITLE: SET THEORY AND ABSTRACT ALGEBRA

**COURSE GUIDE**

# MTH 211
# SET THEORY AND ABSTRACT ALGEBRA


Adapted from Indira Gandhi National Open University

Course Team Dr. Bankole Abiola (Developer) - NOUN
Dr. Sunday Reju (Programme Leader) - NOUN
Bankole Abiola (Coordinator) - NOUN


**NATIONAL OPEN UNIVERSITY OF NIGERIA**

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

E-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published By:
National Open University of Nigeria

First Printed 2009

ISBN: 978-058-643-1



Printed by:

**CONTENTS** **PAGES**

## Introduction

You are welcome to Set Theory and Abstract Algebra. This course is a 3-credit course and it is offered at the undergraduate level.

This course consists of 2-modules of 4 units each. The prerequisite for this course is MTH131 – Elementary Set Theory.
This Course Guide tells you briefly what the course is all about, what materials you will be using and how you can walk your way through these materials.

## What You Will Learn in This Course

Set Theory and Abstract Algebra is course that is compulsory for all B.Sc (Hons) Mathematics students, Computer Science Students and Communications Technology Students. All Students in Education Majoring in Mathematics as teaching subjects are required to pass this course. This text is an informal axiomatic treatment of Set Theory and Abstract Algebra.

The text contains expository treatment of fundamentals of Algebras. Topics such as Sets and Functions, Groups Subgroups Lagrange's Theorem, Polynomial Rings, Special Integral Domains and Irreducibility and Field Extensions are given expository treatments.

Each unit begins with clear statements of pertinent definitions principles and relevant theorems, and further illustrated with some graded and solved problems. The supplementary exercises are meant to illustrate the work further.

## Course Aims

The aim of the course can be summarized as follows:

- To introduce you to concept of Algebra at the University Level
- To expose you to idea of groups theory , subgroups and the relevant theorems on groups
- To prepare you rigorously for more advance courses in algebra

## Course Objectives

Set out below are the wider objectives of the course as a whole. On successful completion of this course you should be able to:

- Explain the meaning of Groups ,Subgroups, Polynomial Rings Integral Domain, Irreducibility and Field Extensions

- Be able to give examples of groups subgroups, polynomial rings
- Solve related problems concerning these topics.

## Working through this Course

To complete this course, you are required to read the study units, read the recommended textbooks and other materials provided by the NOUN.

## Assignment File

The assignment File contains details of the work you must submit to your tutor for marking. It contains a more compact form of the Tutor-marked

## Assessment

There are two aspects of the assessment of the course. First are the tutor-marked assignments; second there is a written examination. In tackling the assignments, you are expected to apply information, knowledge and techniques gathered during the course. The assignments must be submitted to your tutor for formal assessment in accordance with the stipulated deadlines.

## How to Get the Most from the Course

In distance learning, the study units replace the lecturer. This is an advantage over the conventional mode of learning; because it affords the opportunity of reading and working through all the specially designed materials at your pace, at a time and place that suit you best. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and the course as a whole. Next is a set of learning objectives. These objectives let you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the unit you must go back and check whether you have achieved the objectives. If you make a habit of doing this you will significantly improve your chances of passing the course.

Exercises are interspersed within the units, and answers are given. Working through these exercises will help you to achieve the objectives of the unit and help you to prepare for the assignments and examination.

The following is a practical strategy for working through the course.

1) Read this Course Guide thoroughly.

2) Organize a study schedule

3) Once you have created your own study schedule, do everything you can to stick to it.

4) Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow.

5) Review the objectives for each study unit to confirm that you have achieved a unit's objectives; you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

6) When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments.

| | |
|---|---|
| Course Code | MTH 211 |
| Course Title | Set Theory and Abstract Algebra |
| Adapted from | Indra Gandhi National Open University |
| Course Team | Dr. Bankole Abiola (Developer) - NOUN<br>Dr. Sunday Reju (Programme Leader) - NOUN<br>Bankole Abiola (Coordinator) - NOUN |


**NATIONAL OPEN UNIVERSITY OF NIGERIA**

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

E-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published By:
National Open University of Nigeria

First Printed 2009

ISBN: 978-058-643-1



Printed by:

**CONTENTS** **PAGES**

# 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 $\phi$ (phi). For example, the set of all natural numbers less than 1 is $\phi$.

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. S0 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 $r\frac{1}{2}$ 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

$Z = \{x \mid x \text{ is an integer}\}$.

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 = $\{a+ib \mid a, b \in R\}$. (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 $\mathbf{B} \subseteq \mathbf{A}$.

for every set A, $\mathbf{A} \subseteq \mathbf{A}$.

Also, for any set A, $\phi \subseteq \mathbf{A}$.

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 '$\exists$' $x \ni B$ 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** $\mathbf{A \subseteq B}$ **and** $\mathbf{B \subseteq A}$.

**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 $x \in A \Rightarrow x \in B$

**SELF ASSESSMENT EXERCISE 2**

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

Then show that:

a. $A \cup B \not\subseteq C$
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 $A_1 \bigcup A_2 \bigcup \ldots\ldots \bigcup A_k$ 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 $\phi$ , 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 $\bigcup_{i=1}^{k} A_i$.

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, $\{x \in X \mid x \in A \text{ and } x \in B\}$.

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. $(A^c) = A$.

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. $A \times B = \phi$ if $A = \phi$ or $B = \phi$.

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 $A_1, A_2, A_3 \ldots\ldots A_n$ 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

$\mathbf{R} \times \mathbf{R} = \{(a_1, a_2) \mid a_{1,} \in \mathbf{R}, a_2 \in \mathbf{R}\}$
$\mathbf{R} \times \mathbf{R} \times \mathbf{R} = \{(a_1, a_2, a_3) \quad a_{1,} \in \mathbf{R}$, for 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 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 $\{(a, a^2) \mid a \in N\}$. 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 into 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 **∀** 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 **∀** 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 x 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 | 1Rn, n $\in$ **N**}
= { n | n $\in$ N and 5 divides 1-n}
= { n | n $\in$ N and 5 divides n-1}
= {1, 6, 11, 16, 21 ...},

Similarly,

[2] = { n | n $\in$ N and 5 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).

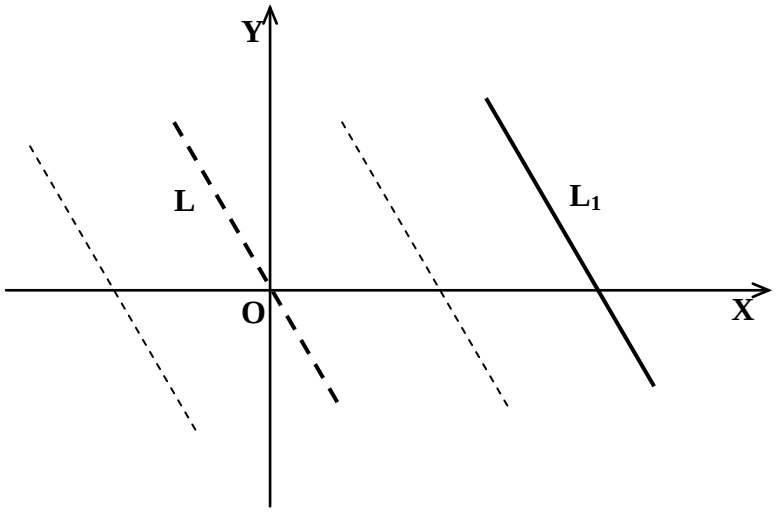


**Fig. 1: The equivalence class of $L_1$**

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-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-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 $\pi_1$: A x B $\rightarrow$ A: $\pi_1$ ((a, b)) = a. $\pi_1$ is called the **projection** of A x B onto A. You can see that the range of $\pi_1$ is the whole of A. Therefore, $\pi_1$ is onto. Similarly, $\pi_2$: A x B $\rightarrow$ B: $p_2((a, b)) = b$, the projection of A x B onto B, is a surjective function.

If a function is both one-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 $\phi$ is assumed to be finite.
Try the following self assessment exercise now.

**SELF ASSESSMENT EXERCISE 14**

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

**SELF ASSESSMENT EXERCISE 15**

Let f: $Z \to Z$ 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: $A \to B$: $f(a) = c$, where c is a fixed element of B.

**SELF ASSESSMENT EXERCISE 16**

What must X be like for the constant function f: $X \to \{c\}$ 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: $A \to B$ 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 $g \circ f \neq f \circ g(1)$.)

**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 $f: A \to A$, 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 $g: B \to A$, 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 $f: A \to B$ be a given function. If there exists a function $g: B \to A$ 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 $f: R \to R$ defined by $f(x) = x + 3$. If we define $g: R \to R$ 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: $\mathbf{R} \to \mathbf{R}$ 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, $f \circ g(x) = 3(g(x)) + 5 = \left[\frac{(x - 5}{3}\right] + 5 = x$ $\forall x \in \mathbf{R}$.

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: $\mathbf{R} \to \mathbf{R}$: $f(x) = \frac{x}{3}$?

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

**Example 7**

Let f: $\mathbf{R} \to \mathbf{R}$, 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: $\mathbf{R} \to \mathbf{R}$, 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 $\forall\ \mathbf{R}$ x. 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 $\to$ 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) | 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. $f(x) = x^2$ **V** x $\in$ **R**.
b. f(x) = 0 **V** x $\in$ **R**.
c. f(x) = 11x + 7 **V** x $\in$ **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 $a \leq b$ **∀** $x \in S$. 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 $S_n = 1^3 + \ldots\ldots\ldots\ldots\ldots + n^3$, 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 $S_n = 1^3 + \ldots\ldots\ldots\ldots\ldots + (n-1)^3 + n^3$

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

$= \frac{(n-1)^2 n^2}{4} + n^3$, 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 | 0, ± 1 | a, ± a | a.
b. a | b $\Rightarrow$ ac | bc.
c. a | b and b | c $\Rightarrow$ a | c.
d. a | b and b | a $\Leftrightarrow$ a = ± b.
e. c | a and c | b $\Rightarrow$ c | (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 Ï 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., $(n - 1) = q_1b + r_1$ 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,

$$n = \begin{cases} q_1b + (r_1 + 1), \text{if } (r_1 + 1) < b \\ (q_1 + 1)b + 0, \text{if } r_1 + 1 = b \end{cases}$$

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 $d \mid d'$ and $d' \mid d$. Thus, $d = \pm d'$ (**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 $S = \{xa + yb \mid x, y \in Z, (xa + yb) > 0\}$.

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
$a = qd + r$, $0 £ r < d$. 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 $\nmid$ 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 $a_i$ 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 $n = p_1^{m_1}\, p_2^{m_2} \ldots\ldots p_r^{m_r}$, 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 $\in$ I 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 $\in$ **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 $x \in A$ Ü $x \in B \cup A$. $\therefore A \cup B = B \cup A$.

c. $x \in A \cup \phi \Rightarrow x \in A$ or $x \in \phi \Rightarrow x \in A$, since $\phi$ 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**

$$\begin{aligned}(x, y) \in (A \cup B) \times C &\Leftrightarrow x \in A \cup B \text{ and } y \in C \\ &\Leftrightarrow x \in A \text{ or } x \in B \text{ and } y \in C \\ &\Leftrightarrow x \in A \text{ and } y \in C \text{ or } x \in B \text{ and } y \in C \\ &\Leftrightarrow (x, y) \in A \times C \text{ or } (x, y) \in B \times C \\ &\Leftrightarrow (x, y) \in (A \times C) \cup (B \times C).\end{aligned}$$

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 | (a – b), then 5 | (b – a). $\therefore$, R is symmetric.
If 5 | (a – b), then 5 | (b – c), then 5 | {(a – b) + (b – c)}, i.e.
5 | (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**

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

**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.
$f^{-1}: \mathbf{R} \to \mathbf{R} : f^{-1}(x) = \dfrac{x - 7}{11}$.

**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 | 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

Birkhaffand Melhnew (1972). *A Survey of Modern Algebra.*

Blacksell: Topics in Algebra.

# 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. these 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 $\Delta$ 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 $a \times b$ 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 ï 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) **V** 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 = bc + ba **V** 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 **V** 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 $a * b = \frac{a + b}{2}$ **V** a, b $\in$ **R**. Then $a(b * c) = a\left(\frac{b + c}{2}\right) = \frac{ab + ac}{2} = ab * ac$, and

$(b * c)a = \left(\frac{b + c}{2}\right)a = \frac{ba + ca}{2} = ba * ca$ **V** 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.
$= e'$, 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 x R $\rightarrow$ 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 **V** a $\in$ R. So we want e $\in$ R such that a + e – 1 = a **V** a $\in$ R. Obviously, e = 1 will satisfy this. Also, 1 $\oplus$ a = a **V**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 **V** 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 $\phi$ 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.

Fig. 1 : Arthur Cayl

| | -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 |

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 $a_1 * \ldots\ldots\ldots * a_k$ 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

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

Then

$(a_1 * \ldots\ldots * a_m) * (a_{m+1} * \ldots\ldots * a_{m+n})$
$= (a_1 * \ldots\ldots * a_m) * ((a_{m+1} * \ldots\ldots * a_{m+n-1}) * a_{m+n})$
$= ((a_1 * \ldots\ldots * a_m) * (a_{m+1} * \ldots\ldots * a_{m+n-1})) * a_{m+n}$, since $*$ is associative
$= (a_1 * \ldots\ldots * a_{m+n-1}) * a_{m+n}$, by induction
$= (a_1 * \ldots\ldots * a_{m+n}$, 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 (**Z**, +) is a group, but (**Z**,) is not.

**Solution**

+ is an associative binary operation on **Z**. the identity element with respect to + is 0, and the inverse of nay $n \in$ **Z** is **(-n)**. Thus, (**Z**, +) satisfies G1, G2 and G3.

Therefore, it is a group.

Now, multiplication in **Z** is associative and $1 \in$ **Z** is the multiplicative identity. But does every element in **Z** have a multiplicative? 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 $a * e = a$ **V** $a \in G$.
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 $a.1 = a$ **V** $a \in G$. Therefore, 1 is the identity element. It also shows us that $(G, \cdot)$ satisfies G3'. Therefore, $(G, \cdot)$ is a group.

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

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

Note that the group in Example 4 has only 4 elements, while those in Example 3 and 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 ´ 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,

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

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 $(G, \cdot)$ 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, $(ab)^{-1} = a^{-1} b^{-1}$ ~~V~~ $a, b \in G$ 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 $GL_2(\mathbf{R})$ (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** $\Delta$, 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**

$\Delta$ 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. $\Delta$ is also commutative since $A \Delta B = B \Delta A$ $\forall$ $A, B \in \wp(S)$.

Also, $\phi$ 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 $\wp$A(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 ∈ **Z**?

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

**Definition**

Let G be a group. For a ∈ 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 ∈ 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 ∈ G and m, n ∈ 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 **$a \equiv b$ (mod n)**. For example, $4 \equiv 1$ (mod n 3), since $3 \mid (4 - 1)$.

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

$\equiv$ 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 $\overline{r}$.

Thus, $\overline{r} = \{m \in Z \mid m \equiv r(\text{mod } n)\}$.

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

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

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

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

Let $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{n-1}\}$. We define the operation + on $Z_n$ by $\overline{a} + \overline{b} = \overline{a+b}$.

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

| + | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | | | | |
| $\overline{1}$ | | | | |
| $\overline{2}$ | | | | |
| $\overline{3}$ | | | | |

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, $\overline{2} + \overline{2} = \overline{0}$ 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. $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$ ∀ $\overline{a}, \overline{b} \in Z_n$, i.e., addition is commutative in $Z_n$.

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

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

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

Thus, every element $\overline{a}$ 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 $\overline{a}.\overline{b} = \overline{ab}$. Then, $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$ ∀ $\overline{a}, \overline{b} \in \mathbf{Z}_n$. Also $(\overline{a}\,\overline{b})\overline{c} = \overline{a}(\overline{b}\,\overline{c})$ ∀ $\overline{a}, \overline{b}, \overline{c} \in Z_n$. Thus, multiplication in $\mathbf{Z}_n$ is a commutative and associative binary operation.

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

But $(\mathbf{Z}_n,.)$ is not a group. This is because every element of $\mathbf{Z}_n$, for example $\overline{0}$ 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 $Z_4^* = \{\overline{1}, \overline{2}, \overline{3}\}$ is not a group because . is not even a binary operation on $Z_4^*$, since $\overline{2}.\overline{2} = \overline{0} \notin Z_4^*$. 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 $(f _o g) _o h = f(g _o h)$ ∀ f, g, h ∈S(X).
ii. $I_x$ is the identity element because $f _o I_x = I_x _o f$ ∀ $f \in S(X)$.
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 $S_n$ is called a **permutation on n symbols**.

Suppose we want to construct an element f in $S_n$. We can start by choosing f(1). Now, f(1) can be any one of the n symbols 1, 2, ….,n. Having chosen f(1), we can choose f(2) from the set {1, 2, ….n}\{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

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

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

{1, 2, 3, 4} → {1, 2, 3, 4}: f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1. the elements in the top row can be 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 $x_1$……., $x_r$ 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 ($x_i$ …$x_r$),
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-1b-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

- discussed various types of binary operations.
- defined and give examples of groups.

- proved and used the cancellation laws and laws of indices for group elements.
- 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. $x \oplus y = y \oplus x$, $\forall\ x, y \in$
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. $\Delta$ 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 $x * e = e * x = x$ $\forall\ x \in$ **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 | $\phi$ | {0} | {1} | S |
|---|---|---|---|---|
| $\phi$ | $\phi$ | $\phi$ | $\phi$ | {1} |

| | | | | |
|---|---|---|---|---|
| {0} | $\phi$ | {0} | $\phi$ | {0} |
| {1} | $\phi$ | $\phi$ | {1} | {1} |
| S | $\phi$ | {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 $\in$ **Z,** a – (a – b) = b. So, a – x has a solution for any a, b $\in$ **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 $\in$ **Z**.

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

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

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

**ANSWER TO SELF ASSESSMENT EXERCISE 11**

| + | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |

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

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

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

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 + 2nπ is also an argument of z for all n ∈ **Z**,. However, there is a unique value of these arguments which lies in the interval [-π,π]. 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 = sinθ = 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 $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, then
$z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$.

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

We can similarly show that if $z_2 \neq 0$,

**An argument of $\frac{z_1}{z_2}$ = an argument of $z_1$ – an argument of $z_2$.**

In particular, if $\theta$ is an argument of $z$ ($\neq 0$), then $(-\theta)$ is an argument of $z^-$
We end by stating one of the important theorems that deals with complex numbers.

**De Moivre's Theorem:** If $z = r(\cos\theta + i \sin\theta)$ and $n \in N$, then $z^n = 1^n (\cos n\theta + i \sin n\theta)$.

## 7.0 REFERENCES/FURTHER READING

Birkhaff and Melhnew: *A Survey of Modern Algebra.*

# 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 o! (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
$a, b \in H \Rightarrow ab^{-1} \in H$.

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

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

**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

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

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

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

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

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

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

**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 $SL_3(\mathbf{R})$. Therefore, $SL3(\mathbf{R}) \neq \phi$.

Now, for $A, B \in SL_3(\mathbf{R})$.

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

$\therefore AB^{-1} \in SL_3(\mathbf{R})$

$\therefore SL_3(\mathbf{R}) \leq GL_3(\mathbf{R})$.

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 mZ**.

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 **Z** $\subseteq$ H. Why? Well, consider any element st$\in$ s**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 **V** 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 $\in$ **H**. Thus, r $\in$ H. By minimality of sin S, we must have r = 0, i.e., m = ns. Thus, H $\subseteq$s**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 $\in$ **C is z** = r(cosθ + i sinθ), where r = |z| and θ ia an argument of z. Moreover, if $\theta_1$ is an argument of $z_1$ and $\theta_2$ 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 nθ+ i sin nθ), that is,
cos (θ) + i sin(θ) = $r^n$ (cos nθ) + i sin nθ). …….. (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 + 2πk (k $\in$ **Z**) and nθ are arguments of the same complex number. Thus, nθ can take any one of the values 2πk, k $\in$ **Z**. Does this mean that as k ranges over Z and θ ranges over $\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} = \cos\frac{2\pi m}{n} + i \sin\frac{2\pi m}{n}$ 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 $\leq$ 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 $z_j$, $\frac{2\pi j}{6} + i\sin\frac{2\pi j}{6}$, j1, 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.

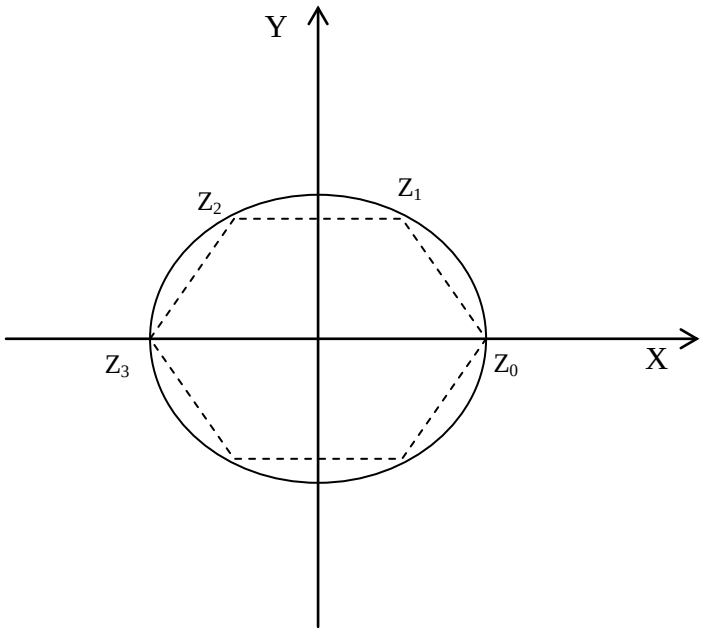


**Fig. 1: $6^{th}$ Roots of Unity**

Now, let $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Then all the nth roots of 1 are 1, $\omega$, $\omega^2$, ……., $\omega^{n-1}$, 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, $\omega^{n-1}$. 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., $\omega^{n-1}$ is the inverse of $\omega^1$ 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 $Z(G) = \{g \in G \mid xg = gx \ \forall\ x \in G.\}$.

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,

$a \in Z(G) \quad \Rightarrow ax \ \forall\ x \in G.$
$\Rightarrow x = a^{-1} xa \ \forall\ x \in G$, 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 $ab^{-1} \in K$ ∀ a, b ∈ 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 ∈ 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 $m\mathbf{Z} \subseteq k\mathbf{Z} \Leftrightarrow k \mid m$. Now $m\mathbf{Z} \subseteq k\mathbf{Z} \Leftrightarrow m \in m\mathbf{Z} \subseteq k\mathbf{Z} \Rightarrow m \in k\mathbf{Z} \Rightarrow m = kr$ for some $r \in \mathbf{Z}$ 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, $ab^{-1} \in$ K. 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**Z** and 3**Z** of **Z**. Let S = 2**Z** $\cup$ 3**Z**. Now, 3 $\in$ 3**Z** $\subseteq$ S, 2 $\in$ 2Z $\subseteq$ S, but 1 = 3 – 2 is neither in 2**Z** nor in 3**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 $a \in A \setminus B$ and $e \in B \setminus A$. 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 **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 $HK = \{I \circ I, I \circ (1\ 3), (1\ 2) \circ I, (1\ 2) \circ (1\ 3)\}$
$= \{I, (1\ 3), (1\ 2), (1\ 3\ 2)\}$

HK is not a subgroup of G, since it is not even closed under composition. (Note that $(1\ 3) \circ (1\ 2) = (1.\ 2\ 3) \notin HK$.)

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

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

Hence, we have shown that HK = KH.

Conversely, assume that HK = KH. We have to prove that HK $\leq$ G. Since $e = e^2 \in$ HK, HK $\neq \phi$.
Now, let a, b $\in$ HK. Then a = hk and $b = h_1 k_l$ for some h, $h_1 \in$ H and 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, $\exists$ $h_2k_2 \in$ 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 $\leq$ 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, $<S> = \cap \{H \mid H \leq G, S \not\subset H\}$.
If $S = \phi$, then $<S> = \{e\}$.
If $<S> = G$, 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

$<S> = \{a_1^{n_1} a_2^{n_2} .....a_k^{n_k} \mid a_i \in S for\ 1\ \ i\ \ k, n_1, \ldots\ldots, n_k\ \ Z.\}$

**Proof**

Let $A = \{a_1^{n_1} a_2^{n_2} .....a_k^{n_k} \mid a_i \in S for\ 1\ \ i\ \ k, n_1, \ldots\ldots, n_k\ \ Z.\}$
Since $a_1 \ldots\ldots, a_k \in S \subseteq <S>$ 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 $x = (a_1^{n_1} a_2^{n_2} .....a_k^{n_k})\ (b_1^{m_1} b_2^{m_2} .....b_r^{m_r})^{-1} 1$

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

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 $n_1 a_1 + n_2 a_2 + \ldots\ldots\ldots n_r a_r$, where $a_1, a_2 \ldots, a_r \in S$ and $n_1, n_2 n_r \in Z$.

For example, Z is generated by the set of odd integers $S = \{\pm 1, \pm 3, \pm 5, \ldots.\}$. 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
$S_1 \ldots..$ , $S_k$ in Sand $n_l$, ….. $n_k$ in Z such that $n_1 s_1 + \ldots...+ n_k s_k = 1$.

(**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 $G = < \{a\} >$ for some $a \in G$. We usually write $< \{a\} >$ as $< \mathbf{a} >$.

Note that $< a > = \{a^n \mid n \in Z\}$.

A subgroup H of a group G is called a **cyclic subgroup** if it is a cyclic group. Thus, < (12) > is a cyclic subgroup of $S_3$ and 2Z = <2> 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 <a> $\subseteq$K. This is because <a> is the smallest subgroup of G containing

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

Then < (1 2)> = {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 $G \neq < e >$.

**SELF ASSESSMENT EXERCISE 12**

Show that <a> = <a-1> 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, $n \in \mathbf{Z}$ 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, $r \in Z$, $0 \leq r \leq k$-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 $H \neq \{e\}$ 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.

- The definition and examples of subgroups.
- The intersection of subgroups is a subgroup.
- The union of two subgroups H and K is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.
- The product of two subgroups H and K is a subgroup if and only if HK = KH.

- The definition of a generating set.
- A cyclic group is abelian, but the converse need not be true.
- 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. $\{e\} \neq$ . Also for any e $e^{-1} = e \in \{e\}$ ….., by Theorem 1, $\{e\} \leq G$.
$G \leq \phi$. Also for any $x \in G$, $x^{-1} \in G$. ∴, for a, $b \in G$.
A, b e G ∴ $ab^{-1}$ e G. ∴ $G \leq G$.

**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 $A \bigcup B$ 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 $A \bigcup B \nleqslant G$.
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, $(1\ 2) \circ (14) = (142) \notin AB$. $\therefore AB \nleq S_4$

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

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

**ANSWER TO SELF ASSESSMENT EXERCISE 10**

We know that $G = < S >$. Therefore, for any $g \in G$,
$\exists\ s_1\ldots\ldots,s_k \in S$ and $n_1,\ldots.., n_k \in Z$ such that $g = s_1^{n_1} \ldots\ldots\ldots s_k^{n_k} m$
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 READING

Blacksell: *Topics in Algebra*.

Birkhaffand Melhew (1972). *Survey of Modern Algebra.*

# 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 | h E H} a **right coset** of H in G. The element x is a **representative of Hx**.

We can similarly define the left coset

xH {xh | h E 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 | h∈ H} and x + H = { x + h | h∈ 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 | h∈ H} = {h | h ∈ 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,….. }

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

Similarly, you can 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) ◦ (1 2 3), (1 2) ◦ (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 Hare 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

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & i \\ 0 & -i \end{bmatrix}$, $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ 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~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 ~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 $\{x | = \{y \in G | y - x\} = \{y \in G | xy^{-1} \in H\}$.

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∩Hy = ϕ.

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} **V** 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 $| Hx_1 | = | Hx_2 | - - | Hx_r | = o(H)$.

Fig 1: Joseph Louis Lagrange (1736 –1813)

Thus the total number of elements in the union on the right hand (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 d obtaining all the subgroup of a finite group.

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 $g \in G$. 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-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 gm = e for some m $\in$**N** iff n | m.

**Proof**

We will first show that $g^m$ e $\Rightarrow$ n | 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-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 $o(\overline{4})$, 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= $\overline{2}, \overline{4},$ 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 $\bar{r}\,\bar{s} = \overline{rs}$ ∀ $\bar{r}, \bar{s} \in Z_n$. 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 | ar
$\Rightarrow$ ar = 1 (mod 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 $= 1 \pmod{p}$. (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.

- The definition and examples of right and left cosets of a subgroup.
- Two left (right) cosets of a subgroup are disjoint or identical.
- Any subgroup partitions a group into disjoint left (or right) cosets of the subgroup.

- The definition of the order of a group and the order of an element of a group
- 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.
- 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 $ab^{-1} \in K$ ~~V~~ 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 defied 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. $\overline{3} \neq \overline{0}, 2\overline{2} = \overline{6} = \overline{2}, 3\overline{3} = \overline{9} = \overline{1}, 4\overline{3} = \overline{12} = \overline{0}, \because o(\overline{3}) = 4.$
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

$o(\bar{r}) = o(r, \overline{1}) = \dfrac{18}{(18, r)}$, for any $\bar{r} \in \mathbf{Z}_{18}$

$\therefore o(\overline{2}) = 9, o(\overline{4}) = 9, o(\overline{5}) = 18.$

**ANSWER TO SELF ASSESSMENT EXERCISE 8**

Since o(x) = o(< x >) and o(< x >) | o(G), o(x) | o(G).
Thus, using Theorem 4, $x^{o(G)} = e$.

**ANSWER TO SELF ASSESSMENT EXERCISE 9**

$o(Z_8) = 8 = 2 \times 4.$
$\overline{2} \in Z_8$ such that $o(\overline{2}) = 4.$ Then $< \overline{2} > < Z_8$.
Similarly, $\overline{4} \in Z_8$ such that $o(\overline{4}) = 2. \therefore < \overline{4} > <$ $\mathbf{Z}_8$.

**ANSWER TO SELF ASSESSMENT EXERCISE 10**

We know that in $Z_{23}$, $(\overline{3})^{\phi(23)} = \overline{1}$,
that is, $3^{22} = \overline{1}$. $\therefore 3^{44} = \overline{1}$
$\therefore 3^{47} = 3^{-3,} 3^{44} = \overline{3}^{-3,} = \overline{27}$
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 READING

Blacksell: *Topics in Algebra*.

## MODULE 2



## UNIT 1 THE BASICS

### CONTENTS



## 1.0 INTRODUCTION

We are considering in this unit a special ring, whose specialties lay in the property of their multiplication. We shall examine a type of ring called Integral Domain. In MTH 312 we shall examine Rings into details and also examine their mathematical structures.

Next, we will look at rings like Q, R, C, and $Z_p$ (where p is a prime number). In these rings the non-zero elements form an abelian group under multiplication. Such rings are called fields. These structures are very useful, one reason being that we can “divide” in them.

Related to integral domains and fields are certain special ideals called prime ideals and maximal ideals. In this unit we will also discuss them and their corresponding quotient rings.

Finally, we shall see how to construct the smallest field that contains a given integral domain. This is essentially the way that Q is constructed from Z. we call such a field the field of quotients of the corresponding integral domain.

In this unit, we have tried to introduce you to a lot of new concepts. You may need some time to grasp them. Don't worry; take as much time as you need. But by the time you finish it, make sure that you have attained the following objectives. Only then will you be comfortable in the remaining units of this course.

## 2.0 OBJECTIVES

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

- check whether an algebraic system is an integral domain or not
- obtain the characteristic of any ring
- check whether an algebraic system is a field or not
- define and identify prime ideals and maximal ideals
- prove and use simple properties of integral domains and fields
- construct or identify the field of quotients of an integral domain.

## 3.0 MAIN CONTENT

### 3.1 Integral Domains

You know that the product of two non-zero integers is a non-zero integer, i.e., if m, n $\in$ Z such that m = 0, n $\neq$ 0, then mn $\neq$ 0. Now consider the ring $Z_6$. We find that $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$, yet $\bar{2}.\bar{0} = \bar{0}$. So, we find that the product of the non-zero elements $\bar{2}$ and $\bar{3}$ in $Z_6$ is zero. As you will soon realize, this shows that $\bar{2}$ (and $\bar{3}$) is a zero divisor, i.e., $\bar{0}$ is divisible by $\bar{2}$ (and $\bar{3}$).

So, let us see what a zero divisor s.

**Definition**

A non-zero element in a ring R is called a zero divisor in R if there exists a non-zero element b in R such that ab = 0

(Note that b will be a zero divisor~ too!)

Now do you agree that $\bar{2}$ is a zero divisor in $Z_6$? What about $\bar{3}$ in $Z_4$? Since $\bar{3}$ x $\neq \bar{0}$ for every non-zero x in $Z_4$, $\bar{3}$ is not a zero divisor in $Z_4$.

Our short discussion may help you to do the following exercise.

*E 1) Let n e N and m | n, 1 < m < n. Then show that $\bar{m}$ is a zero divisor in $Z_n$.*

Now let us look at an example of a zero divisor m C[0,1]. Consider the function f $\in$ C[0,1] given by f(x) =

$$f(x)=\begin{cases} x-\frac{1}{2}, 0\le x\le 1/2 \\ 0, 1/2\le x\le 1 \end{cases}$$

Let us define g: [0,1] '-) R by

$$g(x)=\begin{cases} 0, 0\le x\le 1/2 \\ x-1/2, 1/2\le x\le 1 \end{cases}$$

Then g$\in$ C[0.l], g ≠ 0 and (fg) (x) = 0 $\forall x\in$ [0,l], Thus, fg is the zero function. Hence, f is a zero divisor in C[0,1].

For another example, consider the Cartesian product of two non-trivial rings A and B. For every a ≠ 0 in A. (a.0) is a zero divisor in A x B, This is because, for any b ≠ 0 in B, (a.0) (0.b) = (0.0)

Now let us look al the ring $\wp$(X), where X is a set with at least two elements. Each non empty proper subset A of X is a zero divisor because A.$A^c$ = A$\cap A^c = \phi$, the zero element of $\wp$(X).

Try these exercises now.

E 2) List all the zero divisors m Z.

E 3) For Which rings with unity will I be a zero divisor?

E 4) Let R be a ring and a $\in$R be a zero divisor. Then show that every element of the principal deal Ra is a zero divisor.

Let us now talk of a type of ring that is without zero divisors.

**Definition**

We call a non-zero ring R an **integral domain** if

i) R is with identity and
ii) R has no Zero divisors.

Thus, an integral domain is a non-zero ring with identity in which the product of two non-zero elements.
This kind of ring gets its name from the set of integer, one of its best known examples. Other examples of domains that immediately come to mind are **Q.R** and **C**. What about C[01,]? You have already seen that it has zero divisors. Thus C[0.1] is not a domain

The next result gives us an important class of examples of integral domains

**Theorem 1**

Zp is an integral domain iff p is a prime number,

**Proof**

Firstly, let us assume that p is a prime number. Then you know that $Z_p$ is a non-zero ring with identity. Let us see if it has zero divisors/ for this, suppose $\bar{a},\bar{b}\in Z_p$ satisfy $\bar{a},\bar{b}=\bar{0}$ then $a\bar{b}=\bar{0}$, i.e., p | ab. Since p is a prime number, using E 25 of Unit 1 we see that p | a or p | b. Thus, a = $\bar{a}=\bar{0}$ $or\bar{b}=\bar{0}$. What we have shown is that if $\bar{a}\neq\bar{0}$ and $\bar{b}\neq\bar{0}$, then $\bar{a}\bar{b}\neq\bar{0}$. Thus, $Z_p$ is the trivial ring, which is not a domain.

Conversely, we will show that if p is not a prime, then $Z_p$ is not a domain. So, suppose p is not a prime. If p = 1, then $Z_p$ is the trivial ring, which is not a domain.

If p is a composite number and m | p, then by E 1 you know that $\bar{m}\in Z_p$ is a zero divisor. Thus, Zp has zero divisors. Hence, it is not a domain.

Try this exercise now

E 5) Which of the following rings are not domains? Why?
$Z_4$, $Z_5$, 2Z, Z + iZ, R x R, {0}

Now consider a ring R. we know that the cancellation law for addition holds in R, i.e whether a+b = a+c in R, then b = c. But, does ab = ac imply b = c? it need not. For example, o.1 = 0.2 in Z but $1\neq 2$. So, if a = 0, ab = ac need not imply b = c. But, if $a\neq 0$ and ab = ac, is it true that b = c? We will prove that this is true for integral domains.

**Theorem 2**

A ring R has no zero divisors if and only if the cancellation law for multiplication holds in R (i.e., if a,b,c$\in$ R such that a $\neq 0$, and ab = ac, then b = c)

**Proof**

Let us first assume that R contains no zero divisors. Assume that a,b,c$\in$R such that a$\neq$0. Suppose ab = 0 for some b$\in$R. Then ab = 0 = a0. Using the cancellation law for multiplication, we get b = 0. So, a is not a zero divisor, i.e., R has no zero divisors.

Using this theorem we can immediately say that the cancellation aw holds for multiplication in an integral domain.

Now, you can use this property of domains to solve the following exercises.

E 6) In a domain, show that the only solutions of the equation $x^2 = x$ are x = 0 and x = 1.

E 7) Prove that 0 is the only nilpotent element (see Example 9 of Unit 10) in a domain.

Now let us introduce a number associated with an integral domain, in fact, with any ring. For this let us look at $Z_4$ first. We known that 4x = $\bar{0} \forall x \in Z_4$. In fact, 8x = $\bar{0}$ and 12 x = $\bar{0}$ also for any x $\in Z_4$.

But 4 is the least element of the set $\{n \in N \mid nx = \bar{0} \forall x \in Z_4\}$. This shows that 4 is the characteristics pf $Z_4$ as you will see now.

**Definition**

Let R be a ring. The least positive integer n such that nx = $0 \forall x \in$ R is called the characteristic of R. If there is no positive integer n such that nx= $0 \forall x \in$ R, then we say that the characteristic of R is zero.

We denote the characteristic of the ring R by char R.

You can see that char $Z_n$ = n and char Z = 0.

The following exercises will give you some practice in obtaining the characteristic of a ring.

E 8) Show that char $\wp(X) = 2$, where X is a non empty set.

E 9) Let R be a ring and char R = m. What is char (R x R)

Now let us look at a nice result for integral domains. It helps in considerably reducing our labour when we want to obtain the characteristic of a domain.

**Theorem 3**

Let m be a positive integer and R be an integral domain. Then the following conditions are equivalent.

a) m 1 = 0.
b) ma = 0 for all a $\in$ R.
c) ma = 0 for some a $\neq$ in R.

**Proof**

We will prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).
(a) $\Rightarrow$ (b): We know that m l = 0.

Thus, for any a $\in$ R, ma = (la) ={ml) (a) = 0a = 0, i.e., (b) holds.

(b) $\Rightarrow$ (c): If ma = 0 a $0\forall\ a \in$ R, then it is certainly true for some a $\neq$ 0 in R.

(c) $\Rightarrow$ (a) : Let mil = 0 for some a $\neq$ 0 in R. Then 0 = ma = m (1a) = (m.) a. As a $\neq$ 0 and R is without zero divisors, we get m1 = 0.

What Theorem 3'tells us is that **to find** the **characteristic of a domain we on1y need to look at the set {n,1 | n $\in$ N}.**

Let us look at some examples.

i) char Q=0, since n.1$\neq$0 for any n $\in$ N.
ii) Similarly, char R = 0 and char C = 0.
iii) You have already seen that char $Z_n$ = n. Thus, for any positive integer n, there exists a ring with characteristic n.

Now let us look at a peculiarly of the characteristic of a domain.

**Theorem 4**

The characteristic of an integral domain is either zero or a prime number.

**Proof**

Let R be a domain. We will prove that if the characteristic of R is not zero, then it is a prime number. So suppose char R = m, where $m \neq 0$. So m Iii the least positive integer such that m.1 = 0. We will show that m is a prime number by supposing that it is not, and then proving that our supposition is wrong.

So suppose m = st, where $s,t \in N$, $1 < s < m$ and $1 < t < m$. Then $m.1 = 0 \Rightarrow (st).\ l = 0 \Rightarrow (s.l)\ (t.1) = 0$. As R is without zero divisors, we get s.l = 0 or t.1 = 0. But, s and t are less than m. So, we reach a contradiction to the fact that m = char R. Therefore, our assumption that m = st, where $1 < s < m$, $1 < t < m$ is wrong. Thus, the only factors of m are 1 and itself. That is, m is a prime number.

You can now use your knowledge of characteristics to solve the following exercise

E 10) Let R be an integral domain of characteristic p. Pr0ve that

a) $(a+b)^p = a^p + b^p$ and
$(a-b)^p = a^p - b^p$ for all $a, b \in R$."

b) the subset $\{ a^p \mid a \in R\}$ is it subring of R.

c) the map $\Phi : R \to R : \Phi(a) = a^p$ is a ring homomorphism.

d) if R is a finite integral domain, then $\Phi$ is an isomorphism.

E 11) Let R be a ring with unity 1 and char R = m. Define $f: Z \to R$: f (n) = n.1. Show that f is a homomorphism. What is Kerf?

E 12) Find the characteristic of $Z_3 \times Z_4$. Use this ring as an example to show why Theorems 3 and 4 are only true for integral domains.

We will now see what algebraic structure we get after we impose certain restrictions on the multiplication of a domain. If you have gone through our course Linear Algebra, you will already be familiar with the algebraic system that we are going to discuss, namely, a field.

## 3.2 Field

Let (R, +,.) be a ring. We know that (R, +) is an abelian group. We also know that the operation is commutative and associative. But (R,.) is not an abelian group. Actually, even if R has identity, (R.,) will never be a group since there is no element $a \in R$ such that a.0 = 1. But can (R\{0}.,) be a group? It can, in some cases. For example, from Unit 2 you know that **Q*** and **R*** are groups with respect to multiplication. This allows us to say that **Q** and **R** are fields a term we will now define.

**Definition**

A ring (r, +.,) is called a **field** if (R\{0}.,) is an abelian group.

Thus, for a system (R, +.,) to be a field it must satisfy the ring axioms R1 to R6 as well as the following axioms.

i) is commutative,
ii) R has identity (which we denote by 1) and $1 \neq 0$, and
iii) every non-zero element x in R has a multiplicative inverse, which we denote by $x^{-1}$.

Just as a matter of information we would like to tell you that a ring that satisfies only (ii) and (iii) above, is called a **division ring** or a **shew field** or a **non-commutative field**. Such rings are very important in the study of algebra, but we will not be discussing them in this course.

Let us go back to fields now. The notion of a field evolved during the $19^{th}$ century through the research of the German mathematicians Richard Dedekind and Leopold Kronecker in algebraic number theory. Dedekind used the German word Korper, which assdfsdf field, for this concept. This is why you will often find that a field is denoted by K.

As you may have realized, two of the best known examples of fields are **R** and **C**. These were the fields that Dedekind considered. Yet another example of a field is the following ring.

**Example 1**

Show that $\mathbf{Q} + \sqrt{2Q} = \{a + \sqrt{2b} \mid a, b \in Q\}$ is a field.

**Solution**

From Unit 9 you know that F = Q + $\sqrt{2Q}$ is a commutative ring with identity 1 + $\sqrt{2.0.}$

$$(a+\sqrt{2b}) = \frac{1}{a+\sqrt{2b}} = \frac{2-\sqrt{2b}}{(a+\sqrt{2b})\,(a-\sqrt{2b})} = \frac{a-\sqrt{2b}}{a^2-2b^2}$$

$$= \frac{a}{2^2-2b^2} + \sqrt{2}\ \frac{(-b)}{2^2-2b^2} \in F$$

(Note that $a^2-2b^2 \neq 0$, since $\sqrt{2}$ is not rational and either $a \neq 0$ or $b \neq 0$.)

Thus, every non-zero element has a multiplicative inverse. Therefore, Q+$\sqrt{2}Q$ is a field.

Can you think of an example of a ring that is not a field? Does every non-zero integer have a multiplicative inverse in Z? No. Thus, Z is not a field.

By now you have seen several examples of fields. Have you observed that all of them happen to be integral domains also? This is not a coincidence. In fact, we have the following result.

**Theorem 5**

Every field is an integral domain.

**Proof**

Let F be a field. Then $F \neq \{0\}$ and $1 \in F$. we need to see if F has zero divisors. So let a and b be elements of F such that ab = 0 and $a \neq 0$ and F is a field, $a^{-1}$ exists. Hence, b =1.b = ($a^{-1}$a) b = $a^{-1}$ (ab) = $a^{-1}$ 0 = 0. Hence, if $a \neq 0$ and ab = 0, we get b = 0. i.e., F has no zero divisors. Thus, F is a domain.

Now you try these exercises!

E 13) Which of the following rings are not fields?
2Z, $Z_5$, $Z_6$, Q x Q

E 14) Will a subring of a field be a field? Why?

Theorem 5 may immediately prompt you to ask if every domain is a field. You have already seen that Z is a domain but not a field. But if we restrict ourselves to finite domains, we find that they are fields.

**Theorem 6**

Every finite integral domain is a field.

**Proof**

Let R = $\{a_0 = 0, 1_1 = 1, a_2\ldots\ldots,2_n\}$ be a finite domain. Then R is commutative also. To show that R is a field we must show that every non-zero element of R has a multiplicative inverse.

So, let $a = a_i$ be a non-zero element of R (i.e., $i \neq 0$). Consider the elements $aa_1,\ldots, aa_n$. For every $j \neq 0$, $aj \neq 0$; and since $a \neq 0$, we get $aaj \neq 0$.

Hence, the set $\{aa_1, aa_2\ldots..,aa_n\} \subseteq \{a_1,\ldots..,a_n\}$.

Also, aa1, aa2,…, $aa_n$ are all distinct elements of the set $\{a_1,\ldots..,a_n\}$, since $aaj = aa_k \Rightarrow aj = ak$, using the cancellation law for multiplication.

Thus, $\{aa_1,\ldots.,aa_n\} = \{a_1,\ldots.,a_n\}$.

In particular, $a_1 = aaj$, i.e., $1 = aaj$ for some j. thus, a is invertible in R. hence every non-zero element of R has a multiplicative inverse. Thus, R is a field.

Using this result we can now prove a theorem which generates several examples of finite fields.

**Theorem 7**

$Z_n$ is a field if and only if n is a prime number.

**Proof**

From Theorem 1 you know that $Z_n$ is a domain if and only if n us a prime number. You also know that $Z_n$ has only n elements. Now we can apply Theorem 6 to obtain the result.

Theorem 7 unleashes a load of examples of fields: $Z_2$, $Z_3$, $Z_5$, $Z_7$, and so on. Looking at these examples, and other examples of fields, can you say anything about the characteristic of a field? In fact. Using Theorems 4 and 5 we can say that.

**Theorem 8**

The characteristic of a field is either zero or a prime number.

So far the examples of finite fields that you have seen have consisted of p elements, for some prime p. In the following exercise we give you an example of a finite field for which this is not so.

E 15) Let R = {0,1,a,1+a}. Define + and in R as given in the following Cayley tables

| + | 0 | 1 | a | 1+a | | . | 0 | 1 | a | 1+a |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | a | 1+a | | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1+a | a | and | 1 | 0 | 1 | a | 1+a |
| a | a | 1+a | 0 | 1 | | a | 0 | a | 1+a | 1 |
| 1+a | 1+a | a | 1 | 0 | | 1+a | 0 | 1+a | 1 | a |

Show that R is a field. Find the characteristic of this field.

Let us now look at an interesting condition for a ring to be a field

**Theorem 9**

Let R be a ring with identity. Then R is a field if and only if Rand {0} are the only ideals of R.

**Proof**

Let us first assume that R is a field. Let I be an ideal of R. If $I \neq \{0\}$, there exists a non-zero element $x \in I$. As $x \neq 0$ and R is a field, xy = 1 for some $y \in R$. Since $x \in I$ and I is an ideal, $xy \in I$. i.e., $1 \in I$.

Thus, by Theorem 4 of Unit 10, I = R. So, the only ideals of R are {0} and R.

Conversely, assume that Rand {0} are the only ideals of R. Now, let $a \neq 0$ be an element of R. Then you know that the set $Ra = \{ra \mid r \in R\}$ is a non-zero ideal of R. Therefore, Ra = R. Now, $1 \in R = Ra$. Therefore, 1 = ba for some $b \in R$, i.e., $a^{-1}$ exists. Thus, every non-zero element of R has a multiplicative inverse. Therefore, R is a field.

.

This result is very useful. You will be applying it again and again in the rest of the units of this block.

Using Theorem 9, we can obtain some interesting facts about **field homeomorphisms** (i.e., ring homeomorphisms from one field to another). We give them to you in the form of an exercise.

16) Letf: F $\rightarrow$ K be a field homomorphism. Show that either f is the zero map or f is 1-1.

E 17) Let R be a ring isomorphic to a field F. Show that R must be a field.

E 17 again goes to show that isomorphic algebraic structures must be algebraically identical.

Now that we have discussed domains and fields, let us look at certain ideals of a ring, with respect to which the. quotient rings are domains or fields.

## 3.3 Prime and Maximal Ideals

In Z we know that if P is a prime number and p divides the product of the integers a and b, then either p divides a or p divides b. In other words, if ab $\in$ pZ, then either $\in$ pZ or b $\in$ pZ. Because of this property we say that pZ is a prime ideal, a term we will define now.

**Definition**

A proper ideal P of a ring R is called a **prime ideal** of R if whenever ab $\in$ P for a, b$\in$ R, then either a $\in$ P or b $\in$ P.

You can see that {0} is a prime ideal of Z because ab$\in$ {0}$\Rightarrow$ a $\in$ {0} or b$\in$ {0}, where a,b $\in$ Z.

Another example of a prime ideal is

**Examp1e 2**

Let R be an integral domain. Show that I = {(0,x) | x $\in$ R) is a prime ideal of R x R.

**Solution**

Firstly, you know that I is an ideal of R x R. Next, it is a proper ideal since I $\neq$ R x R. Now, let us check if I is a prime ideal or not. For this let $(a_1,b_2)$, $(a_2,b_2)$ $\in$ R x R such that $(a_1,b_2)$, $(a_2,b_2)$ $\in$ I Then $(a_1a_2b_1,b_2)$ = (0,x) for some x $(a_1,b_2)$, $(a_2,b_2)$ $\in$ R $\therefore$ $a_1a_2 = 0$, i.e., at = 0 or $a_2 = 0$,

since R is a domain. Therefore $(a_1,b_1) \in I$ or $(a_1,b_2) \in I$. Thus, I is a prime ideal.

Try the following exercises now. They will help you get used to prime ideals.

E 18) Show that the set $I= \{f \in C[0,l] \mid f(0) = 0\}$ is a prime ideal of C[0,l].

E 19) Show that a ring R with identity is an integral domain if and only if the zero ideal {0} is a prime Ideal of R.

Now we will prove the relationship between integral domains and prime ideals.

**Theorem 10**

An ideal P of a ring R with identity is a prime ideal of R if and only if the quotient ring R/P is an integral domain.

**Proof**

Let us first assume that P is a prime ideal of R. Since R has identity, so has R/P. Now, let a+P and b+P be in R/P such that (a+P) (b+P) = P, the zero element of R/P. Then ab+P = P, i.e., $ab \in P$. As P is a prime ideal of R either $a \in P$ or $b \in P$. So either a+P = P or b+P = P.

Thus, R/P has no zero divisors.

Hence, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let $a,b \in R$ such that $ab \in P$. Then ab + P = P in R/P, i.e., (a+P) (b+P) = P in R/P. As R/P is an integral domain, either a+P = P or b+P = P, i.e., either $a \in P$ or $b \in P$. This shows that P is a prime ideal of R.

Using Theorem 10 and Theorem 1 we can say that an ideal mZ of Z is prime in m is a prime number. Can we generalize this relationship between prime numbers and prime ideals in Z to any integral domain? To answer this let us first try and suitably generalize the concepts of divisibility and prime elements.

**Definition**

In a ring R, we say that an element a **divides** an element b (and denote it by a | b) if b = ra for some $r \in R$. In this case we also say that a is a factor of b, of a is a **divisor** of b.

Thus, $\bar{3}$ divides $\bar{6}$ in $Z_7$, since $\bar{3}.\bar{2} = \bar{6}$.

Now let us see what a prime element is.

**Definition**

A non-zero element p of an integral domain R is called a prime element if

i) p does not have a multiplicative inverse, and

ii) whenever a, b $\in$ R and p | ab, then p | a or p | b.

Can you say what the prime elements of Z are? They are precisely the prime numbers and their negatives.

Now that we know what a prime element is, let us see if we can relate prime ideals and prime elements in an integral domain.

**Theorem 11**

Let R be an integral domain. A non-zero element p $\in$ R is a prime element if and only if Rp is a prime ideal of R.

**Proof**

Let us first assume that p is a prime element in R. Since p does not have a multiplicative inverse, 1 $\notin$ Rp. Thus, Rp is a proper ideal of R. Now let a, b $\in$ R such that ab $\in$ Rp. Then ab = rp for some r $\in$ R.

$\Rightarrow$ p | ab
$\Rightarrow$ p | a or p | b, since p is a prime element
$\Rightarrow$ a = xp or b = xp for some x $\in$ R
$\Rightarrow$ a $\in$ Rp or b $\in$ Rp

Thus ab $\in$ Rp $\Rightarrow$ either a $\in$ Rp or b $\in$ Rp, i.e., Rp is a prime ideal of R.

Conversely, assume that Rp is a prime ideal. Then Rp $\neq$ R. Thus, 1 $\notin$ Rp, and hence, p does not have a multiplicative inverse. Now suppose p divides ab, where a, b $\in$ R. Then ab = rp for some r $\in$ R, i.e., ab $\in$ Rp.

As Rp is a prime ideal, either a $\in$ Rp or b $\in$ Rp. Hence, either p | a or p | b. Thys, p is a prime element in R.

Theorem 11 is very useful for checking whether an element is a prime element or not, or for findings out when a principal ideal is a prime

ideal. For example, now we can use E 19 to say that 0 is a prime element of R iff R is a domain.

Prime ideals have several useful properties. In the following exercises we ask you to prove some of them

E 20) Let f: R ~ S be a ring epimorphism with kernel N. Show that

a) if J is a prime ideal in S, then f (J) is a prime ideal in R.
b) if 1 is a prime ideal in R containing N, then f(l) is a prime ideal in S.
c) the map 0 between the set of prime ideals of R that contain N and the set of all prime ideals of S given by $\phi$ (I) = f(I) is a bijection.

E 21) If II and 12 are ideals of a ring such that neither II ,nor 12 contains the other, then show that the ideal $\bigcap I_1 I_2$ is, not prime.

Now consider the ideal 2Z in Z. Suppose the ideal nZ in Z is such that $2Z \subseteq nZ \subseteq Z$. Then $n \mid 2 \therefore n = \pm 1$ or $n = \pm 2$. $\therefore nZ = Z$ or $nZ = 2Z$.

This shows that no ideal can lie between 2Z and Z. That is, 2Z is maximal among the proper ideals of Z that contain it. So we say that it is a "maximal ideal", Let us define this expression.

**Definition**

A proper ideal M of a ring R is called a maximal ideal if whenever I is an ideal of R such that $M \subseteq I \subseteq R$, then either I = M or 1 = R.

Thus, a proper ideal M is a maximal ideal if there is no proper ideal of R which contains it. An example that comes to mind immediately is the zero ideal in any field F. This is maximal because you know that the only other ideal of F is F. itself.

To generate more examples of maximal ideals, we can use the following characterization of such ideal.

**Theorem 12**

Let R be a ring with identity. An ideal M in R is maximal if and only if R/M is a field

**Proof**

Let us first assume that M is a maximal ideal of R. We want to prove that R/M is a field. For this it is e'1ough to prove that R/M has no non-

zero proper ideals (see theorem 9). So, let 1 be an ideal of R/M. Consider the canonical homomorphism $\eta$: R $\rightarrow$ R/M: $\eta$ (r) = r + M. Then, from Theorem 3 of Unit 11, you know that $\eta^{-1}$ (I) is an ideal of R containing M, the kernel of $\eta$. Since M is a maximal ideal of R, $\eta^{-1}$(I) = M or $\eta^{-1}$ (I) = R. Therefore, I = $\eta(\eta^{-1}$ (I)) is either $\eta$(M) or $\eta$(R), That is, I = { $\bar{0}$ } or I = R/M, where 0 = 0+M = M. Thus, RIM is a field.

Conversely, let M be an ideal of R such that R/M is a field. Then the only ideals of R/M are { $\bar{0}$ } and R/M. Let I be an ideal of R containing M. Then, as above, $\eta$ (I) = { $\bar{0}$ } or, $\eta$(I) = R/M.

$\therefore$ I = $\eta^{-1}$ ($\eta$(I)) is M or R. Therefore, M is a maximal ideal of R.

Now look at the following consequence of Theorem 12 (and a few other theorems too).

**Corollary**

Every, maximal ideal of a ring with identity is a prime ideal.

We ask you to prove it in the following exercise.

E72) Prove the corollary given above.

Now, the corollary is a one-way statement. What about the converse? That is, is every prime ideal maximal? What about the zero ideal in Z? Since Z is a domain but not a field and Z = Z/{0}, Z/{0} is a domain but not a field. Thus, {0} is a prime ideal but not a maximal ideal of Z.

Now let us use Theorem 12 to get some examples of maximal ideals.

**Example 3**

Show that an Idea mZ of Z is maximal iff m is a prime number.

**Solution**

From Theorem 7 you know that $Z_m$ is a field iff m is a prime number. You
Also know that Z/mZ $\tilde{}$ Zm. Thus, by E 17,Z/mZ is a field iff m is prime. Hence, by Theorem 12,mZ is maximal in Z iff m is a prime number.

**Example 4**

Show that $\bar{2}Z_{12}$ is a maximal ideal of $Z_{12}$. Thus by E 23 of Unit 11, we see that $Z_{12}/\bar{2}Z_{12} \simeq (Z/12Z)/(2Z/12Z) \simeq Z/2Z \simeq Z_2$, which is a field. Therefore, $\bar{2}Z_{12} = (\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10})$ is maximal in $Z_{12}$

Now, $\{\bar{0}, \bar{4}, \bar{8}\} = \bar{4}Z_{12} \subset \bar{2}Z_{12} \subset Z_{12}$.
Try the following exercises now

E 23) Show that $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is maximal in $Z_{10}$.

E 24) Use Example 4 of Unit 11 to prove that the ideal $\{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$ is maximal in C[0,1].

So, let us see what we have done in this section. We first introduced you to a special ideal of a ring, called a prime ideal. Its speciality lies in the fact that the quotient ring corresponding to it is an integral domain.

Then we discussed a special kind of prime ideal, i.e., a maximal ideal. Why do we consider such an ideal doubly special? Because, the quotient ring corresponding to it is a field, and a field is a very handy algebraic structure to deal with.

Now, if we restrict our attention to domains, can you think of any other method of obtaining a field from a domain? In the next section we look at such a method.

## 3.4 Field of Quotients

Consider **Z** and **Q**. You know that every element of **Q** is of the form $\frac{a}{b}$, where a $\in$ **Z** and b $\in$ **Z*.** Actually, we can also denote $\frac{a}{b}$ by the ordered pair (a,b) $\in$ **Z** x **Z***. Now, in **Q** we know that $\frac{a}{b} = \frac{c}{d}$ iff ad = bc. Let use put a similar relation on the elements of **Z** x **Z***.

Now, we also know that the operations on **Q** are given by $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{b\,d}$ *and* $\frac{a}{b}\,\frac{c}{d} = \frac{a\,c}{b\,d}$ $\forall$ $\frac{a}{b}\,\frac{c}{d} \in$ **Q**.

Keeping these in mind we can define operations on **Z** x **Z***. Then we can suitably define an equivalence relation on **Z** x **Z*** to get a field isomorphic to **Q**.

We can generalise this procedure to obtain a field from any integral domain. So, take an integral domain R. Let K be the following set of ordered pairs:

$$K = \{(a,b) \mid a,b \in R \text{ and } b \neq 0\}$$

We define a relation ~ in K by

$$(a,b) \sim (c.d) \text{ if } ad = bc.$$

We claim that ~ is an equivalence relation. Let us see if this is so.

i) $(a,b) \sim (a,b)$ $\forall (a,b) \in K$, since R is commutative. Thus, ~ is reflexive.

ii) Let $(a,b), (c.d) \in K$ such that $(a,b) \sim (c.d)$. Then $ad = bc$, i.e., $cb = da$. Therefore, $(c,d) \sim (a,b)$. Thus, ~ is symmetric.

iii) Finally, let $(a,b), (c,d), (u,v) \in K$ such that $(a.b) \sim (c,d)$ and $(c,d) \sim (u,v)$. Then $ad = bc$ and $cv = du$. Therefore, $(ad)\ v = (bc)v = bdu$, i.e., $avd = bud$. Thus, by the cancellation law for multiplication (which is valid for a domain), we get $av = bu$, i.e., $(a,b) \sim (u,v)$. Thus, ~ is transitive.

Hence, ~ is an equivalence relation.

Let us denote tl1eequivalence class that contains (a,b) by [a,b]. Thus, $[a,b] = \{(c,d) \mid c,d \in R, d \neq 0 \text{ and } ad = bc\}$

Let F be the set of all equivalence classes of K with respect to

Let us define + and in F as follows. (Itri1ighthelpyou to keep in mind the rules for adding and multiplying rational numbers.)

$[a,b] + [c,d] = [ad+bc,bd]$ and

$[a,b]\ [c,d] = [ac,bd]$.

Do you think + and are binary operations on F?

Note that $b \neq 0$ and $d \neq 0$ in the integral domain R imply $bd \neq 0$. So, the right-hand sides of the equations given above are well defined

equivalence classes. Thus, the sum and product of two elements in F is again an element in F.

We must make sure that these operations are well defined.

So, let [a,b] = [a´,b´] and [c´,d´] = [c´,d´]. We have to show that [a,b] + [c,d] = [a´,b´] + [c´,d´], i.e:, [ad+bc,bd] = [a´d´+b´c´,b´d´].

Now, (ad+bc)b'd' -(a´d´ + b´c´) bd

= ab´dd´ + cd´bb´- a´bdd´- c´dbb´

= (ab´-a´b)dd´ + (cd´-c´d) bb'

= (0)dd´ + (0)bb´ since (a,b) ~ (a´,b´) and (c,d) ~ (c´,d´).

= 0.

Hence, [ad + bc,bd] = [a´ d´ + b´c´,b´d´], i.e., + is well defined.

Now, let, us show that (a,b] .[c,d] = [a´,b´] . [c´,d´],

i.e., [ac,bd] = [a´c´,b´d´].

Consider (ac) (a´c´,b´d´)

= ab´cd´ - ba´dc´ = ba´cd´ - ba´cd´, since ab´ = ba´ and cd´ = dc´

= 0

Therefore, [ac,bd} = [a´c´,b´d´]. Hence, .is well defined.

We will now prove that F is a field.

i) + is associative : For [a,b], [c,d], [u,v] $\in$ F,
([a,b] + [c,d]) + [u,v] = [ad+bc,bd] + [u,v]
= [(ad+bc)v + ubd, bdv]
= [adv + b(cv+ud), bdv]
= [a,b] + [cv+ud,dv]
= [a,b] + ([c,d] + [u,v})'

ii) +is commuta1ive: For [a,b], [c,d] $\in$ F,
[a,b] + [c,d] = [ad + bc,bd] = [cd + da,db] = [c,d] + [a,b]

iii) [0,1] is the additive identity for F: For [a,b] $\in$ F,
[0,1] + [a.b] = [0.b+l.a, l.b] = [a,b]

iv) The additive inverse of [a,b] $\in$ F is [-a,b]:
[a,b] + [-a,b] = [ab-ab,$b^2$] = [0,$b^2$] = [0,1], since 0.1 = 0.$b^2$,

We would like you to prove the rest of the requirements for F to be a field (see the following exercise).

E 25) Show that, in F is associative, commutative, distributive over +, and [1, 1] is the multiplicative identity for F.

So we have put our heads together and proved that F is a field.

Now, let us define f : R $\rightarrow$ F : f(a) = la. I]. We want to show that f is a homomorphism.

Firstly, for a, b $\in$ R,

f(a+b) = [a+b,l] = [a,1] + [b,1]. , ..

= f(a) + f(b), and

f(ab) = [ab,l] = [a,1]. [b,1] = f(a) .f(b).

Thus, f is a ring homomorphism.

Next, let a,b $\in$ R such that f(a) = f(b). Then [a, 1] = [b,I], i.e., a = b. Therefore, f is 1 – 1.

Thus, f is a homomorphism.

So, 1m f = f(R) is a subring of F which is isomorphic to R.

As you know, isomorphic structures are algebraically identical.

So, we can identify R with f(R), and think of R as a subring of F. Now, any element of F is of the form

[a,b] = [a, 1] [1,b] = [a,1] $[b,1]^{-1}$ = f(a) $f(b)^{-1}$, where b $\neq$ 0. Thus, identifying x $\in$ R with f(x) $\in$ f(R), we can say that any element of. F is of the form $ab^{-1}$, where a,b $\in$ R. b $\neq$ 0.

All that we have discussed in this section adds up to the proof of the following theorem.

**Theorem 13**

Let R be an integral domain. Then R can be embedded in a field F such that every element of F has the form $ab^{-1}$ for a, b $\in$ R, b $\neq$ 0.

The field F whose existence we have just proved is called the **field of quotients** (or the **field of fractions**) of R.

Thus, **Q** is the field of quotients of **Z**. What is the field of quotients of **R**? The following theorem answers this question.

**Theorem 14**

If f : **R** $\rightarrow$ **K** is a homomorphism of an integral domain R into a field K, then there exists a homomorphism

g : F $\rightarrow$ K : g([a,1]) = f(a), where F is the field of quotients of R.

We will not prove this result here, since it is a little technical. But let u~ look at this theorem closely. It says that **the field of quotients of an integral domain** is the **smallest field containing it**. Thus, the field of quotients of any field is the field itself. So, the field of quotients of **R** is **R** and of $\mathbf{Z}_p$ is $\mathbf{Z}_p$, where p is a prime number.

Try these exercises now.

E 26) Is **R** the field of quotients of **Z** + $\sqrt{2}$ **Z**? Or, is it **C**? Or, is it **Q**+ $\sqrt{2}$ **Q**? Why'?

E 27) At what stage of the construction of the field F in Theorem 13 was it crucial to assume that R is a domain?

Let us now wind up this unit with a summary of what we have done in it.

## 5.0 SUMMARY

In this unit we have covered the following points.

- The definition and examples of an integral domain.
- The definition and examples of a field.
- Every field is a domain.
- A finite domain is a field.
- The characteristic of any domain or field is either zero or a prime number.
- The definition and examples of prime and maximal ideals.
- The proof and use of the fact that a proper ideal I of a ring R with identity is prime (or maximal) iff R/I is an integral domain (or a field),
- Every maximal ideal is a prime ideal.

- All element p. of an integral domain R is prime iff the principal ideal pR is a prime ideal or R.
- $Z_n$ is a field iff n is a prime number.
- The construction of the field of quotients of an Integral domain.

**ANSWER TO SELFASSESSMENT EXERCISE**

E1) Let n = mr, where r $\in$ N.

Then $\overline{m}\,\overline{r} = \overline{n} = \overline{0}$ *in* $Z_n$

Since 1 < m < n, $\overline{m} \neq \overline{0}$. Similarly, $\overline{r} \neq \overline{0}$

Thus $\overline{m} \in$ $Z_n$ IS a zero divisor.

E 2) Z has no zero divisors.

E 3) For none since 1 x = x $\neq 0 \; \forall x \neq 0$ in the ring.

E 4) Let b $\neq$ 0 be in R such ab = 0. Then, for any r $\in$ R, (ra)b = 0 Thus, every element of Ra is a zero divisor

E 5) $Z_4$, since 2 is a zero divisor.

2Z, since 1 $\notin$ 2Z.
R x R, since (1,0) is a zero divisor.

{0}, since a domain must be non-zero.

E 6) $x^2$= x $\Rightarrow$ x(x-l) = 0 $\Rightarrow$ x = 0 or x-l = 0

$\Rightarrow$ x = 0 or x = 1.

E 7) Let R be a domain and x $\in$ R be nilpotent. ,
then $x^n$ =.0 .for some n $\in$ N. Since R has no zero divisors, this implies that x = 0.

E 8) We want to show that 2A = $\phi \forall A \subseteq$ X, and that 2 is the least such natural number. Firstly, for any A $\subseteq$ X,
2A = A $\Delta$ A = (A \ A) $\cup$ (A \ A) = $\phi$

Also, since X $\neq \phi$, 1.X $\neq \phi$. Thus, char $\wp$ (X) $\neq$ 1.

$\therefore char \wp$ (X) = 2

E9) Let char (R x R) = n. We know that mr =0 $\forall$ r $\in$ R.

Now, let (r,s) be any element of R x R.

Then m(r,s) = (mr,ms) = (0,0), since r,s $\in$ R.

Thus, n $\leq$ m

On the other hand, if r $\in$ R, then (r,0) $\in$ R x R

$\therefore$ n(r,0) = (0,0).

i.e., (nr,0) = (0,0)

i.e., nr = 0

This is true for any r $\in$ R.

$\therefore$ m $\leq$ n.

Thus, (1) and (2) show that m = n, i.e., char R = char (R X R)

E 10a) By the binomial expansion (E II of Unit 9),

$(a+b)^p = a^p + {}^pC_1\, a^{p-1} b + \ldots\ldots + {}^pC_{p-1}\, ab^{p-1} + b^p$

Since $p \mid {}^pC_n$ $\forall$ n = 1,….., $p^{-1}$, ${}^pC_n x = 0$ $\forall x \in$ R and $\forall$ n = 1,….,$P^{-l}$.

Thus, ${}^pC_1\, a^{p-1} b = 0 = .. = {}^pC_1\, ab^{p-1}$

$\therefore (a+b)^p = a^p + b^p$.

You can similarly show that $(a-b)^p = a^p - b^p$,

b) Let $S = \{a^p \mid a \in R\}$

Firstly, $S \neq \phi$.

Secondly, let $\alpha - \beta$ $(a-b)^p \in S$. Then $\alpha = a^p$, $\beta = b^p$ for some a,b $\in$ R.

Then $\alpha - \beta = (a-b)^p \in S$ and $\alpha\beta = (ab)^p \in S$.

Thus, S is, a subring of R

c) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$,
$\phi(ab) = (ab)P = aPbP = \phi(a)\,\phi(b)$.
Thus, $\phi$ is a ring homomorphism.
$\phi$ is 1-1 because .
$\phi(a) = \phi(b). \Rightarrow a^p = b^p \Rightarrow (a-b)^p = 0$, from (a).
$\Rightarrow$ a-b = 0, since R is without zero divisors.
$\Rightarrow$ a = b.

d) We have to show that if R is finite then 0 is surjective,
Let R have n elements. Since $\phi$ is 1-1, 1m $\phi$ also has n elements.
Also 1m $\phi \subseteq$ R. Thus, Im $\phi$ = R.
Hence, $\phi$ is surjective.

E 11) You Can easily show that f is a ring homomorphism.

Ker f = $\{n \in Z \mid n.1 = 0\}$
= $mZ_4$, since char R = m.

E 1 2) char ($Z_3$ x $Z_4$) = 1.c.m. of char $Z_3$ and char $Z_4$ = 12.

Thus, the characteristic of $Z_3$ x $Z_4$ is neither 0 nor a prime.

Note that $Z_3$ x $Z_4$ is not a domain, since it has several zero divisors.

Now let us see why Theorem 3 is not valid for $Z_3$ x $Z_4$.

Take $(\bar{1},\bar{0}) \in Z_3$ x $Z_4$. Then $3(\bar{1},\bar{0}) = (\bar{0},\bar{0}) \in Z_3$ x $Z_4$

But $3(\bar{1},\bar{0}) \neq (\bar{0},\bar{0})$. Thus, Theorem 3(a) and Theorem 3(c) arc not equivalent in this case

E 13) 2Z since $2 \in 2Z$ is not invertible in 2Z.

$Z_n$ since it is not a domain

Q x Q, since it is not a domain.

E 14) No. For example, Z is a subring of **Q**,**Q** is a field, but **Z** is not.

E 15) From the tables you can see that R is commutative with identity and every non-zero element has an inverse: Thus, R is a field.

Also $2x = 0 \ \forall \ x \in$ Rand $1.x \neq 0$ for some x E R.

Thus, char R = 2.

E 16) Ker I is an ideal of F. Thus, by Theorem 9.

Ker f = {0} or Ker f = F.

If Ker f = {0}, then f is 1-1.

If Ker f = F, then f = 0.

E 17) Let $\phi$ $F \rightarrow$R be an isomorphism. Then $\phi(1)$ is the identity of 1m $\phi$ = R, Also, since F is commutative, so is R. Now, let $\in$ R. r $\neq$ O. Since $\phi$ is onto, $\exists$ a $\in$ F such that $\phi$ (a) = r. Since r $\neq$ 0, 2 $\neq 0$. Since F is a field, $\exists$ b $\in$ F such that lib = 1.

Thus, $\phi$(ab) = $\phi$(1), i.e., r$\phi$(b) = $\phi$(1)i.e., r has a multiplicative inverse.

Thus, R is a field

18) Firstly, 1 is an ideal of C[0,1]

(because f.g.$\in$ I $\Rightarrow$ f-g, $\in$ I, and

T$\in$ C[0.I], f$\in$I $\Rightarrow$Tf$\in$I.)

Secondly, since any non-zero constant function is in

C[0,1] \I. I is a proper ideal.

Finally, let fg $\in$ J. Then f(0) g(0) = 0 in R. Since R is a domain, we must have f(0) = 0 or g(0) = 0, i.e., f $\in$ I or g $\in$ I

Thus, I is a prime idela of C[0,1].

E 19) R is a ring with identity. Thus, we need to show that R is without zero divisor iff {0} is aprime ideal in R.

Now, {0} is a prime ideal in R

iff ab $\in${0} $\Rightarrow$ a $\in$ {0} or b $\in$ {0} for a, b $\in$ R

iff ab = 0 $\Rightarrow$ a = 0 or b = 0

iff R is without zero divisors.

So, we have shown what we wanted to show

E 20) a) From Theorem 3 of Unit 11, you know that $f^{-1}$ (J) is an ideal of R. Since f is syrjective and J $\neq$ S, $f^{-1}$ (J) $\in$ R

Now, let a,b$\in$ R such that ab $\in$ $f^{-1}$ (J)

$\Rightarrow$ f(ab) $\in$ J.

$\Rightarrow$ f(a) f(b) $\in$ J.

$\Rightarrow$ f(a) $\in$ J or f(b) $\in$ J, since J is a prime ideal.

$\Rightarrow$ a $\in$ $f^{-1}$ (J) or b $\in$ $f^{-1}$ (J).

Thus, $f^{-1}$ (J) is a prime ideal in R

b) Firstly, since f is onto, you know that f(I) is an ideal of S. Also, since 1 $\notin$ 1 and $f^{-1}$(f(I)) = I (from Theorem 4 of Unit 11). F(1) $\notin$, f(I). Thus, f(I) $\neq$ S.

Finally, let x,y $\in$ S such that xy $\in$ f(I)

Since S = Im f, $\exists$ a,b $\in$ R such that x = f(a) and y = f(b)

Then f(ab) = xy $\in$ f(I), i.e., ab $\in$ $f^{-1}$(f(I)) = I

$\therefore$ a $\in$ I or b $\in$ I, i.e., x $\in$ f(I) or y $\in$ f(I)

Thus, f(I) is a prime ideal of S.

c) $\phi$ is 1 – 1 : $\phi$ (I) = $\phi$ (J) $\Rightarrow$ f(I) = f(J)

$\Rightarrow$ $f^{1-}$ (f(I)) = $f^{-1}$ (f(I)) I = J.

$\phi$ is onto: Let J be a prime ideal of S. Then $f^{-1-}$ (J) is a prime ideal of R and $\phi$ ($f^{-1}$(J)) = f($f^{-1}$(J)) = J (from Unit 11). Thus, J $\in$ Im $\phi$.

E 21) Let x $\in$ $I_1$\ $I_2$ and y $\in$ $I_2$ \ $I_1$. Then xy $\in$ $I_1$ and xy $\in$ $I_2$, since $I_1$ and $I_2$ are ideals.

$\therefore$ xy $\in$ $I_1$ $\cap$ $I_2$. But x $\notin$ $I_1$ $\cap$ $I_2$ and y $\notin$ $I_1$ $\cap$ $I_2$

Thus, $I_1$ $\cap$ $I_2$ is not prime.

E 22) M is maximal in R
$\Rightarrow$ R/M is a field, by Theorem 12

$\Rightarrow$ R/M is a domain, by Theorem 5

$\Rightarrow$ M is prime in R, by Theorem 10

E 23) $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\} = \bar{2}\,Z_{10}$ and $Z_{10}/\bar{2}\,Z_{10} \simeq Z_2$, a field.

Thus, as in Example 4, $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$ is maximal in $Z_{10}$.

E 24) In Unit 11 we have shown that this ideal in the kernel of the onto homomorphism $\phi$:C[0,1] $\rightarrow$**R**: $\phi$(f) = f $(\frac{1}{2})$.

$\therefore$ C[0,l]/Ker $\phi \simeq$ **R**, a field.

Thus, Ker $\phi$ is maximal in C[0,1].

E 25) You can prove all these properties by using the corresponding properties of R.

E 26) Any element of the field of quotients F is of the form $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, *where* $c+d\sqrt{2} \neq 0$, a,b,c,d $\in$ **Z**.

Now, $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}, = \frac{a+b\sqrt{2}\;c+d\sqrt{2}}{c^2-2d^2} = \left(\frac{ac-2bd}{c^2-2d^2}\right)+\sqrt{2}\left(\frac{bc-ad}{c^2-2d^2}\right) \in \mathbf{Q}+\sqrt{2}\mathbf{Q}$

*Thus,* $F \subseteq \mathbf{Q} + \sqrt{2}\mathbf{Q}$.

Also, any element of $\mathbf{Q} + \sqrt{2}\mathbf{Q}$ *is* $\frac{a}{b}+\sqrt{2}\frac{c}{d}$, a,b,c,d $\in$ **Z**, b $\neq$ 0, d $\neq$ 0

Now $\frac{1}{2}+\sqrt{2}\frac{c}{d} = \frac{ad+bc\sqrt{2}}{b\,d} = \frac{ad+bc\sqrt{2}}{b\,d+0\sqrt{2}}$ with ad, bc, bd $\in$ **Z**

Thus, $\frac{a}{b}+\sqrt{2}\frac{c}{d} \in F$.

Hence, $\mathbf{Q} + \sqrt{2}\mathbf{Q} \subseteq F$

Thus, F = $\mathbf{Q} + \sqrt{2}\mathbf{Q}$

E 27) If R is 'hot a domain, the relation -need not be transitive, and hence, F is not defined.

# UNIT 2 POLYNOMIAL RINGS

## CONTENTS



## 1.0 INTRODUCTION

In the past you must have come across expressions of the form x+1, $x^2$+2x+1, and so on. These are examples of polynomials. You have also dealt with polynomials in the course Linear Algebra. In this unit we will discuss sets whose elements are polynomials of the type $a_0 + a_1 x + \ldots. + a_n x^n$, where $a_0, a_1 \ldots\ldots, a_n$ are elements of a ring R. You will see that this set, denoted by R [x], is a ring also.

You may wonder why we are talking of polynomial rings in a block on, domains and fields. The reason for this is that we want to focus on a particular case, namely, R [x], where R is a domain. This will turnout to be a domain also, with 'a lot of useful properties. In particlI1ar, the ring of polynomials over a field satisfies a division algorithm, which is similar to the one satisfied by Z (see Sec. 1.6.2). We will prove this property and use it to show how many roots any polynomial over a field can have.

In the next two units we will continue to work with polynomials and polynomial rings. So read this unit carefully and make sure that you have achieved the following objectives.

## 2.0 OBJECTIVES

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

- identify polynomials over a given ring
- prove and use the fact that R [x], the set of polynomials over a ring R, is a ring
- relate certain properties of R[x] to those of R
- prove and use the division algorithm for F[x], where F is a field.

## 3.0 MAIN CONTENT

## 3.1 Ring of Polynomials

As we have said above, you may already be familiar with expressions of the type 1 + x, 2 + 3x + 4x $x^5$-l, and so on. These are examples of polynomials over the ring **Z**. Do these examples suggest to you what a polynomial over any ring R is? Let's hope that your definition agrees with the following one.

**Definition**

A **polynomial** over a ring R in the indeterminate x is an expression of the form

$a_0x^0 + a_lx^l + a_2x^2 + ... + a_nx^n$,

Where n is a non-negative integer and $a_0, a_1, ..., a_n \in R$.

While discussing polynomials we will observe the following conventions. We will

i) write $x^0$ as1, so that we will write $a_0$ for $a_0x^0$!lox\),

ii) write $x^1$ as x.

iii) write $x^m$ instead of l.$x^m$ (i.e., when $a_m = 1$).

iv) omit terms of the type $0.x^m$.

Thus, the polynomial $2 + 3x^2 - l.x^3$ is $2x^0 + 0.x^1 + 3x^2 + (-1)x^3$

Henceforth, whenever we use the word polynomial, we will mean a polynomial in the indeterminate x. we will also be using the shorter notation $\sum_{i=0}^{n} a_i x^i$ for the polynomial $a_0 + a_1 x + \ldots + a_n x^n$.

Let us consider a few more basic definitions related to a polynomial.

**Definition**

Let $a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial over a ring R. Each of $a_0$ $a_1, \ldots, a_n$ is a coefficient of this polynomial. If $a_n \neq 0$, we call $a_n$ the leading coefficient of this polynomial.

If $a_1 = 0 = a_2 = \ldots = a_n$, we get the constant polynomial, $a_0$. Thus, every element of R is a constant polynomial.

In particular, the constant polynomial 0 is the **zero polynomial**.

It has no leading coefficient.

Now, there is a natural way of associating a non-negative integer with any non-zero polynomial.

**Definition**

Let $a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial over a ring R, where $a_n \neq 0$. Then we call the integer n the **degree** of this polynomial, and we write.

$$\deg\left(\sum_{i=0}^{n} a_i x^i\right) = n, \text{ if } a_n \neq 0$$

We define the degree of the zero polynomial to be $-\infty$. Thus, **deg 0** = $-\infty$.

Let us consider some examples.

i) $3x^2 + 4x + 5$ is a polynomial of degree 2, whose coefficients belong to the ring of integers **Z**. Its leading coefficient is 3.

ii) $x^2 + 2x^4 + 6x + 8$ is a polynomial of degree 4, with coefficients in **Z** and leading coefficient 2. (Note that this polynomial can be rewritten as $8 + 6x + x^2 + 2x^4$).

iii) Let R be a ring and $r \in R$, $r \neq 0$. Then r is a polynomial of degree 0, with leading coefficient r.

Before giving more examples we would like to set up some notation

**Notation**

We will denote the set of all polynomials over a ring R by R[x]. (Please note the use of the square brackets [ ]. Do not use any other kind of brackets because R [x] and R (x) denote different sets).

$$Thus, R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in R \,\forall\, i = 0,1,\ldots\ldots,\ldots n, \; where en \geq 0, n \in Z \right\}$$

We will also often denote a polynomial $a_0 + a_1 x + \ldots + a_n +^n$ by f(x), p (x), q(x), etc.

Thus, an example of an element from $Z_4$ [x] is f(x) = $\bar{2}\, x^2 + \bar{3}\, x + \bar{1}$

Here deg f(x) = 2, and the leading coefficient of f(x) is $\bar{2}$.

To check your understanding of what we have said so far, you can try these exercises now.

E 1) Identify the polynomials from the following expressions. Which of these are elements of Z[x]?

a) $x^6 + x^5 + x^4 + x^2 + x + 1$

b) $\frac{2}{x^2} + \frac{1}{x} + x + x^2$

c) $\sqrt{3}\, x^2 + \sqrt{2}\, x + \sqrt{5}$

d) $1 + \frac{1}{2} x + \frac{1}{3} x^2 + \frac{1}{4} x^3$

e) $x^{1/2} + 2x^{3/2} + 3 x^{5/2}$

f) -5.

It E 2) Determine the degree and the leading coefficient of the following polynomials in **R**[x].

a) $\sqrt{2}\, x + 7$

b) $1 - 7x^3 + 3x$

c) $1 + x^3 + x^4 + 0.x^5$

d) $\frac{1}{3} x + \frac{1}{5} x^2 + \frac{1}{7} x^3$

e) 0.

Now, for any ring R, we would like to see if we can define operations on the set R [x] so that it becomes a ring. For this purpose we define the operations of addition and multiplication of polynomials.

**Definition**

Let $f(x) = 2_0 + a_1x + .. + a_n x^n$ and $g(x) = b_0 + b_1 x + .. + b_m x^m$ be two polynomials in R[x]. let us assume that $m \geq n$. Then their **sum** f(x) + g(x) is given by $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1) x + .. + (a_n + b_n) x^n + b_{n+1}x^{n+1} + .. + b_m x^m$.

$$= \sum_{i=0}^{m} (a_1 + b_i) x^i, \text{where } a_i = 0 \text{ for } i > n.$$

For example, consider the two polynomials p(x),q(x) in Z[x] given by $p(x) = 1+2x + 3x^2$, $q(x) = 4 + 5x + 7x^3$

Then

$p(x) + q(x) = (1+4) + (2+5)x + (3+0) x^2 + 7x^3 = 5 + 7x + 3X^2 + 7X^3$.

Note that $p(x) + q(x) \in Z[x]$ and that

deg (p(x)+q(x)) = 3 = max(deg p(x), deg q(x)).

From the definition given above, it seems that deg (f(x)+g(x)) = max (deg f (x), deg g (x)). But this is not always the case. For example, consider $p(x) = 1 + x^2$ and $q(x) = 2 + 3x - x^2$ in **Z** [x].

Then $p(x) + q(x) = (1+2) + (0+3)x + (1-1)x^2 = 3 + 3x$.

Here deg (p(x) + q (x)) = 1 < max (deg p(x), deg q(x)).

So, what we can say is that

**deg (f(x) + g(x) ::; Max (deg f(x), deg g(x)**

$\forall$ f(x), g(x) $\in$ R [x].

Now let us define the product of polynomials.

**Definition**

If $f(x) = a_0 + a_ix + ..+ a_n x^n$ and $g(x) = b_0 + b_i x + ..+ b_m x^m$ are two polynomials in R [x], we define their **product** f(x). g(x) by

$f(x) .g(x) = c_0 + c_1x + .. + c_{m+n}x^{m+n}$,

where $c_i = a_ib_0 + a_{i-1} b_1 + ...+ a_0 b_i \ \forall$ i=0,1,...,m + n.

Note that $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$.

As an illustration, let us multiply the following polynomials in $\mathbf{Z}[x]$ :

$p(x) = 1 - x + 2x^3$ , $q(x) = 2 + 5x + 7x^2$.

Here $a_0 = 1$, $a_i = -1$, $a_2 = 0$, $a_3 = 2$, $b_0 = 2$, $b_1 = 5$, $b_2 = 7$.

Thus, $p(x)\, q(x) = \sum_{i=0}^{5} c_i\, x^i$, where

$c_0 = a_0b_0 = 2$,

$c_1 = a_1b_0 + a_0b_1 = 3$,

$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = 2$,

$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = -3$ (since $b_3 = 0$),

$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 10$ (since $a_4 = 0 = b_4$),

$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = 14$ (since $a_5 = 0 = b_5$),
So $p(x), q(x) = 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5$

Note that $p(x), q(x) \in \mathbf{Z}[x]$, and deg $(p(x)\, q(x)) = 5 =$ deg $p(x)$ + deg $q(x)$

As another example, consider

$p(x) = \bar{1} + \bar{2}x, + 2x$, $q(x) = \bar{2} + \bar{3}x^2 \in Z_6[x].2 +$

Then, $p(x).\, q(x) = \bar{2} + \bar{4}x + \bar{3}x^2 + \bar{6}x^3 = \bar{2} + \bar{4}x + \bar{3}x^2$.

Here, deg $(p(x).q(x) = 2 <$ deg $p(x)$ + deg $q(x)$ (since deg $p(x) = 1$, deg $q(x) = 2$).

In the next section we will show you that

**deg (f(x) g(x) ≤ deg f(x) + deg g(x)**

Now try the following exercise. It will give you some practice in adding and multiplying polynomials.

E3) Calculate

a) $(2 + 3x^2 + 4x^3) + (5x + x^3)$ in $\mathbf{Z}$ [x].

b) $((\bar{6} + \bar{2}x^2) + (\bar{1} - \bar{2}x + \bar{5}x^3)$ in $\mathbf{Z}_7$ [x].

c) $(\bar{1} + x)\ (\bar{1} + \bar{2}x + x^2)$ in Z[x].

d) $(\bar{1} + x)\ (\bar{1} + \bar{2}x + x^2)$ in $\mathbf{Z}_3$ [x]

e) $(2 + x + x^2)\ (5x + x^3)$ in $\mathbf{Z}$[x]

By now you must have got used to addition and multiplication of polynomials. We would like to prove that fur any ring R, R [x] is a ring with respect to these operations. For this we must note that by definition, + and. are binary operations over R[x].

Now let us prove the following theorem. It is true for any ring, commutative or not.

**Theorem 1**

If R is a ring, then so is R [x], where x is an indeterminate.

**Proof**

We need to establish the axioms RI -R6 of Unit 9 for (R[x], + ,.).

i) Addition is commutative: We need to show that

p (x) + q (x) = q (x) + p(x) for any p (x) , q (x) $\in$ R [x].

Let $p(x) = a_0 + a_1x + ... + a_nx^n$, and

$q(x) = b_0 + b_1 x + ... + .b_mx^m$ be in R[x].

Then, $p(x) + q(x) = c_0 + c_1 x + ... + c_tx^t$ ,

where $c_i = a_i + b_i$ and t = max(m,n).

Similarly,

$q(x) + p(x) = d_0 + d_1 x + ... + d_s x^s$,

Since addition is commutative in R, $c_1 = d_1\ \forall\ i \geq 0$

So we have

p(x) + q (x) = q(x) + p(x).

ii) Addition is associative: Again, by using the associatively of addition in R, we can show that if p (x),q(x), s(x) $\in$ R[x], then

$\{p(x)+q(x)\} + s(x) = p(x) + (q(x)+ s(x)\}$,

iii) Additive identity : The zero polynomial is the additive identity in R [x]. This is because, for any $p(x) = a_0+ a_1 x + ...+ a_n x^n \in R[x]$,

$0+p(x)= (0 +a_0) + (0 + a_l) x + ...+ (0 + a_n) x^n$

$= a_0 + at\ K + ...+ a_n x^n.$

$= p(x)$

iv) Additive invers: For $p(x) = a_0 + a_1 x +... + a_n x^n \in R[x]$, consider the polynomial

$-p(x) = – a_0 – a_1 x –…– a_n x^n$, $–a_i$ being the additive inverse of at in R. Then

$-p(x) + (-p(x)) = (a_0 –a_0) + (a_1 –a_1) x + ...+ (a_n –a_n)x^n$

$= 0 + 0\ x + 0.x^2 + .., + 0.x^n$
$= 0.$

Therefore, -p (x) is the additive inverse of p (x).

v) Multiplication is associative:

Let $p(x) = a_0 + a_1 x +...+ a_n x^n$,

$q(x) = b_0 + b_1 x + ...+ b_m x^m$,

and $t(x) = d_0 + d_1 x + ...+ d_r x^r$, be in R [x]

Then

$p(x), q(x) = c_0 + c_l x + … + c_s x^s$, where s = m+n and

Therefore,

$\{p(x), q(x)\}\ t(x) = e_0 + e_1 x + … + e_t x^t$,

where t = s + r = m+n+r and

$e_k = c_k d_0 + c_{k-1} d_1 + ...+ c_0 d_k$

$= (a_k b_0 + ...+ a_0 b_k)\, d_0 + (a_{k-1} b_0 + ...+ a_0 b_{k-1}) d_1 + ... + a_0 b_0 d_k,$

Similarly, we can show that the coefficient of $x^k$ (for any $k \geq 0$).in p(x) {q (x) t(x)1}

is $a_k b_0 d_0 + a_{k-1} (b_1 d_0 + b_0 d_l) + ...+ a_0, (b_k d_0 + b_{k-1} d_1 + \ldots + b_0 d_k)$

= e k, by using the properties of + and in R.

Hence, {p(x), q(x)}, t(x) = p(x), {q (x), t (x)}

vi) Multiplication distributes over addition:

Let $p(x) = a_0 + a_l x + ...+ a_n x^n$.

$q(x) = b_0 + b_1 x + ...+ b_m x^m$

and $t(x) = d_0 + d_1 x + \ldots + d, x^r$ be in R[x].

The coefficient of $x^k$ in p (x). (q(x) +t (x)) is

$c_k = a_k (b_0 + d_0) + a_{k-1} (b_1 + d_1) + ... + a_0 (b_k + d_k).$

And the coefficient of $x^k$ in p (x) q (x) + p (x) t(x) is

$(a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k) + (a_k d_0 + a_{k-1} d_1 + \ldots + a_0 d_k),$

$= a_k (b_0 + d_0) + a_{k-1} (b_1 + d_1) + \ldots + a_0 (b_k + d_k) = c_k$

This is true $\forall\ k \geq 0$.

Hence, p (x). {q (x) + t (x)} = p (x): q(x) + p (x) t (x).

Similarly, we can prove that

{q(x) + t(x)}. p(x) = q(x) .p(x) + t(x) p(x)

Thus, R [x] is a ring.

Note that the definitions and theorem in this section are true for any ring. We have not restricted ourselves to commutative rings. But, the case that we are really interested in is when R is a domain. In the next section we will progress, towards this case.

## 3.2 Some Properties of R[x]

In the previous section you must have realised the intimate relationship between the operations on a ring R and the operations on R [x]. The next theorem reinforces this fact.

**Theorem 2**

Let R be a ring.

a) If R is commutative, ~o is R [x].
b) If R has identity, so does R [x].

**Proof**

a) Let $p(x) = a_0 + a_t x + ... + a_n x^n$ and

$q(x) = b_0 + b_1 x + ... + b_m x^m$ be in R [x].

Then $p(x)\, q(x) = c_0 + c_1 x + ... + c_s x^s$, where $s = m + n$ and

$c_k = a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k$

$= b_k a_0 + b_{k-1} a_l + ... + b_1 a_{k-1} + b_0 a_k$, since both addition and multiplication are commutative in R.

= coefficient of $x^k$ in q (x) p(x).

Thus, for every $\geq 0$ the coefficients of xi in p(x) q(x) and q(x) p(x) are equal

Hence, p (x) q(x) = q(x) p(x).

b) We know that R has identity I. We will prove that the constant polynomial 1 is the identity of R [x]. Take any

$p(x) = a_0 + a_1 x + ... + a_n x^n \in R[x]$.

Then I. $p(x) = c_0 + c_1 x + ... + c_n x^n$ (since deg 1 = 0),

where $c_k = a_k 1 + a_{k-1} 0 + a_{k-2} 0 + ... + a_0 0 = a_k$

Thus 1 P (x) = p (x)

Similarly, p (x) l = p(x)
This shows that 1 is the identity of R [xl.

In the following exercise we ask you to check if the converse of Theorem 2 is true.

E 4) If R is a ring such that R [x] is commutative and has identity, then

a) is R commutative?

b) does R have identity

Now let us explicitly state a result which will help in showing us that R is a domain iff R [x] is a domain. This result follows just from the definition of multiplication of polynomial

**Theorem 3**

Let R be a ring and f(x) and g (x) be two non-zero elements of R [x]. Then deg (f (x) g (x) $\leq$ deg f(x) + deg g (x),

with equality if R is an integral domain.

Proof: Let f (x) = $a_0 + a_l x + ...+ a_n x^n$, $a_n \neq 0$,

and g (x) = $b_0 + b_1 x + ... + b_m x^m$, $b_m \neq 0$.

Then deg f(x) = n, deg g (x) = m. We know that

f (x) g (x)= $c_0 + c_1 x + ... + c_{m+n} x^{m+n}$,

where $C_k = a_k b_0 + a_{k-1} b_1 +... + a_0 b_k$.

Since $a_{n+1}$ , $a_{n+2}$,… and $b_{m+1}$ $b_{m+2}$, … are all zero,

$c_{m+n} = a_n b_m$ .

Now, if R is without zero divisors, then $a_n b_m \neq 0$, since $a_n \neq 0$

and $b_m \neq 0$. Thus, in this case,

deg (f(x) g (x) = deg f(x) + deg g (x).

On the other hand, if R has zero divisors, it can happen that $a_n b_m = O$. In this case,

deg (f (x) g (x) < m+n = deg f(x) + deg g(x).

Thus, our theorem is proved.

The following result follows immediately from Theorem 3.

**Theorem 4**

R [x] is an integral domain <=> R is an integral domain.

**Proof**

From Theorem 2 and E 4 we know that R is a commutative ring with identity iff R [x] is a commutative ring with identity. Thus, to prove this theorem we need to prove that R is without zero divisors iff R [x] is without zero divisors.

So let us first assume that R is without zero divisors.

Let $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, and $q(x) = b_0 + b_l x + \ldots + b_m x^m$

be in R [x], where $a_n \neq 0$ and $b_m \neq 0$.

Then, in Theorem 3 we ha'/e seen that deg $(p(x)\, q(x) = m + n \geq 0$.

Thus, $P(x)\, q(x) \neq 0$

Thus, R [x] is without zero divisors.

Conversely, let us assume that R [x] is without zero divisors. Let a and be non-zero elements of R: Then they are non-zero elements of R [x] also. Therefore, $ab \neq 0$. Thus, R is without zero divisors. So, we have proved the theorem.

See if you can solve the following exercises now.

E 5) Which of the following polynomial rings are free from zero divisors?

a) R[x], where $R = \{a + b\sqrt{-5} \mid a,b \in Z\}$
b) $Z_7$ [x]
c) $Z_6$ [x]
d) R[x], where R = C [0,1]

E 6) Let R be a domain. Show that char R = char R [x].

E 7) Let, R and S be commutative rings and f: R $\rightarrow$+ S be a ring homomorphism. Show that the map

$\phi$: R [ x] $\rightarrow$S [x] : $\phi$ ($a_0$+$a_1$x + ...+ $a_n$ $x^n$) = f ($a_0$) + f ($a_l$) x + … +, f($a_n$) $x^n$ is a homomorphism:

Now, you have seen that many properties of the ring R carry over to R [x1. Thus, if F is a field, we 'should expect F[x] to be a field also. But this is not so. F [x] can never be a field

This is because any polynomial of positive degree in F [x] does not have a multiplicative inverse. Let us see why.

Let f (x) $\in$ F [x] and deg f (x) = n > 0. Suppose g (x) $\in$ F [x] such that

f(x) g (x) = 1. Then

0 = deg 1 = deg (f(x) g (x) = deg f(x) + deg g (x), since F [x] is a domain.

= n +deg g (x) $\geq$ n > 0.

We reach a contradiction.

Thus, F [x] cannot be a field.

But there are several very interesting properties of F [x], which are similar to those of Z, the set of integers. In the next section we shall discuss the properties of division in F [x]. You will see how similar they are to the properties of Z that we have discussed in Sec. 1.6,2.

## 3.3 The Division Algorithm

In Sec. l.6.2 we discussed various properties of divisibility in Z. In particular, we proved the division algorithm for integers. We will now do the same for polynomials over a field F.

**Theorem 5 (Division Algorithm)**

Let F be a field. I.-et f(x) and g(x) be two polynomials in F [x], with g(x) $\neq$ 0. Then

a) there exist two polynomials q(x) and r (x) in F [x] such that

f (x) = q (x) g (x) + r (x), where deg r(x) < deg g (x).

b) the polynomials q (x) and r (x) are unique.

**Proof**

a) If, deg f (x) < deg g (x), we can choose q (x) = 0.

Then f, (x) = 0. g(x) + f (x), where deg f(x) < deg g (x).

Now, let us assume that deg f(x) $\geq$ deg g (x).

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $a_n \neq 0$, and
$g(x) = b_0 + b_1 x + \ldots + b_mx^m$, $b_m \neq 0$, with $n \geq m$.

We shall apply the principle of induction (see Sec. 1.6.1) on deg f(x), i.e., n.

If n = 0, then m = 0, since $g(x) \neq 0$. Now

$f(x) = a_0$, $g(x) = b_0$, and hence

$f(x) = (a_0 b_0 + 0 = q(x) g (x) + r (x)$, where $q(x) = a_0b_0^{-1}$ and r(x) = 0.

Thus,

f(x) = q(x) g(x) + r(x), where deg r(x) < deg g(x).

So the algorithm is true when n = 0. Let us assume that the algorithm is valid for all polynomials of degree $\leq$ n -1 and try to establish that it is true for f(x). Consider the polynomial

$f_1 (x) = f(x) a_nb_m^{-1} x^{n-m} g(x)$

$= (a_0 + a_1 x + \ldots + a_nx^n) - (a_nb_m^{-1}b_0x^{n-m} + a_nb_m^{-1}b_1x^{n-m+1} + \ldots + a_nb_mx^n)$

Thus, the coefficient of $x^n$ in $f_l (x)$ is zero; and hence,

deg $f_l(x) \leq$ n–l.

By the induction hypothesis, there exist $q_l (x)$ and r (x) in

F[x] such that $f_l (x) = q_l (x) g(x) + r(x)$, where deg r(x) < deg g(x).

Substituting the value of $f_1(x)$, we get

$f(x) - a_nb_m^{-l} x^{n-m} g(x) = q_1(x) g(x) + r(x)$,

i.e., $f(x) = \{a_nb_m^{-l} x^{n-m} + q_1(x)\} g(x) + r(x)$

$1 = q(x)\, g(x)+r(x)$, where $q(x) = a_n b_m^{-1} x^{n-m}+q_l(x)$
and deg $r(x) <$ deg $g(x)$.

Therefore, the algorithm is true for f(x). and hence, for all polynomials in F[x].

b) Now let us show that q(x) and r(x) are uniquely determined.

If possible, let

$f(x) = q_1(x)\, g(x)+r_1(x)$ where deg $r_l(x) <$deg $g(x)$. and
$f(x) = q_2(x)\, g(x)+r_2(x)$ where deg $r_2(x) <$deg $g(x)$.

Then

$q_1(x)\, g(x)+r_l(x) = q_2(x)\, g(x)+r_2(x)$, so that
$\{q_1(x)-q_2(X)\}\, g(x) = r_2(x)-r_l(x)$ ……(1)

Now if $q_1(x) \neq q_2(x)$ then deg $\{q_1(x) -q_2(x)\} \geq 0$, so that
deg $[\{q_l(x) – q_2(x)\}\, g(x)] \geq$ deg $g(x)$.

On the other hand, deg $\{r_2(x)-r_1(x)\} <$ deg $g(x)$, since
deg $r_2(x) <$deg $g(x)$ and deg $r_1(x) <$ deg $g(x)$.

But this contradicts Equation (1). Hence, Equation (l) will remain valid only if $q_1(x) –q_2(x) = 0$. And then $r_2(x) –r_1(x) = 0$,

i,e., $q_1(x) = q_2(x)$ and $r_l(x) = r_2(x)$.

Thus we have proved the uniqueness of q(x) and r(x) in the expression $f(x) = q(x)\, g(x)+r(x)$.

Here q(x) is called the quotient and r(x) is called the remainder obtained on dividing f(x) by g(x).

Now, what happens if we take g(x) of Theorem 5 to be a linear polynomial? We get the remainder theorem. Before proving it let us set up some notation.

**Notation**

Let R be a ring and $f(x) \in R[x]$.Let
$f(x)=a_0+a_lx+...+a_nr^n \in R$
Then, for all $r \in R$, we define
$f(r) = a_0+a_1r+...+a_nr^n \in R$.

That is, f(r) is the value of f(x) obtained by substituting r for x.

Thus, if $f(x) = 1+x+x^2 \in Z[x]$, then

f(2) = 1+2+4 = 7 and f(0) = 1+0+0 = 1.

Let us now prove the remainder theorem. which is a corollary to the division algorithm.

**Theorem 6 (Remainder Theorem)**

Let F be a field. If $f(x) \in F[x]$ and $b \in F$, then here exists unique polynomial $q(x) \in F[x]$ such that f(x) = (x-b) q(x)+f(b,).

**Proof**

Let g(x) = x-b. Then, applying the division algorithm to f(x) and g(x), we can find unique q(x) and r(x) in F[x], such that
f(x) = q(x) g(x)+r(x)

= q(x) (x-b)+r(x), where deg r(x) < deg g(x) = 1.

Deg r (x) < 1, r (x) is an element of F, say a.

So, f(x) = (x-b) q(x)+a.

Substituting b for x, we get

f(l) = (b-b) q(b) + a

= 0.q(b)+a = a

Thus, a = f(b).

Therefore, f(x) = (x-b) q(x)+f(b).

Note that deg f(x) = deg(x-b)+deg q(x) = 1 +deg q(x).

Therefore, deg q(x) = deg f(x)–l.

Let us apply the division algorithm in a few situations now.

**Example 1**

Express $x^4+x^3+5x^2$ -x as

$(x^2+x+l)$ q(x)+r(x) in Q[x].

**Solution**

We will apply long division of polynomials to solve this problem.

$$
\begin{array}{r}
x^2 + 4 \\
x^2+x+1\overline{)\,x^4+x^3+5x^2-x} \\
\underline{x^4+x^3+x^2} \\
4x^2\backslash_x \\
\underline{4x^2+4x+4} \\
-5x-4
\end{array}
$$

Now, since the degree of the remainder -5x- 4 is less than deg ($x^2$+x+ I), we stop the process, We get

$x^4+x^3+5x^2$ -x = ($x^2$+x+l) ($x^2$+4) -(5x+4).

Here the quotient is $x^2$+4 and the remainder is -(5x+4).

Now you can try some exercises.

E 8) Express f as gp+r, where deg r < deg g, in each of the following cases.

a) f = $x_4$+1, g = $x_3$ in **Q**[x]
b) f = $x^3 + \bar{2}x^2 - x + \bar{1}$ in $\mathbf{Z}_3$[x]
c) f = $x^3 - 1$, g = x – 1 in **R**[x]

E 9) You know that if p,q $\in$ Z, q $\neq$ 0, then $\frac{p}{q}$ can be written as the sum of an integer and a fraction $\frac{m}{q}$ with | m | < | q |. What is the analogous property, fur elements of F[x]?

Now, let us see what happens when the remainder in the expression f = pg+r is zero

## 3.4 Roots of Polynomials

In Sec. 12.4 you have seen when we can say that an element in a ring divides another element. Let us recall the definition in the context of F[x], where F is a field.

**Definition**

Let f(x) and g(x) be in F[x], where F IS a field and g (x) $\neq$ 0. We say that g(x) **divides** f(x)(or g(x) is a **factor** of f(x), or f(x) is **divisible** by g(x) if there-exists q(x) $\in$ F[xl such that

f(x) = q(x) g(x).

We write g(x) j f(x) for 'g(x) divides f(x), and g(x) ~ f(x) for 'g(x) does not divide f(x).

Now, if f(x) $\in$ F[x] and g(x) $\in$ F[x], where g(x) $\neq$ 0, then does Theorem say when g(x) | f(x)? It does, We find that g(x) | f(x) if r(x) = 0 in Theorem 5.

In the fol1owing exercise we make an important, similar statement. You can prove it by applying Theorem 6.

E 10) Let F be a field and f(x) $\in$ F[x] with deg f(x) $\geq$ 1. Let a $\in$ F.

show that f(x) is divisible by x-a iff f(a) = 0.

This exercise leads us to the following definition.

**Definition**

Let F be a field and f(x) $\in$ F[x]. We say that an element a $\in$ F is a root (or zero) of f(x) if f(a) = 0.

For example, 1 is a root of $x^2$-1 $\in$ **R**[x], since $1^2$-1 = 0.

Similarly, - 1 is a root of f(x) = $x^3+x^2+\frac{1}{2}$ x + $\frac{1}{2}$ $\in$ **Q** [x], since- .

f(-1) = 1+1 - $\frac{1}{2}$ + $\frac{1}{2}$ = 0.

Not that, in E 10 you have proved the following criterion for an element to be a root of a polynomial:

Let f be a field and f (x) $\in$ F[x]. Then a $\in$ F is a root of f(x) if and only if (x-a)|f(x).

We can generalize this criterion to define a root of multiplicity m of a polynomial in F[x].

**Definition**

Let F be a field and f(x) $\in$ F[x] We say that **a $\in$ F is a root of multiplicity m** (where) m is a positive integer of

f(x) it $(x-a)^m$ | f(x) but $(x-a)^{m+l}$ x f(1).
For example, 3 is a root of multiplicity 2 of the polynomial $(x-3)^2$ (x+2) **Q**[x]; and (-2) is a root of multiplicity 1 of this polynomial.

Now is it easy to obtain all the roots of a given polynomial? Any linear polynomial ax+b $\in$ F[x] will have only one root namely, $-a^{-l}b$. This is because ax+b = 0 iff $x = -a^{-l}b$.

In the case of a quadratic polynomial $ax^2+bx+c \in F[x]$, you know that its two roots are obtained by applying the quadratic formula.

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

For polynomials of higher degree we may be able to obtain some roots by trial and error. For example, consider $f(X) = x^5-2x+1 \in \mathbf{R}[x]$, Then, we try out x = 1 and find f(1) = 0. So, we find that l is a zero of f(x). But this method doesn't give us all the roots of f(x),.

Now you can try these exercises.

E 11) Find the roots of the following polynomials, along with their multiplicity.

a) $f(x) = \frac{1}{2}x^2 - \frac{1}{2}x + 3 \in \mathbf{Q}[x]$

b) $f(x) = x^2 + x + \bar{1} \in \mathbf{Z}_3[x]$

c) $f(x) = x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} \in \mathbf{Z}_5[x]$

E 12) Let F be a field and a $\in$ F Define a function

$\phi : F[x] \to F: \phi(f(x)) = f(a)$.

This function is the evaluation at a.

Show that

a) $\phi$ is an onto ring homomorphism.

b) $\phi(b) = b \ \forall \ b \in F$.

c) Ker $\phi = \langle x - a \rangle$

So, what does the Fundamental Theorem of Homomorphism say in this case?

As we have just seen; it is not easy to find all the roots of a given polynomial. But we can give a definite result about the number of roots of a polynomial.

**Theorem 7**

Let f(x) be a non-zero polynomial of degree n over a field F. Then f(x) ha: at most n roots in F.

**Proof**

If n = 0, then f(x) is anon-zero constant polynomial.

Thus, it has no roots, and hence, it has at most 0 (= n) roots in F.

So, let us assume that $n \geq 1$. We will use the principle of induction on n. If deg t(x) = 1, then

$f(x) = a_0 + a_1 x$, where $a_0\ a_l \in F$ and $a_l \neq 0$.

So f(x) has only one root, namely, $(-a_1^{-1}\ a_0)$

Now assume that the theorem is true for all polynomials in F[x] of degree < n. We will show that the number of roots of f(x), $\leq$ n.

If f(x) has no root in F, then the number of root of f(x) in F is $0 \leq n$. So, suppose f(x) has a root $a \in F$.

Then f(x) = (x-a) g(x), where deg g(x) = n-l.

Hence, by the induction hypothesis g(x) has at most n-1 roots in F, say $a^l,...,a_{n-1}$ Now,

$a_1$ is a root of g(x) $\Rightarrow$ $g(a_i) = 0 \Rightarrow f(a_i) = (a_i\text{-}a)\ g(a) = 0$

$\Rightarrow$ $a_i$ is it root of(x) $\forall$ i = 1,..., n-l.

Thus, each root of g(x) is It root of f(x).

Now, $b \in F$ is a root off(x) iff f(b) = 0, i.e., iff (b-a) g(b) = 0, i.e., iff b-a = 0 or g(b) = 0, since F is an integral domain. Thus, b is a root of f(x) iff b = a or b is a root of g(x). So, the only roots of f(x) are a and $a_1 \ldots, a_{n-1}$. Thus, f(x) has at the most n roots, and so, the theorem is true for n.

Hence, the theorem is true for all $n \geq 1$.

Using this result we know that, for example, $x^3-1 \in \mathbf{Q}[x]$ can't have more than 3 roots in **Q**.

In Theorem 7 we have not spoken about the roots being distinct. But an obvious corollary of Theorem 7 is that

**if $f(x) \in F[x]$ is of degree n, then f(x) has at most n distinct roots in F.**

We will use this result to prove the following useful theorem.

**Theorem 8**

Let f(x) and g(x) be two non-zero polynomials of degree, n over the field F if there exist n+1 distinct elements $a_1,...,a_{n+1}$ in F such that $f(a_i) = g(a) \ \forall \ i = 1, ..., n+1$, then f(x) = g(x).

**Proof**

Consider the polynomial h(x) = f(x) -g(x)

Then deg $h(x) \leq n$, but it has n+1 distinct roots $a_1,..., a_{n+1}$.

This is impossible, unless h(x) = 0, i.e., f(x) = g(x).

We will now give you an example to show you that Theorem 7 (and hence Theorem 8) need not be true for polynomials over a general ring.

**Example 2**

Prove that $x^3 + \bar{5}\, x \in Z_6\,[x]$ has more roots than its degree. (Note that $Z_6$ is not a field.)

**Solution**

Since the ring is finite, it is easy for us to run through all its elements and check which of them, are roots of

$$f(x) = x^3 + \bar{5}\, x.$$

So, by substitution we find that

$f(0) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{4})$.

In fact, every element of $Z_6$ is a zero of f(x). Thus, f(x) has 6 zeros, while deg f(x) =3.

Try these exercises now.

E 13) Let p be a prime number. Consider $x^{p-1} - \bar{1} \in Z_p[x]$. Use the fact that $Z_p$ is a group of order p to show that every non-zero element of $Z_p$ is a root of $x^{p-1} - \bar{1}$.

Thus, show that $x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) ...(x - \overline{p-1})$.

E 14) The polynomial $x^4 + \bar{4}$ can he factored into, linear factors in $Z_5$ [x]:

Find this factorization.

So far, we have been saying that a polynomial of degree n over F has at most n roots in F. If can happen that the polynomial has no root in F. for example, consider the polynomial $x^2+1 \in R[x]$. From Theorem 7 you know that it can have 2 roots in **R**, at the most. But as you know, this has no roots in **R** (it has two roots, i and – i, in **C**).

We can find many other examples of such polynomials in **R**[x]. We call such polynomials irreducible over **R.** We shall discuss them in detail in the next two units.

## 4.0 CONCLUSION

Polynomial rings are very important class of rings in mathematics. Hardily can we not come across polynomial expressions in our daily mathematical endeavours, since we need to add or subtract two mathematical algebraic expressions from each other. It is required of you to read this unit carefully before you proceed to the next unit.

## 5.0 SUMMARY

In this unit we have covered the following points.

- The definition and examples of polynomials over a ring.
- The ring structure of R[x], where R is a ring.
- R is a commutative ring with identity iff R[x] is a commutative ring with identity.
- R is an integral domain iff R[x] is an integral domain.

- The division algorithm in F[x], where F is a field, which states that if f(x), g(x) $\in$ F[x], g(x) $\neq$ 0, then there exist unique q(x), r(x) $\in$ F[x] with f(x) = q(x) g(x)+r(x) and deg r(x) < deg g(x).
- a $\in$ F is a root of f(x) $\in$ F[x] iff (x-a) | f(x).
- A non-zero polynomial of degree n over a field F can have at the most n roots.

## 6.0 TUTOR-MARKED ASSIGNMENT

1. The polynomials are (a), (c), (d), (f).

   (b) and (e) are not polynomials since they involve negative and fractional powers of x.

   (a) and (t) are in **Z**[x].

2. The degrees are 1,3,4.3, - $\infty$, respectively. The leading coefficients of the first four are $\sqrt{2,}$ = 7, 1, $\frac{1}{7}$, respectively, o has no leading coefficient.

3a. $2+5x+3x^2+(4+1)x^3 = 2+5x+3x^2+5x^3$

b. $(\bar{6}+\bar{1})-\bar{2}x+\bar{2}x^2+\bar{5}x^3=-\bar{2}x+\bar{2}x^2+\bar{5}x^3$, $\sin ce\,\bar{7}=\bar{0}$

c. $1+3x+3x^2+x^3$

d. $\bar{1}+x^3, \sin ce\,\bar{3}=\bar{0}$

e. $10x+5x^2+7x^3+x^4+x^5$

4. Every element of R is an element of R[x]. Therefore multiplication in R is also commutative.
   Also, the identity of R[x] is an element of R, and hence is the identity of R.

5. (a) and (b)

6. We know that R[x] is a domain. Let char R = n. By Theorem 3 of Unit 12 we know, that n is the least positive integer sucl1that n.l = 0. Since 1 is also the identity of R[x], the same theorem of Unit 12 tells us that char R.

7. Let $p(x) = a_0+a_1x+...+a_nx^n$, $q(x) = b_0+b_1x+...+b_mx^m \in R[x]$.

Then $\phi(p(x)+q(x)) = \phi\left(\sum_{i=0}^{t}(a_i+b_i)x^i\right)$, where t = max (m,n)

$$= \sum_{i=0}^{t} f(a_i+b_i)x^i$$

$$= \sum_{i=0}^{t} [f(a_i)+f(b_i)]x^i$$

$$= \sum_{i=0}^{t} f(a_i)x^i + \sum_{i=0}^{t} f(b_i)x^i$$

$= \phi\ (p(x))+\phi\ (q(x))$, since $f(a_i) = 0 = f(b_j)$

Whenever $a_i = 0$, $b_j = 0$.

Also, $\phi\ (p(x)q(x)) = \phi\ (\sum_{i=0}^{m+n} c_ix_i)$, where $c_i = a_ib_0+a_{i-1}b_1+\ldots+a_0b_i$

$$= \sum_{i=0}^{m+n} f(c_i)x^i$$

$$= \sum_{i=0}^{m+n} [f(a_i)f(b_0) + f(a_{i-1})\ f(b_1) +\ldots+(a_0)\ f(b_i)]x^i$$

since f is a ring homomorphism;

$= \phi\ (p(x))\ \phi\ (q(x))$.

Thus, $\phi$ is a ring homomorphism.

8a. $f = x.g+l$, $q = x$, $r = l$

*b*)
$$x+\bar{1}\ \overline{\sqrt{x^3+\bar{2}x^2-x+\bar{1}}}\ \ x^2+x-\bar{2}$$
$$\underline{x^3=x^2}$$
$$x^2-x+\bar{1}$$
$$\underline{x^2+x}$$
$$-\bar{2}x+\bar{1}$$
$$\underline{-\bar{2}x+\bar{1}}$$
$$\bar{3}$$

Thus, f = ($x^2$ + x - $\bar{2}$) g + $\bar{0}$, since $\bar{3}=\bar{0}$.

c) f = ($x^{2+x+1}$)g + 0

9. Let f(x), g(x) $\in$ F[x], with g(x) $\neq$ 0. By Theorem 5, f(x) = g(x) q(x)+r(x) with deg r(x) < deg g(x). Now, this equality is still true if we consider it over the field of fractions of F[x]. Then, we can divide throughout by g(x), and get

$$\frac{f(x)}{g(x)} = q(x)+\frac{r(x)}{g(x)}, \text{ where deg r(x) < deg g(x).}$$

10. By Theorem 6,

f(x) = (x-a) q (x)+f(a)
Thus, f(x) = (x-a) q(x) iff f(a) = 0, i.e.,
(x-a) | f(x) iff f(a) = 0.

11a. By the quadratic formula, the roots are 3 and 2, each with multiplicity 1.

b. $x^2+x+\bar{1}=(x-\bar{1})^2$, since $-\bar{2}=\bar{1}$ in $\mathbf{Z}_3$

Thus, $\bar{1}$ is the only zero, and its multiplicity is 2.

c. By trial, one zero is 1. Now, applying long division, we get $x^4+\bar{2}x^3-\bar{2}x-\bar{1}=(x-\bar{1})(x^3+\bar{3}x^2+\bar{3}x+\bar{1})$ again, by trial and error we find that $x+\bar{1}$ is a factor of thus, $x^4+\bar{2}x^3-\bar{2}x-\bar{1}=(x+\bar{1})^3$

This shows that $\bar{1}$ is a root of multiplicity 1. and $-\bar{1}$ ($=\bar{4}$) is a root of multiplicity 3.

12a. Let $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$.

Then $\phi$ (f(x)+g(x)) = $\phi$ ( $\sum_{i=0}^{t}$ $(a_i+b_i)\, x^i$), where t = max(m,n).

$$= \sum_{i=0}^{t} (a_i + b_i)a^i$$

$$= \sum_{i=0}^{t} a_i a^i + \sum_{i=0}^{t} b_i a^i$$

= f(a)+g(a)

= $\phi$ (f(x))+ $\phi$ (g(x)), and

$$\phi\ (f(x)\ g(x)) = \phi\left(\sum_{i=0}^{m+n} (a_i b_0 + a_{i-1}b_1 + \ldots + a_0 b_i)x^i\right)$$

$$= \sum_{i=0}^{m+n} (a_i b_0 + a_{i-1}b_1 + \ldots + a_0 b_i)a^i$$

= f(a) g(a)

= $\phi$ (f(x)) $\phi$ (g(x)).

Thus, $\phi$ is a homomorphism.

Now, given any element b $\in$ F, $\exists$ the constant polynomial

f(x) $\in$F[x] such that f(a) = b, i.e., (f(x)) = b.

Thus, $\phi$ is surjective.

b) This is what we have shown in the previous two lines.

c) f(x) $\in$ Ker $\phi$ iff $\phi$ (f(x)) = 0 iff f(a) = 0

iff (x-a) | f(x) iff f(x) $\in$ <x-a>

Thus, Ker $\phi$ = <x-a>

The Fundamental Theorem of Homomorphism says that

$F[x]/\langle x-a\rangle \simeq F$.

13. $(Z_p^*,.)$ *is a group and* $o(Z_p^*) = p-1$)

Thus, by E 8 of Unit 4, $x^{p-1} = \bar{1} \forall\ x \in Z_p^*$,

i.e., each of the p-1 elements of $Z_p^*$ is a root of $x^{p-1}-\bar{1}$

Therefore, $(x-\bar{1}) \ldots (x-\overline{p-1}) \mid (x^{p-1}-\bar{1})$.

Since, $x^{p-1}-\bar{1}$ can have at most p-1 rots in $Z_p$, we find that the (p-1) elements of $Z_p^*$ are yjr only rooyd of $x^{p-1}-\bar{1}$ .

Thus, $x^{p-1}-\bar{1} = (x-\bar{1})\ldots(x-\overline{p-1})$.

14. The polynomial $x^4 + \bar{4}$ is the same as $x^4 - \bar{1}$ in $Z_5[x]$,

since $\bar{4} = -\bar{1}$ . Thus, applying the result in E 13, we get,

$x^4 + \bar{4} = (x-\bar{1})(x-\bar{2})(x-\bar{3})(x-\bar{4})$

# UNIT 3 SPECIAL INTEGRAL DOMAINS

## CONTENTS



## 1.0 INTRODUCTION

In this unit we shall look lit three special kinds of integral domains. These domains were mainly studied with a view to develop number theory. Let us say a few introductory sentences about them.

In Unit 6 you saw that the division algorithm holds for F[x] where F is a field. In Unit 1 you saw that it holds for **Z**. Actually, there are lots of other domains for which this algorithm is true. Such integral domains are called Euclidean domains. We shall discuss their properties in Sec. 7.2

In the next section we shall look at some domains which are algebraically very similar to Z. These are the principal ideal domains, so called because every ideal in them is principal.

Finally, we shall discuss domains in which every non-zero non-invertible element can be uniquely factorised in a particular way. Such domains are very appropriately called unique factorisation domains. While discussing them we shall introduce you to irreducible elements of a domain.

While going through the unit you will also see the relationship between Euclidean domains, principal ideal domains and unique factorisation domains.

## 2.0 OBJECTIVES

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

- check whether a function is a Euclidean valuation or not
- identify principal ideal domains
- identify unique factorisation domains
- obtain "the g.c.d of any pair of elements in a unique factorisation domain
- prove and use the relationship between Euclidean domains principal ideal domains and unique factorisation domains.

## 3.0 MAIN CONTENT

### 3.1 Euclidean Domain

In this course you have seen that Z and F[x] satisfy a division algorithm. There are many other domains that have this property. In this section we will introduce you to them and discuss some of their properties. Let us start with a definition.

**Definition**

Let R be an integral domain. We say that a function d: $R \setminus \{0\} \rightarrow$ NU{0} is
A **Euclidean valuation** on R if !.he following conditions are satisfied:

i) $d(a) \leq d(ab) \ \forall \ a, b \in R \setminus \{0\}$, and

ii) for any $a, b \in R, b \neq 0 \ \exists$ q. $r \in R$ such that

$a = bq+r$, where $r = 0$ or $d(r) < d(b)$.

And then R is called a **Euclidean domain.**

Thus, a domain on which we can define a Euclidean valuation is a Euclidean domain,

Let us consider an example.

**Example 1**

Show that Z1S a Euclidean domain.

**Solution**

Define, d: $Z \to N \cup \{0\}$: d(n) = | n |
Then, for any a,b $\in$ Z\{0},

d(ab) = |ab| = |a| |b| $\geq$ |a| (since |b| $\geq$ 1 for b $\neq$ 0)

= d(a),

i.e., d(a) $\leq$ d(ab).

Further, the division algorithm in **Z** (see Sec.l. 6.2) says that if a, b $\in$ Z, b $\neq$ 0, then $\exists$ q, r $\in$ **Z** such that

i.e., a = bq+r,. where r= 0 or 0 < |r| < |b|,

i.e, a = bq+r, where r = 0 or d(r) < d(b).

Hence, d is a Euclidean valuation and **Z** is a Euclidean domain.

For other examples, try the following exercises.

E 1) Let F be a field. Show that F, with the Euclidean valuation d defined by d(a) = 1 $\forall$ a $\in$ F\.{0}, is a Euclidean domain.

E 2) Let F be a field. Define the function

d: F[x] \ {0} $\to$ **N** $\cup$ {0} : d(f(x)) = deg f(x).

Show that d is a Euclidean valuation on F[x], and hence, F[x] is a Euclidean domain.

Let us now discuss .some properties of Euclidean domains. The first property involves the concept of units. So let us define this concept. Note that this definition is valid for any integral domain.

**Definition**

Let R be an integral domain. An element a $\in$ R is called a unit (or an **invertible element**) in R, if we can find an element b $\in$ R, such that ab = 1, i.e., if a has a multiplicative inverse.

For example, both 1 and -1 are units in **Z** since 1.1 = 1 and (-1).(-1) = 1.

**Caution**

Note the difference between **a unit** in R and **the unity** in R. The unity is the identity with respect to multiplication and is certainly a unit. But a ring can have other units too, as you have just seen in the case of **Z**.

Now, can we obtain all the units in a domain? You know that every non-zero element in a field F is invertible. Thus, the set of units of F is F \ {0}. Let us look at some other cases also.

**Example 2**

Obtain all the units in F[x], where F is a field.

**Solution**

Let $f(x) \in F[x]$ be a unit. Then $\exists\ g(x) \in F[x]$ such that $f(x)\,g(x) = 1$. Therefore,

deg (f(x)g(x)):deg (1) = 0, i.e.,

deg f(x)+deg g(x) = 0.

Since deg f(x) and deg g(x) are non-negative integers this equation can hold only if deg f(x) = 0 = deg g(x). Thus, f(x) must be a non-zero constant, i.e. an element of F\ {0}. Thus, the units of F[x] are the non-zero element of F. That is, the units of F and F[x] coincide.

**Example 3**

Find all the units in $R = \{a + b\sqrt{-5} \mid a,b \in \mathbf{Z}\}$.

**Solution**

Let $a+b\sqrt{-5}$ be a unit in R. The there exists

$C+d\sqrt{-5} \in R$ such that

$$(a+b\sqrt{-5})\,(c+d\sqrt{-5}) = 1$$

$\Rightarrow$ $(ac-5bd)+(bc+ad\sqrt{-5}) = 1$

$\Rightarrow$ ac-5bd = 1and bc+ad = 0

$\Rightarrow$ $abc-5b^2d = b$ and bc+ad = 0

⇨ $a(-ad)-5b^2d = b$, substituting be $=-ad$.

⇨ $(a^2+5b^2)d = -b$

So, if $b \neq 0$, then $(a^2+5b^2) \mid b$, which is not possible.

$\therefore b = 0$.

Thus, the only units of R are the invertible elements of **Z**.

We have asked you to find these elements and other units in E 3 below

E 3) Find all the units in

a) **Z,** b) $\mathbf{Z}_6$, c) $\mathbf{Z}+i\mathbf{Z}$.

E 4) Let R be an integral domain. Prove that $u \in R$ is a unit iff

$Ru = R$

Now we are in' a position to discuss some very simple properties of a Euclidean domain.

**Theorem 1**

Let R be a Euclidean domain with Euclidean valuation d. Then, for any $a \in R \setminus \{0\}$, $d(a) = d(1)$ iff a is a unit in R.

**Proof**

Let us first assume that a that $a \in R \setminus \{0\}$ with $d(a) = d(1)$

By the division algorithm in R, $\exists$ $q,r \in R$ such that $1 = aq+r$,

where $r = 0$ or $d(r) < d(a) = d(1)$.

Now, if $r \neq 0$, $d(r) = d(r.1) \geq d(1)$. Thus, d(d) d(1) can't happen.

Conversely, assume that is a unit in R. Let be R such that $ab = 1$. Then $d(a) \leq d(ab) = d(1)$. But we know that $d(a) = d(a.1) \geq d(1)$. So, we must have $d(a) = d(1)$.

Using this theorem, we can immediately solve Example 2 since f(x) is a unit in F[x] iff deg f(x) = deg (1) = 0.

Similarly, Theorem 1 tells us that $n \in \mathbf{Z}$ is a unit in **Z** iff $|n| = |1| = 1$. Thus, the only unit in **Z** are 1 and (-1).

Now let us look at the ideals of a Euclidean domain.

**Theorem 2**

Let R be a Euclidean domain with Euclidean valuation. d. Then every ideal I of R is of the form I = Ra for some $a \in R$.

**Proof**

If $I = \{0\}$, then I = Ra, where a = 0. So let us assume that $I \neq \{0\}$. Then $I\backslash \{0\}$ is non-empty, Consider the set $\{d(a) \mid a \in I\backslash\{0\}\}$. By the well ordering principle (see Sec. 1.6.1) this set has a minimal element. Let this be d(b), where $b \in I.\backslash \{0\}$. We will show that I = Rb.

Since $b \in I$ and I is an ideal of R,

$Rb \subseteq I.$ …….(1)

Now take any $a \in I$. Since $I \subseteq$ Rand R is a Euclidean domain, we can. find $q,r \in R$ such that

a = bq + r, where r = 0 or d(r) < d(b).

Now, $b \in I \Rightarrow bq \in I$. Also, $a \in I$. Therefore, r =a -bq $\in$ I.

But r = 0 or d(r) < d(b). The way we have chosen d(b), d(r) < q(b) is not possible.

Therefore, r = 0, and hence, $a = bq \in Rb$.

Thus, $I \subseteq Rb.$ .....(2)

From (I) and (2) we get

1= Rb.

Thus, every ideal I of a Euclidean domain R with Euclidean valuation d is principal, and is generated by $a \in I$, where d(a) is a minimal element of the set $\{d(x) \mid x \in I \setminus \{0\}\}$.

So, for example, every ideal of **Z** is principal, a fact that you have already proved in Unit 10.

Now try the following exercises involving the ideals of a Euclidean domain.

E 5) Show that every ideal of F[x] is principal, where F is a field.

E 6) Using **Z** as an example show that the set

S = {a $\in$ R \ {0} | d(a) >d(l)} $\cup${0} is not an ideal of the Euclidean domain with Euclidean valuation d.

Theorem 2 leads us to a concept that we shall discuss now.

## 3.2 Principal Ideal Domain (PID)

In the previous section you have proved that every ideal of F[x] is principal, where F is a field. There are several other integral domains, apart from Euclidean domains, which have this property. We give such rings a very appropriate name.

**Definition**

We call an integral domain R a **principal ideal domain** (PID, in short) if every ideal in R is a principal ideal.

Thus, **Z** is a PID. Can you think of another example of a PID? What about **Q** and **Q**[x]? In fact, by Theorem 2 all Euclidean domains are PlDs. But, the converse is not true. That is, every principal Ideal domain is not a Euclidean domain.

For example, the ring of all complex numbers of the form $a+\frac{b}{2}(1+i\sqrt{19})$, where a, b $\in$ Z, is a principal ideal domain, but not it Euclidean domain. The proof of this too technical for this course, so you can take our word for it for the present!

Now let us look at an example of an integral domain that is not a PID.

**Example 4**

Show that Z[x] is not a PID.

**Solution**

You know that **Z**[x] is a domain, since **Z** is one. We will show that all its ideals are not principal. Consider the ideal of Z[x] generated by 2 and

x, i.e., $< 2,x>$. We want to show that $< 2, x > \neq <f(x)>$ for any $f(x) \in \mathbf{Z}[x]$.

On the contrary, suppose that $\exists f(x) \in Z[x]$ such that $<2,x> = <f(x)>$. Clearly, $f(x) \neq 0$. Also, $\exists$ $g(x), h(x) \in \mathbf{Z}[x]$ such that

$2 = f(x)\, g(x)$ and $x = f(x)\, h(x)$.

Thus, deg f(x) + deg g(x) = deg 2 = 0 …… (1)

and deg f(x) + deg h(x) = deg x = 1 …….. (2)

(1) shows that deg h(x) = 0, i.e., $f(x) \in \mathbf{Z}$, say f(x) = n.

Then (2) shows that deg h(x) = 1. Let h(x) = ax+b with $a,b \in \mathbf{Z}$

Then $x = f(x)\, h(x) = n(ax+b)$

Comparing the coefficients on either side of this equation, we see that na = 1 and nb = 0. Thus, n is a unit in **Z**, that is, $n = \pm 1$

Therefore, $1 \in < f(x)> = <x,2>$. Thus, we can write

$1 = x\,(a_0+a_1x^4+a_1x^r) + 2(b_0+b_1x+\ldots+b_sx^s)$, where $a_1,b_j \in Z \,\forall\, I = 0, 1\ldots..r$ and $j = 0, 1,\ldots\ldots,s$

Now, on comparing the constant term on either side we see that $1 = 2b_0$. This can't be true, since 2 is not invertible in **Z**. So we reach a contradiction.

Thus, $<x,2>$ is not a principal ideal.

Thus, $\mathbf{Z}[x]$ is not a P.I.D.

Now, try the following exercise.

E 7) Show that a subring of a PID need not be a PID.

E 8) Will any quotient ring of a PID be a PID? Why?

Remember that a PID must be an integral domain.

We will now discuss some properties of divisibility in PIDs. You may recall from Unit 12 that if R is a ring and $a,b \in R$, with $a,b \neq 0$, then a **divides** b if there exists $c \in R$ such that b = ac.

Now we would like to generalize the definition of some terms that you came across in Unit 1 in the context of **Z**.

**Definition**

Given two elements a and b in a ring R, we say that $c \in R$ is a **common divisor** of a and b if c | a and c | b.

An element $d \in R$ is a **greatest common divisor** (g.c.d. in short) of a, $b \in R$ if

i) d | a and d | b, and

ii) for any common divisor c of a and b, c | d.

We will show you that if the g.c.d of two elements exists, it is unique up to units, i.e., if d and d` are two g.c.ds of a and, then d=ud`, for some unit u. For this we need a result that you can prove in the following exercise.

E 9) Let R be an integral domain. Show that

a) u is a unit in R iff u | 1.
b) for a, $b \in R$, a | b and b | a iff a and b are associates in R.

So now let us prove the following result.

**Theorem 3**

Let R be an integral domain and a, $b \in R$. If a g.c.d of a and b exists, then it is unique up to units.

**Proof**

So, let d and d` be two g.c.ds of a and b. Since d is a common divisor and d` is a g.c.d, we get d | d`. Similarly, we get d` | d. Thus, by E 9 we see that d and d` are associates in R. thus, the g.c.d of a and b is unique up to units.

Theorem 3 allows us to say **the** g.c.d instead of **a** g.c.d. We denote the g.c.d of a and b by **(a,b).** (This notation is also used for elements of R x R. But there should be no cause for confusion. The context will clarify what we are using the notation for).

How to we obtain the g.c.d of two elements in practice? How did we do it in **Z**? we looked at the common factors of the two elements and their

product turned out to be the required g.c.d. We will use the same method in the following example.

**Example 5**

In **Q**[x] find the g.c.d of

$p(x) = x^2+3x - 10$ and

$q(x) = 6x^2 - 10\ x - 4$

**Solution**

By the quadratic formula, we know that the roots of p(x) are 2 and – 5, and the roots of q(x) are 2 and – 1 / 3

Therefore, p(x) = (x-2) (x+5) and q(x) is the product of the common factors of p(x) and q(x), which is (x-2).

Try this exercise now

E 10) Find the g.c.d of

a) $\bar{2}$ and $\bar{6}$ in **Z** / <8>
b) $x^2+8x15$ and $x^2+12x+35$ in **Z**[x].
c) $x^3-2x^2+6x-5$ and $x^2-2x+1$ in **Q**[x].

let us consider the g.c.d of elements in a PID

**Theorem 4**

Let R be a PID and a, b $\in$ R. Then (a,b) exists and is of the form ax+by for some x,y $\in$ R.

**Proof**

Consider the dieal <a,b>. Since R is a PID, this ideal must be principal also. Let d $\in$ R such that <a,b> = <d>. we will show that the g.c.d of a and b is d.

Since a $\in$<d>, d | a, Similarly, d | b.

Now suppose c $\in$ R such that c | a and c | b.

Since d $\in$<a,b>, $\exists$ x, y $\in$ R such that d = ax+by.

Since c | a and c | b, c | (ax+by), i.e., c | d.

Thus, we have shown that d = (a,b), and d = ax+by for some x,y $\in$ R.

The fact that F[x] is a PID gives us the following corollary to Theorem a.

**Corollary**

Let F be a field. Then any two polynomials f(x) and g(x) in F[x] have a g.c.d which is of the form a(x) f(x) + b(x) g(x) for some a(x) $\in$ F[x].

For example, in 10 (c), (x–1) = $\frac{1}{5}(x^3 - 2x^2 + 6x - 5) + \frac{(-x)}{5}(x^2 - 2x + 1)$

Now you can use Theorem 4 to prove the following exercise about **relatively prime** elements in a PID, i.e., pairs of elements whose g.c.d is 1.

E 11) Let R be a PID and a,b,c $\in$ R such that a | bc. Show that if (a,b) = 1, then a | c.

(**Hint**: By Theorem 4, $\exists$ x,y $\in$ R such that ax+by = 1).

Let us now discuss a concept related of a prime element of a domain (see Sec. 12.4).

**Definition**

Let R be an Integral domain. We say that an element x $\in$ R IS **irreducible** if

i) x is not a unit, and

ii) if x = ab with a,b $\in$ R, then a is a unit or b is a unit.

Thus, an element is irreducible if it cannot be factored in a non-trivial way, i.e., its only factors are its associates and the units in the ring.

So, for example, the irreducible elements of **Z** are the prime, numbers and their associates. This means that an element in **Z** is prime iff it is irreducible.

Another domain in which we can find several examples is F[x}, where F is a field. Let us look at the irreducible elements in **E**9(x), i.e., the irreducible polynomials over **R** and **C.** Consider the following important

theorem about polynomials in **C**[x]. You have already come across this in the Linear Algebra course.

**Theorem 5 (Fundamental Theorem of Algebra)**

Any non-constant polynomial in **C**[x] has a rot in C. (In fact, it has all its roots in C).

Does this tell us anything about the irreducible polynomials over C? Yes. In fact, we can also write it as.

**Theorem 5**

A polynomial is irreducible in **C**[x] iff it is linear

**Theorem 6**

Any irreducible polynomial in **R**[x] has degree 1 or degree 2.

We will not prove these results here but we will use them often when discussing polynomials over **R** or **C**. You can use them to solve the following exercise.

E 12) Which of the following polynomials is irreducible? Give reasons for your choice.

a) $x^2-2x+1 \in \mathbf{R}[x]$
b) $x^2+x+1 \in \mathbf{C}[x]$
c) $x-i \in \mathbf{C}[x]$
d) $x^3-3x^2+2x+5 \in \mathbf{R}[x]$

Let us now discuss the relationship betwee9 prime and irreducible elements in a PID.

**Theorem 7**

In a PID an element is prime iff it is irreducible.

**Proof**

Let R be a PID and $x \in R$ be irreducible. Let $x \mid ab$, where $a,b \in R$. Suppose $x \times a$. Then (x,a) = 1, since the only factor of x is itself, up to units. Thus, by E 11, $x \mid b$, Thus, x is prime.
To prove the converse, you must solve the following exercise.

E 13) Let R be a domain and p $\in$ R be a prime element. Show that p is irreducible.

(**Hint:** Suppose P = ab. Then p | ab. If p | a, then show that b must be a unit.)

Now, why do you think we have said that Theorem,7 is true for a PID only? From E 13 you can see that one way is true for any domain. Is the other way true for any domain? That is, is every irreducible element of a domain prime? You will get an answer to this question in Example 6. Just now we will look at some uses of Theorem 7.

Theorem 7 allows us to give a lot of examples of prime elements of F[x]. For example, any linear polynomial over F is irreducible, and hence prime. In the next unit we will particularly consider irreducibility (and hence primness) over **Q**[x]

Now we would like to prove a further analogy between prime elements in a PID and prime numbers, namely, a result analogous to Theorem l0 of Unit For this we will first show a very interesting property of the ideals of a PID. This property called the ascending **chain condition**, says that any increasing chain of ideals in a PID must stop after a finite number of steps.

**Theorem 8**

Let R be a PID and $I_1$,$I_2$……, be an infinite sequence of ideals of R satisfying

$I_1 \subseteq I_2 \subseteq ....$ r an ass(

Then $\exists m \in$ N such that $I_m = I_{m+1} = I_{m+2}$=……

**Proof**

Consider the set I = $I_1 \cup I_2 \cup .... \bigcup_{n=1}^{\infty}$ In. We will prove that .I is Firstly, I $\neq \phi, \sin ce\, I_1 \neq \phi\, and\, I_1 \subseteq I.$

Secondly, if a,b $\in$I, then a $\in$I, and b$\in$ $I_s$ for some r,s $\in$ N.

Assume r $\geq$ s. Then $I_s \subseteq I_r$. Therefore, a,b $\in$ $I_r$, Since $I_r$ is an ideal of R, a-b $\in$ $I_r \subseteq$ I. Thus, a-b $\in$ I $\forall$ a, b $\in$I.

Finally, let x $\in$ R and a $\in$ I. Then a $\in$ $I_r$ for some r $\in$ N.

$\therefore xa \in I_r \subseteq I$. Thus, whenever $x \in R$ and $a \in I$, $xa \in I$.

Thus, I is n ideal of R. Since R is a PID, I = <a> for some $a \in R$. Since $a \in I$, $a \in I_m$ for some $m \in N$.

Then $I \subseteq I_m$. But $I_m \subseteq I$. So we see that $I = I_m$.

Now, $I_m = I_{m+2}$, and so on. Thus, $I_m = I_{m+1} = 1_{m+2} = \ldots$

Now, for a moment let us go back to Sec. 12.4, where we discussed prime ideals. Over there we said that an element $p \in R$ is prime iff $< p >$ is a prime ideal of R. If R is a PID, we shall use Theorem 7 to make a stronger statement.

**Theorem 9**

Let R be a PIP. An ideal $< a >$ is a maximal ideal of R iff a is a prime element of R.

**Proof**

If <a> is a maximal ideal of R, then it is a prime ideal of R. Therefore, a is a prime element of R.

Conversely, let a be prime and let I be an ideal of R such that $< a > \sim I$. Since R is a PID, I = <b> for some b e R. We will show that b is a unit in R; and hence, by E 4, <b>=R, i.e., I = R.

Now, $<a> \subseteq <b> \Rightarrow a = bc$ for some $c \in R$. Since a is irreducible, either is an associate of a or b is a unit in R. But if b is an associate of a, then <b> = <a>, a contradiction. Therefore, b is a unit in R. Therefore, 1= R.

Thus, <a> is a maximal ideal of R.

What Theorem 9 says is ~hat the prime ideals and maximal ideals coincide in a PID.

Try the following exercise now.

E 14) Which of the following ideal are maximal? Give reasons for your choice.

a) $< 5 >$ in Z,
b) $< x^2-1 >$ in Q [
c) $<x^2+x+1 >$ in R[x],
d) $< x >$ in Z[x].

Now, take any integer n. then we can have n = 0, or n = $\pm$ 1, or n has a prime factor. This property of integers is true for the elements of any PID, as you will see now.

**Theorem 10**

Let R be a ID and a be a non-zero non-invertible element of R. then there is some prime element p in R such that p|a.

**Proof**

If a is prime, take p = a. otherwise, we write $a = a_1b_1$, where neither $a_1$ nor $b_1$ is an associate of a. Then $\langle a \rangle \underset{\times}{\subset} \langle a_1 \rangle$. If $a_1$ is prime take $p = a_1$. Otherwise, we can write $a_1 = a_2b_2$, where neither $a_2$ nor $b_2$ is an associate of $a_1$. Then $\langle a_1 \rangle \underset{\times}{\subset} \langle a_2 \rangle$. Continuing in this way we get an increasing chain

$$\langle a \rangle \underset{\times}{\subset} \langle a_1 \rangle \underset{\times}{\subset} \langle a_2 \rangle \underset{\times}{\subset} \ldots$$

By Theorem 8, this chain stops with some $\langle a_n \rangle$. Then $a_n$ with be prime, since it doesn't have any non-trivial factors. Take $p = a_n$, and the theorem is proved.

And now we are in a position to prove that any non-zero non-invertible element of a PID can be uniquely written as a finite product of prime elements (i.e., irreducible elements).

**Theorem 11**

Let R be a PID. Let $a \in R$ such that $a \neq 0$ and a is not a unit. Then $a = p_1p_2\ldots p_r$, where $p_1, p_2, \ldots, p_r$, are prime elements of R.

**Proof**

If a is a prime element, there is nothing to prove. If not, then $p_1 \mid a$ for some prime $p_1$ in R, by Theorem 10. Let $a = p_1a_1$. If $a_1$ is a prime, we are through. Otherwise $p_2|a_1$ for some prime $p_2$ in R. Let $a_1 = p_2a_2$. Then $a = p_1p_2a_2$. If $a_2$ is a prime, we are through. Otherwise we continue the process. Note that since $a_1$ is a non-trivial factor of a, $\langle a \rangle \underset{\times}{\subset} \langle a_1 \rangle$. Similarly, $\langle a_1 \rangle \underset{\times}{\subset} \langle a_2 \rangle$. So, as the process continues we get an increasing chain of ideals,

$$\langle a \rangle \underset{\times}{\subset} \langle a_1 \rangle \underset{\times}{\subset} \langle a_2 \rangle \underset{\times}{\subset}$$

In the PID R. Just as in the proof of Theorem 10, this chain ends at $\langle a_m \rangle$ for some $m \in N$, and $a_m$ is irreducible.

Hence, the process stops after m steps, i.e., we can write $a = p_1p_2\ldots p_m$, where $p_i$ is a prime element of R $\forall$ i = 1,…, m.

Thus, any non-zero non-invertible element in a PID can be factorised into a product of Primes. What is interesting about this factorization is the following result that you have already proved for Z in Unit 1.

**Theorem 12**

Let R. be a PID and $a \neq 0$ be non-invertible in R. Let $a = P_1P_2...P_n = q_1q_2...q_m$, where $P_i$ and $q_j$ are prime elements of R. Then n = m and each $P_i$ is an associate of some $q_j$ for $1 \leq i \leq n$, $1 \leq j \leq m$.

Before going into the proof of this result, we ask you to prove a property of prime elements that you will need in the proof.

E 15) Use induction on n to prove that if p is a prime element in an integral domain Rand if $p|a_1a_2... a_n$ (where $a_1,a_2,\ldots, a_n \in$ R), then $p_i$ for some i= 1,2,...,n.

Now let us start the proof of Theorem 12.

**Proof**

Since $p_1p_2\ldots p_n = q_1q_2\ldots q_m$, $p_1|p_1p_2\ldots q_m$.

Thus, by E 15, $p_1|q_j$ for some j = 1,……,m. By changing the order of the $q_i$, if necessary, we can assume that j = 1, i.e., $p_1 \mid q_1$. Let $q_1 = p_1u_1$. Since $q_1$ is irreducible, $u_1$ must be a unit in R. So $p_1$ and $q_1$ are associates. New we have

$P_1p_2\ldots p_n = (p_1u_1)\, q_2\ldots q_m$

Canceling $p_1$ from both sides, we get

$p_2p_3\ldots p_n = u_1q_2\ldots q_m$.

Now, if m > n, we can apply the same process to $p_2,p_3$, and so on.

Then we will get

$1 = u_1u_2\ldots u_n\, q_{n+1}\ldots qm$.

This shows that $q_{n+1}$ is a unit. But this contradicts the fact that $q_{n+1}$ is irreducible.

Thus, $m \leq n$.

Interchanging the roles of the ps and qs and by using a similar argument, we get $n \leq m$.

Thus, $n = m$.

During the proof we have also shown that each $p_i$ is an associate of some $q_i$, and vice versa.

What Theorem 12 says is that **any two prime factorizations of an element in a PID are identical, apart from the order in which the factors appear and apart from replacement of the factors by their associates.**

Thus, Theorems 11 and 12 say that every non-zero element in a PID R, which is not a unit, can be expressed uniquely (upto associates) as a product of a finite number of prime elements.

For example, $x^2 - 1 \in \mathbf{R}[x]$ can be written as $(x-1)(x+1)$ or $(x+1)(x-1)$ or $[\frac{1}{2}(x+1)][2(x-1)]$ in $\mathbf{R}[x]$.

Now you can try the following exercise.

E 16) Give the prime factorization of $2x^2-3x+1$ in $\mathbf{Q}[x]$ and $\mathbf{Z}_2[x]$.

The property that we have shown for a PID in Theorems 11 and 12 is true for several oilier domains also. Let us discuss such rings now.

## 3.3 Unique Factorisation Domain (UFD)

In this section we shall look at some details of a class of domains that includes PIDs

**Definition**

We call an integral domain **R a Unique Factorisation Domain** (UFD, in short) if every non-zero element-of R which is not a unit in R can be uniquely expressed as a product of a finite number of irreducible: elements of R.

Thus, if R is a UFD and $a \in R$, with $a \neq 0$ and a being non-invertible, then

i) a can be written as a product of a finite number of irreducible elements, and

ii) if $a = p_1p_2\ p_n = q_lq_2\ldots\ q_m$ be two factorisations into irreducible, then n = m and each $p_i$ is am associate of some $q_j$, where $1 \leq I \leq n$, $1 \leq j \leq m$.

Can you think of an example of a UFD? Do Theorem 11 and 12 help? Of course! In them we have proved that **every PID is a UFD.**

Thus, F[x] is a UFD for any field F.

Also, since any Euclidean domain is a PID, it is also a UFD. Of course, in Unit 1 you directly proved that **Z** is a UFD. Why don't you go through that proof and then try and solve the following exercises.

E 17) Directly prove that F[x] is a UFD, for any filed F.

(**Hint**: Suppose you want to factorise f(x). Then use induction on deg f(x).)

E 18) Give two different prime factorisations of 10 in Z:

So you have seen several examples of UFDs. Now we give you an example of a domain which is not a UFD (and hence, neither a PID nor a Euclidean domain).

**Example 6**

Show that $\mathbf{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbf{Z}\}$ is not a UFD.

**Solution**

Let us define a function

$f: \mathbf{Z}[\sqrt{-5}] \rightarrow NU\ \{0\}$ by $f(a+b\sqrt{-5}) = a^2+5b^2$.

This function is the **norm function,** and is usually denoted by N.

You can check that this function has the property that

$f(\alpha\beta) = f(\alpha)\ f(\beta)\ \forall\ \alpha,\beta \in \mathbf{Z}[\sqrt{-5}]$.

Now, 9 has two factorizations in $\mathbf{Z}[\sqrt{-5}]$, namely,

$9 = 3.3 = (2+\sqrt{-5})\,(2-\sqrt{-5})$

In Example 3, you have already shown that the only units of $\mathbf{Z}[\sqrt{-5}]$ are 1 and – 1. Thus, no two of 3, $2+\sqrt{-5}$ and $2 - \sqrt{-5}$ are associates of each other.

Also, each of them is irreducible. For suppose any one of them,

say $2+\sqrt{-5}$, is reducible. Then

$2+\sqrt{-5} = \alpha\beta$ for some non-invertible $\alpha,\beta \in \mathbf{Z}[\sqrt{-5}]$.

Applying the function f we see that

$f(2+\sqrt{-5}) = f(\alpha)\, f(\beta)$,

i.e., $9 = f(\alpha)\, f(\beta)$.

Since $f(\alpha), f(\beta) \in \mathbf{N}$ and $\alpha, \beta$ are not units, the only possibilities are $f(\alpha) = 3 = f(\beta)$.

So, if $\alpha = a+b\sqrt{-5}$, then $a^2+5b^2 = 3$.

But, if $b \neq 0$, then $a^2 + 5b^2 \geq 5$; and if $b = 0$, then $a^2 = 3$ is not possible in $\mathbf{Z}$. So we reach a contradiction. Therefore, our assumption that $2+\sqrt{-5}$ is reducible is wrong. That is, $2+\sqrt{-5}$ is irreducible.

Similarly, we can show that 3 and $2-\sqrt{-5}$ are irreducible. Thus, the factorization of 9 as a product of irreducible elements is not unique. Therefore, $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.

From this example you can also see that an irreducible element need not be a prime element. For example, $2+\sqrt{+5}$ is irreducible and $2+\sqrt{+5} \mid 3.3$, but $2+\sqrt{+5} \chi 3$. Thus, $2+\sqrt{+5}$ is not a prime element.

Now for an exercise

E 19) Give two different factorisations of 6 as a product of irreducible elements in $\mathbf{Z}[\sqrt{+5}]$.

Now let us discuss some properties of a UFO. The first property says that any two elements of a UFD have a g.c.d; and their g;c.d is the

product of all their common factors. Here we will use the fact any element a in a UFD R can be written as

$A = p_1^{r1}p_2^{r2}\ldots p_n^{rn}$

Where the $p_i$s are distinct irreducible elements of R. For example, in **Z**[x] we have $x^3 – x^2–x+1= (x-1)\ (x+1)\ (x–1) = (x–1)^2\ (x+1)$.

So, let us prove the following result.

**Theorem 13**

Any two elements of a UFD have a g.c.d.

**Proof**

Let R be a UFD and $a.b \in R$.

Let $a = p_1^{r1}p_2^{r2}\ldots p_n^{rn}$ and $b = p_1^{S1}p_2^{S2}\ldots p_n^{Sn}$

Where $p_1,p_2,\ldots, p_n$ are distinct irreducible elements of R and $r_i$ and spare non-negative integers $\forall$ i = 1,2,…,n.

(If some $P_i$ does not occur in the factorisation of a, then the corresponding $r_i = 0$ Similarly, if some $p_i$ is not a factor of b, then the corresponding $s_i = 0$. For example, take 20 and 15 in **Z**. Then $20 = 2^2x3^0\ x.5^1$ and $15 = 2^0\ x3^1x.5^1$)

Now, let $t_i = \min (r_i,s_i)\ \forall$ I = 1, 2,….,n.

Then $d = p_1^{t1}p_2^{t2}\ldots p_n^{tn}$ divides a as well as b, since $t_i \leq r_i$ and $t_i \leq s_i\ \forall$ I = 1,2,….,n.

Now, let c | a and c | b. Then every irreducible factor of c must be an irreducible factor of a and of b, because of the unique factorisation property.

Thus, $c = p_1^{m1}p_2^{m2}\ldots p_n^{mn}$ where $m_i \leq r_i$ and $m_i \leq s_i\ \forall$I = 1,2,…,n. Thus, $m_i \leq t_i\ \forall$

Therefore, c | d.

Hence, d = (a,b).

This theorem tells us that the method we used for obtaining the g.c.d in Example 5 and E 10 is correct.

Now, let us go back to Example 6 for a moment. Over there we found a non-UFD in which an irreducible element need not be a prime elemnt. The following result says that this distinction between irreducible and prime elements can only occur in a domain that is not a UFD

**Theorem 14**

Let R be a UFD. An element of R is prime iff it is irreducible.

**Proof**

By EI3 We know that every prime in R is irreducible. So let us prove the converse.

Let a $\in$ R be irreducible and let a | bc, where b,c$\in$ R.

Consider (a,b). Since a is irreducible, (a,b)=1 or. (a.b) = a

If(a,b) = a, a | b.

If (a,b) = 1, then a $\nmid$b. Let bc = ad, where d $\in$ R.

Let b = $p_1^{r1}$ $p_2^{r2}\ldots p_m^{rm}$ and c = $q_1^{S1}q_2^{S2}\ldots q_n^{Sn}$, be irreducible factorizations of b and c. Since bc = ad and a is irreducible, a must be one of the $p_i$s or one of the $q_i$s. Since a$\chi$b, a $\neq$ $p_i$ for any i. Therefore, a = $q_j$ for some j. That is, a|c.

Thus, If (a,b) =1 , then a |c

So, we have shown that a | bc a | b or a | c.

Hence, a is prime.

For the final property of UFDs that we are going to state, let us go back of Example 4 for a moment. Over there we gave you an example of a PID R, for which R [x] if R is a UFD. We state the following result.

**Theorem 15**

Let R be a UFD. Then R[x] is a UFD

We will not prove this result here, even though it is very useful to mathematicians. But let us apply it. Y 011 can use it to solve the following exercises.

E 20) Give an example of a UFD which is not a PID.

E21) If p is an irreducible clement of a UFD R. then is it irreducible in every quotient ring of R?

E 22) Is the quotient ring of a UFD a UFD? Why?

E 23) Is a subring of a UFD a UFD? Why?

Let us wind up this unit now, with a brief description of what we have covered in it.

## 4.0 CONCLUSION

## 5.0 SUMMARY

In this unit we have discussed the following points.

1) The definition and examples of a Euclidean domain.

2) Z, any field and any polynomial ring over a field arc Euclidean domains.

3) Units associates, factors, the g.c.d of two elements, prime elements and irreducible elements in an integral domain.

4) The definition and examples of a principal ideal domain (PID).

5) Every Euclidean domain is a PID, but the converse is not true. Thus, Z. F and F[x] are PIDs for any field F.

6) The g..c.d of any two elements a and b in a PID R exists and is of the form ax+by for some $x,y \in R$.

7) The Fundamental Theorem of Algebra: Any non-constant polynomial over C has all its roots1n C.

8) In a PID every prime ideal is a maximal ideal.

9) The definition and examples of a unique factorisation domain (UFD).

10) Every PID is a UFD, but the converse is not true. Thus Z. F an~ F[x] are UFDs, for any field F

11) In a UFD (and hence, in a PID) an clement is prime iff it is irreducible

12) Any two elements In a UFD have a g.c.d.

13) If Ris a UFD, then so is R [x]

**ANSWER TO SELFASSESSMENT EXERCISE**

1. $d : F \setminus \{0\} \to N \cup \{0\}: d(x) = 1$

For any $a, b \in F \setminus \{0\}$,

$d(ab) = 1 = d(a)$.

$\therefore d(a) = d(ab) \ \forall \ a,b \in F \setminus \{0\}$

Also, for any $a,b \in F, b \neq 0$,

$a = (ab^{-1})b+0$,

So, F trivially satisfies the second condition for a domain to be Euclidean.

Thus, F is a Euclidean domain.

2. In Unit. 13, you have seen that

$\deg (f(x) g(x) = \deg f(x)+\deg g(x) \ \forall \ f(x),g(x) \in F [x] \setminus \{0\}$.

Now, use Theorem 5 of Unit 13, and you will have proved the result.

3a) $m \in \mathbf{Z}$ is a unit iff $\exists \ n \in \mathbf{Z}$ such that $mn = 1$,i.e., iff $m = \pm 1$.

b) Let $\overline{m}\ m \in \mathbf{Z}_6$ be a unit. Then $\exists \ \overline{n} \in \mathbf{Z}_6$ such that $\overline{m}\ \overline{n} = \overline{1}$

Thus, from Sec. 1.6.2 we see that m is a unit if the g.c.d of m and 6 is 1.

$\therefore \ \overline{m} = \overline{1}$ or $\overline{5}$

c) $\mathbf{Z}/5\mathbf{Z}$ is a field. Thus, the units are all its non-zer6 elements.

d) Let a+ib be a unit. Then $\exists$ c+id $\in \mathbf{Z}$+i$\mathbf{Z}$ such that

(a+ib) (c+id) = 1,
$\Rightarrow$ (ac-bc)+(ad+bc)I = 1

$\Rightarrow$ ac-bd = 1 and ad+bc = 0
$\Rightarrow$ b = 0, as in Example 3.
Thus, a+ib = l or-1, using,(a) above.

4. Let $u \in R$ be a unit. Then $\exists\ v \in R$ such that vu = 1. Thus, for any $r \in R$, r = r. 1 = r(vu) = (rv)u $\in$ Ru.

Thus, $R \subseteq Ru$. $\therefore$ R = Ru,

Conversely, let Ru = R. Since $1 \in R$ =.Ru, $\exists\ v \in R$ such that

1 = vu. Thus, u is a unit in R.

5. Apply Theorem 2 to the Euclidean domain F[x].

6. Let R=**Z**. Then S = $\{n \in Z^* \mid |n| > 1\} \cup \{0\}$

Then $2 \in S$, $3 \in S$ but $2-3 \notin S$ since |2-3| = 1.

Thus, S is not even a subring of R,

7. For example, **Z**[x] is a subring of **Q**[x], which is a PID. But **Z**[xl is not a PID.

8. **Z** is it,PID. But **Z**/6**Z** is not even a domain. Thus, it is not a P1D.

9a. u is a unit iff uv = 1 for some $v \in R$ iff u | 1

b. a | b and b | a

=> b = ac and a = bd for some b,d $\in$ R.
=> b = bdc
=> b = 0 or dc = 1

If b = 0, then a = 0, and then a and b are associates.
If $b \neq 0$, then dc = 1. Thus, c is a unit and b = ac.

Therefore, a and bare associates.

Conversely, let a and b be associates in R, say a = bu, where u is a unit in R. then b | a. Also, let $v \in R$ such that uv = 1. Then av = buv = b. Thus, a | b.

10a. $\bar{2}$.

b) $x^2+8x+15 = (x+3)(x+5)$, $x^2+12x+35 = (x+5)(x+7)$

Thus, their g.c.d is x+5

c) $x^3-2x^2+6x-5 = (x-I)(x^2-x+5)$, $x^2-2x+1 ::: (x-1)^2$,

Thus, their g.c.d is x-1.

11. $\exists\ x,y \in R$ such that $ax+by = 1$

Then $c = 1c = (ax+by)\,c = acx+bcy$

Since $a \mid ac$ and $a \mid bc$, $a \mid (acx+bcy)$

12. (c) is, because of Theorem

(a) is not, since it is $(x-1)^2$
(b) is not, because of Theorem 5'.
(d) is not, because of Theorem 6.

13. Let $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. suppose $p \mid a$. Let $a - pc$. Then $p = ab = pcb \Rightarrow p(1-cb) = 0 \Rightarrow 1 - cb = 0$, since R is a domain and $p \neq 0$. Thus, $bc = 1$, i.e., b is a unit. Similarly, you can show that if $p \mid b$, then a is a unit.

So, $p = ab \Rightarrow$ a is a unit or b is a unit, i.e., p is irreducible.

14(a), (c), since 5 and $x^2+x+1$ are irreducible in **Z** and **R**[x], respectively.
(b) is not, using Theorem 9.
(d) is not, since **Z**[x]/ <x> $\underset{\sim}{}$ **Z**, which is not a field.

15. The result is clearly true for n = 1. Assume that it holds for all $m < n$, i.e., whenever $m < n$ and $p \mid a_1 a_2 ... a_m$ then $p \mid a_i$ for some I = 1,2,…,m.

Now let $p \mid a_1 a_2 ... a_n$. Then $p \mid (a_1 a_2 ... a_{n-1})a_n$.

Since p is a prime element, we find that $p \mid a_1 a_2 ... a_{n-1}$ or $p \mid a_n$

If $p \mid a_1 a_2 ... a_{n-1}$, then $p \mid a_i$ for some i = 1,…,n-l by our assumption.

If $p + a_1 \ldots a_{n-1}$, $p \mid a_n$.

Thus, in either case, $p \mid a_i$ for some i = 1,….,

So, our result is true for n.

Hence, it is true $\forall$ n $\in$ N.

16. $2x^2\_3x+1 = (2x-l)\ (x-1)$ in **Q**[x].

In $\mathbf{Z}_2$ [x] the given polynomial is $x+\bar{1}$, since $\bar{2} = \bar{0}$ and $-\bar{3} = \bar{1}$.

This po1ynonlial is linear, and hence, irreducible over $\mathbf{Z}_2$

Thus, its prime factorisation is just $x+\bar{1}$.

17. Let f(x) be a non-zero non-unit in F[x] and let deg f(x) = n.

Then n > 0. We will prove that f(x) can be written as a product of irreducible elements, by induction on n, If n = 1, then f(x) is linear, and hence irreducible.

Now suppose that the result is true for polynomials of degree < n. Now take f(x). If f(x) is irreducible, there is nothing to prove. Otherwise, there is a prime $f_1(x)$ such that $f_1(x) \mid f(x)$. Let $f(x) = f_1(x)g_1(x)$. Note that deg $f_1(x) > 0$.

Hence, deg $g_1(x)$,< deg f(x). If $g_1(x)$ is prime, we are through. Otherwise we can find a prime element $f_2(x)$ such that $g_l(x) = f_2(x)g_2(x)$. Then deg $g_2(x)$ < deg $g_l(x)$. This process must stop after a finite number of steps, since, each time we get polynomials of lower degree. Thus, we shall finally get

$$f(x) = f_1(x)\ f_2(x)\ldots f_m(x),$$

where each $f_1(x)$ is prime in F[x].

Now, to show that the factorization is unique you go along the lines of the proof of Theorem 12. .'

18. $10 = 2 \times 5 = x\ 2.$

19. $6 = 2.3 = (1+\sqrt{-5})\ (1-\sqrt{-5})$

Using the norm function you should check that each of $2,3,1+\sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathbf{Z}\ [\sqrt{-5}\ ]$.

20. **Z**[x].

21. No. For example, x is irreducible in **Z**[x]; but $\bar{x}$ is zero in **Z**[x]/< x > $\underline{\sim}$ **Z**.
22. The quotient ring of a domain need not be a domain. For example, **Z** is a UFD, but **Z**/<4> is not.

Also, even if the quotient ring is a domain, it may not be a UFD. For example, **Z**[ $\sqrt{-5}$ ] $\underline{\sim}$ **Z**[x]/< $x^2+5$ > is not a UFD, while **Z**[x] is

23. No. For example, **Z**[ $\sqrt{-5}$ ] is a subring of **C**, a UFD. But **Z**[ $\sqrt{-5}$ ] is not a UFD.

# UNIT 4 IRREDUCIBILITY AND FIELD EXTENSIONS

## CONTENTS



## 1.0 INTRODUCTION

In the previous unit we discussed various kinds of integral domains, including unique factorization domains. Over there you saw that **Z**[x] and **Q**[x] are UFDs. Thus, the prime and irreducible elements coincide in these rings; In this unit we will give you a method for obtaining the prime (or irreducible) elements of **Z**[x] and **Q**[x]. This is the Eisenstein criterion, which can also be used for obtaining the irreducible elements of any polynomial ring over a UFD.

After this we will introduce you to field extensions and subfields. We will use irreducible polynomials for obtaining field extensions of a field F from F[x]. We will also show you that every field it; a field extension of **Q** or **Z**p for some prime p. Because of this we call Q and the $\mathbf{Z}_p$ S prim fields. We will discuss these fields briefly.

Fig. 1: Evariste Galois (1811 – 1832)

Finally, we wil1.look at finite fields. These fields were introduced by the young French mathematician Evariste Galois (Fig. l) while he was exploring number theory. We will discuss some properties of finite fields which will show us how to classify them.

Before reading this unit we suggest that you go through the definitions of irreducibility from Unit l4. We also suggest that you go through Units 3 and 4 of the Linear Algebra course if you want to understand the proof of Theorem 7 of this unit. We have kept the proof optional. But once you know what a vector space and its basis are, then the proof IS very.

## 2.0 OBJECTIVES

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

- prove and use Eisenstein's criterion for irreducibility in **Z**[x] and **Q**[x]
- obtain field cxten5ionsof a field F from F[x]
- obtain the prime field of any field
- use the fact that finite field F has $p^n$ elements, where char F = p and $\dim_{Z_p} F = n$.

## 3.0 MAIN CONTENT

### 3.1 Irreducibility in Q[x]

In Module 3 Unit 4 we introduced you to irreducibility irredt1clble polynomials in F[x], where F is a field. We also stated the Fundamental Theorem of Algebra, which said that a polynomial over **C** is irreducible iff it is linear. You also learnt that if a polynomial over **R** is irreducible, it must have degree l or degree 2. Thus, anypo1ynomial over **R** of degree more than 1 is reducible. And. using the quadratic formula, we know which quadratic polynomials over **R** are irreducible.

Now let us look at polynomials over **Q**. Again, as for any field F, a linear polynomial over **Q** is irreducible. Also, by using the quadratic formula we can explicitly obtain the roots of any quadratic polynomial over **Q** and hence figure out whether it is irreducible or not. But, can you tell whether $2x^7+3x^5 – 6x^4 + 3x^3 + 12$ is irreducible over **Q** or not? In two seconds we can tell you that it is irreducible, by using the Eisenstein criterion. This criterion was will build up the theory for proving this useful criterion.

Let us start with a definition.

**Definition**

Let $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbf{Z}[x]$. We define the content of f[x] to be the g.c.d of the integers $a_0$, $a_l$,…, an,

We say that f(x) is **primitive** if the content of f(x) is 1

For example, the content of $3x^2 + 6x + 12$ is the g.c.d. of 3,6 and 12, i.e., 3. Thus, this polynomial is not primitive. But $x^5 + 3x^2 + 4x - 5$ is primitive, since the g.c.d of 1,0,0,3,4,-5 is 1.

You may like to try the following exercises now.

E 1) What are the contents of the following polynomials over **Z**?

a) $1 + x + x^2 + x^3 + x^4$

b) $7x^4 - 7$

c) $5(2x^2 - l)(x + 2)$

E 2) Prove that any Polynomial f(x) e **Z**[x] can be written as dg(x), where d is the conter t

We will now prove that the product of primitive polynomials is a primitive polynomial. This result is well known as **Gauss' lemma.**

**Theorem 1**

Let f(x) and g(x) be primitive polynomials. Then so is f(x) g(x).

**Proof**

Let $f(x) = a_0 + a_lx + ... a_nx^n \in \mathbf{Z}[x]$ and

$g(x) = b_0 + b_lx + ... + b_mx^m \in \mathbf{Z}[x]$.where the

g.c.d of $a_0$, $a_1$,…, $a_n$ is 1 and the g.cd of $b_0$ $b_1$,…, $b_m$ is 1. Now

$f(x)\, g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$

where $c_k = a_0b_k + a_lb_{k-1} + ... + a_kb_0$.

To prove the result we shall assume that it is false and then reach a contradiction. So, suppose that f(x) g(x) is not primitive. Then the g.c.d of $c_0$, $c_1$,..., $c_{m+n}$ is greater than 1, and hence some prime p must divide it.

Thus, $p \mid c_i \ \forall\ i = 0, 1,..., m+n$. Since f(x) is primitive, p does not divide some $a_i$. Let r be the least integer such that $p \nmid a_r$. Similarly, let s be the least integer such that $p \nmid b_s$.

Now consider

$c_{r+s} = a_0b_{r+s}+a_lb_{r+s1} + ...+ a_rb_s + ...+a_{r+s}\, b_0$

$= a_rb_s + (a_0b_{r+s} + a_lb_{r+s-l}+ \ldots + a_{r-l}\, b_{s+1} + a_{r+1}b_{s-1}+\ldots+ a_{r+s}b_0)$

By our choice Of r and s, $p \mid a_0,\ldots, p \mid a_1$, $P \mid a_{r-1}$, and $p \mid b_0$, $p \mid b_l,\ldots, p \mid b_{s-l}$. Also $p \mid c_{r+s}$

Therefore, $p \mid c_{r+s} - (a_0b_{r+s} +... + a_{r-1}\, b_{s+1} + a_{r+1}\, b_{s-l}+ ...+ a_{r+s}b_0)$

i.e., $p \mid a_r\, b_s$

$\Rightarrow p \mid a_r$ or $p \mid b_s$ since p is a prime.

But $p \nmid ar$ and $p \nmid b_s$. So we reach a contradiction. Therefore, our supposition is false. That is, our theorem is true.

Let us shift our attention to polynomials over Q now.

Consider any polynomial over **Q**, say $f(x) = \frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}$. If we take the kcm of all the denominators, i.e., of 2,5, 1 and 3, i.e., 30 and multiply f(x) by it what do we get?

$30f(x) = 45x^3 + 6x^2 + 90x + 10 \in \mathbf{Z}[x]$

Using the same process, we can multiply any $f(x) \in \mathbf{Q}[x]$ by a suitable integer d so that $df(x) \in \mathbf{Z}[x]$. We will use this fact while relating irreducibility in **Q**[x] with irreducibility in **Z**[x].

**Theorem 2**

If $f(x) \in \mathbf{Z}[x]$ is irreducible in **Z**[x], then it is irreducible in **Q**[x].

**Proof**

Let us suppose that f(x) is not irreducible over **Q**[x]. Then we should reach a contradiction. So let f(x) = g(x) h(x) in **Q**[x], where neither g(x) nor h(x) is a unit, i.e., deg g(x) > 0, deg h(x) > 0. Since $g(x) \in \mathbf{Q}[x]$, $\exists\ m \in \mathbf{Z}$ such that $mg(x) \in \mathbf{Z}[x]$. Similarly, $\exists\ n \in \mathbf{Z}$ such that $nh(x) \in \mathbf{Z}[x]$.

Then,

$mnf(x) = mg(x)\, nh(x)$ ……(1)

Now, let us use E2. By E2, $f(x) = rf_1(x)$, $mg(x) = sg_1(x)$, $nh(x) = th_1(x)$, where r, s and t are the contents of f(x), mg (x) and nh (x) and $f_1(x)$, $g_1(x)$, $h_1(x)$ are primitive polynomials of positive degree.

Thus, (1) gives us

$Mnrf_1(x) = stg_1(x)\, h_1(x)$ ……(2)

Since $g_1(x)$ and $h_1(x)$ are primitive, Theorem 1 says that $g_1(x)\, h_1(x)$ is primitive. Thus, the content of the right hand side polynomial in (2) is st. But the content of the left hand side polynomial in (2) is mnr. Thus. (2) says that mnr = st.

Hence, using the cancellation law in (2), we get $f_1(x) = g_1(x)\, h_1(x)$.

Therefore, $f(x) = rf_1(x) = (rg_1(x))\, h_1(x)$ in $\mathbf{Z}[x]$, where neither $rg_1(x)$ nor $h_1(x)$ is a unit. This contradicts the fact that f(x) is irreducible in $\mathbf{Z}[x]$.

Thus, our supposition is false. Hence, f(x) must be irreducible in $\mathbf{Q}[x]$.

What this result says is that to check irreducibility of a polynomial in $\mathbf{Q}[x]$, it is enough to check it in $\mathbf{Z}[x]$. And. for checking it in $\mathbf{Z}[x]$ we have the terrific Eisenstein's criterion that we mentioned at the beginning of this section.

**Theorem 3 (Eisenstein's Criterion)**

Let $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbf{Z}[x]$ Suppose that for some prime number p,

i) $f \nmid a_n$,

ii) $p \mid a_0$ $p \mid a_1, \ldots, p \mid a_{n-1}$, and

iii) $p^2 \nmid a_0$

Then f(x) is irreducible in $\mathbf{Z}[x]$ (and hence in $\mathbf{Q}[x]$)

**Proof**

Can you guess our method of proof? By contradiction, once again! So suppose f(x) is reducible in $\mathbf{Z}[x]$.

Let $f(x) = g(x)\, h(x)$,

Where $g(x) = b_0 + b_1 x + ... + b_m x^m$, $m > 0$ and

$h(x) = c_0 + c_1 x + \ldots + c_r x^r$, $r > 0$.

Then $n = \deg f = \deg g + \deg h = m + r$, and

$a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0 \; \forall \; k = 0, 1 \ldots, n$.

Now $a_0 = b_0 c_0$. We know that $p \mid a_0$. Thus, $p \mid b_0 c_0 \therefore p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, p cannot divide both $b_0$ and $c_0$. Let us suppose that $p \mid b_0$ and $p \nmid c_0$.

Now let us look at $a_n = b_m c_r$. Since $p \nmid a_n$, we see that $p \nmid b_m$ and $p \nmid c_r$. Thus, we see that for some I, $p \nmid b_i$. Let k be the least integer such that $p \nmid b_k$. Note that $0 < k \leq m < n$.

Therefore, $p \mid a_k$.

Now, $a_k = (b_0 c_k + \ldots + b_{k-1} c_1) + b_k c_0$.

Since $p \mid a_k$ and $p \mid b_0, \ldots, p \mid b_{k-1}$, we see that $p \mid a_k - (b_0 c_k + \ldots + b_{k-1} c_1)$, i.e., $p \mid b_k c_0$. But $p \nmid c_0$. So we reach a contradiction.

Thus, $f(x)$ must be irreducible in $\mathbf{Z}[x]$.

Let us illustrate the use of this criterion.

**Example 1**

Is $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ irreducible in $\mathbf{Q}[x]$?

**Solution**

By looking at the coefficients we see that the prime number 3 satisfies the conditions given in Eisenstein's criterion. Therefore, the given polynomial is irreducible in Q[x]

**Example 2**

Let p be a prime number. Is $Q[x]/\langle x^3 - p \rangle$ a field?

**Solution**

From Unit 14 you know that for any field F, if f(x) is irreducible in F[x], then $\langle f(x) \rangle$ is a maximal ideal of F[x].

Now, by Eisenstein's criterion, $x^3 - p$ is irreducible since p satisfies the conditions given in Theorem 3. Therefore, $\langle x^3 - p \rangle$ is a maximal Ideal of **Q**[x].

From Unit 12 you also know that if R is a ring, and M is a maximal ideal of **R**. then **R/M** is a field.

Thus, $\mathbf{Q}[x] / \langle x^3 - p \rangle$ is a field.

In this example we have brought out an important fact. We ask you to prove it in the following exercise.

E 3) For any $n \in N$ and prime number p, show that $x^n - p$ is irreducible over **Q**[x].note that this shows us that we can obtain irreducible polynomials of any degree over **Q**[x].

Now let us look at another example of an irreducible polynomial. While solving this we will show you how Theorem 3 can be used indirectly.

**Example 3**

Let p be a prime number. Show that

$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible in **Z**[x]. f(x) is called the **pth cyclotomic polynomial.**

**Solution**

To start with we would like you to note that f(x) = g(x) h(x) in **Z**[x] iff f(x+1) = g(x+1) h(x+1) in **Z**[x]. Thus, f(x) is irreducible in **Z**[x] iff f(x+1) is irreducible in **Z**[x].

Now, $f(x) = \dfrac{x^p - 1}{x - 1}$

$\therefore\ f(x+1) = \dfrac{x+1^p - 1}{x}$

$= \dfrac{1}{x}(x^p + {}^pC_1\, x^{p-1} + \ldots + {}^pC_{p-1}\, x + 1 - 1)$, (by the binomial theorem)

$= x^{p-1} + px^{p-2} + {}^pC_2 x^{p-3} + \ldots + {}^pC_{p-2}\, x + p.$

Now apply Eisenstein's criterion taking p as the prime. We find that f(x+1) is irreducible. Therefore, f(x) is irreducible.

You can try these exercises now.

E 4) If $a_0 + a_1x + \ldots + a_n x^n \in \mathbf{Z}[x]$ is irreducible in $\mathbf{Q}[x]$, can you always find a prime p that satisfies the conditions (i), (ii) and (iii) of Theorem 3?

E 5) Which of the following elements of $\mathbf{Z}[x]$ are irreducible over $\mathbf{Q}$?

a) $x^2$-12 ..

b) $8x^3 + 6x^2 - 9x + 24$ .

c) $5x + 1$

E 6) Let p be a prime integer. Let a be a non-zero non-unit square-free integer, i.e., $b^2 \not| a$ for any $b \in \mathbf{Z}$. Show that $\mathbf{Z}[x]/\langle x^p+a\rangle$ is an integral domain.

E 7) Show that $x^P + \bar{a} \in \mathbf{Z}$plx] is not irreducible for any it" E Zp' (**Hint:** Does E 13 of Unit 13 help?)

So far we have used the fact that if f(x) E Z[x] IS irreducible over. Z. then it is also irreducible over **Q**, Do you think we can have a similar relationship between irreducibility in **Q**[x] and R[x]? To answer this consider $f(x) = x^2 - 2$. This is irreducible in **Q**[x], but $f(x) = (x - \sqrt{2})$ $(x + \sqrt{2})$ in **R**[x]. Thus, we cannot extend irreducibility over **Q** to irreducibility over **R**.

But we can generalise the fact that irreducibility in **Z**[x] implies irreducibility in Q[x]. This is not only true for **Z** and **Q**; it is true for any UFD R and its field of quotients F (see Sec. 12.5). Let us state this relationship explicitly.

**Theorem 4**

Let R be a UFD with field of quotients F.

i) If $f(x) \in \mathbf{R}[x]$ is an irreducible primitive polynomial, then it is also irreducible in F[x].

ii) (**Eisenstein's Criterion**) Let $f(x) = a_0 + a_1x + \ldots + a_n x^n \in R[x]$ and $p \in R$ be a prime element such that $p \nmid a_n$, $p^2 \nmid a_0$ and $p \mid a_i$ for $0 \leq i < n$. Then f(x) is irreducible in F[x].

The proof of this result is on the same lines as that of Theorems 2 and 3. We will not be doing it here. But if you are interested, you should try and prove the result yourself.

Now, we have already pointed out that if F is a field and f(x) is irreducible over F, then $F[x]/\langle f(x)\rangle$ is a field. How is this field related to F? That is part of what we will discuss in the next section.

## 3.2 Field Extensions

In this section we shall discuss subfields and field extensions. To start with let us define these terms. By now the definition may be quite obvious to you.

**Definition**

A non-empty subset S of a field F is caned a **subfield** of F if it is a field with respect to the operations on F. If $S \neq F$, then S is called a **proper subfield** of F.

A field K is called a **field extension** of F if F is a subfield of K. Thus, **Q** is a subfield of **R** and **R** is a field extension of **Q**. Similarly, **C** is a field extension of **Q** as well as of **R**.

Note that a non-empty subset S of a field F is a subfield of F iff

i) S is a subgroup of (F,+), and .
ii) The 'set of all non-zero elements of S forms a subgroup of the group of non-zero elements of F under multiplication.

Thus, by Theorem 1 of Unit 3, we have the following theorem.

**Theorem 5**

A non-empty subset S of a field F is a subfield of F if and only if

i) $a \in S, b \in S \Rightarrow a-b \in S$, and

ii) $a \in S, b \in S, b \neq 0\ ab^{-1} \in S$.

Why don't you use Theorem 5 to do the following exercise now.

E 8) Show that

a) **Q** + i**Q** is a subfield of **C**

b) **Z** + $\sqrt{2}$ **Z** is not a subfield or **R**.

Now, let us look at a particular field extension of a field F. Since F[x] is an integral domain, we can obtain its field of quotients (see Module 3 Unit 2). We denote this field by F(x). Then F is a subfield of F(x). Thus, F(x) is a field extension of F. Its elements are expressions of the form $\frac{f(x)}{g(x)}$, where f(x), g(x) ∈ F[x} and g(x) ≠ o.

There is another way of obtaining a field extension of a field F from F[x]. We can look at quotient rings of F[x] by its maximal ideals. You know that an ideal is maximal in F[x] iff it is generated by an irreducible polynomial over F. So, F[x]/<f(x), 1s a field iff f(x) is irreducible over F.

Now, given any f(x) ∈ F[x], such that deg f(x) > 0, we will show that there is a field monomorphism from F into F[x]/<f(x). This will show that F[x)/<f(x» contains an isomorphic copy of F; and hence, we can say that it contains F.

So, let us define $\phi$: F→ F[x]/<f(x)>: $\phi$(a) = a + <f(x)».

Then, $\phi$ (a+b) = $\phi$ (a) + $\phi$ (b), and

$\phi$ (ab) = $\phi$ (a) $\phi$ (b)

Thus, $\phi$ is a ring homomorphism.

What is Ker $\phi$ ?).

Ker $\phi$ = {a ∈ F | a + <f(x)> = <f(x)>}

= {a ∈ F | a + ∈ <f(x)>}

= {a ∈ F | f(x) | a}

= {0}, since deg f > 0 and deg a ≤ 0.

Thus, $\phi$ is 1-1, and hence an inclusion.

Hence, F is embedded in F[x]/<f(x)>

Thus, if f(x) is irreducible in F[x], then F[x]/<f(x)> is a field extension of F.

Now for a related exercise!

E 9) Which of the following rings are field extension of **Q**?

a) **Q**[x]/$<x^3 + 10>$,
b) **R**[x]/$<x^2 + 2>$,
c) **Q**,
d) **Q**[x]/$<x^2-5x + 6>$.

Well, we have looked at field extensions of any field F. Now let us look at certain fields, one of which F will be an extension of.

### 3.2.1 Prime Fields

Let us consider any field F. Can we say anything about what its subfields look like? Yes, we can say something about one of its subfields. Let us prove this very startling and useful fact. Before goi1lg into the proof we suggest that you do a quick revision of Theorems 3. 4 al1d 8 of Unit 12. Well, here's the result.

**Theorem 6**

Every field contains a subfield isomorphic to Q or to $Z_p$, for some prime number p.

**Proof**

Let F be a field. Define a function

f : **Z** $\rightarrow$ F : f(n) = n.1 = 1 + 1 + … + 1 (n times).

In E 11) of Module 3 Unit 2 you have shown that f is a ring homomorphism and Ker f = p**Z**, where p is the characteristic of F.

New, from Theorem 8 of Unit 12 you know that char F = 0 or char F = p, a prime. So let us look at these two cases separately.

**Case 1**

(Char F – 0): In this case f is one-one, $\therefore$ **Z** = f(**Z**). Thus, f(**Z**) is an integral domain contained in the field F. Since F is a field, it will also contain the field of quotients of f(**Z**). This will be isomorphic to the field

of quotients of **Z**, i.e., **Q**. Thus, F has a subfield which is isomorphic to **Q**.

**Case 2**

(Char F = p, for some prime p) :

Since,p1s a prime number, **Z**/p**Z** is a field.

Also, by applying the Fundamental Theorem of Homomorphism to f, we get **Z**/p**Z** $\underset{\sim}{}$ f(Z).

Thus, f(Z) is isomorphic to **Z**p and is contained in F. Hence, F has subfield isomorphic to **Z**p.

Let us reword Theorem 6 slightly. What it says is that :

**Let F be a field.**

i) If char F = 0, then F has a subfield isomorphic to Q.
ii) If char F = p, then F has a subfield isomorphic to $Z_p$.

Because of this property of **Q** and $\mathbf{Z}_p$ (where p is a prime number) we call these fields **prime fields.**

Thus, the prime fields are **Q**, $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ etc.

We call the subfield isomorphic to a prime field (obtained in Theorem 6), the **prime subfield** of the given field.

Now, suppose a field F is an extension of a field K. Are the prime subfields of K and F isomorphic or not? To' answer this let us look at char K and char F. We want to know if char K = char F or not. Since F ~s a field extension of K, the unity of F and K is the same, namely, 1. Therefore, the least positive integer "such that n.l = 0 is the same for F as well as K. Thus, char K = char-F. Therefore, the prime subfields of K and F are isomorphic.

So, now can you do the following exercises?

E 10) Show that the smallest subfield of any field is its prime subfield.

E 11) Let F be a field which has no proper subfields. Show that F is isomorphic to a prime field.

E 12) Obtain the prime subfields of **R**, **Z**s and the field given in E 15 of Unit 12.

E 13) Show that given any field, if we know its characteristic then we can obtain its prime subfield and vice versa.

A very important fact brought out by E 10 and E 11 is that: **a field is a prime field iff it has no proper subfields.**

Now let us look at certain field extensions of the fields $\mathbf{Z}_p$.

You have dealt a lot with the finite fields $\mathbf{Z}_p$. Now we will look at field extensions of these fields. You know that any finite F has characteristic p, for some prime p. And then F is an extension of $\mathbf{Z}_p$. Suppose F contains q elements. Then q must be a power of p. That is what we will prove now.

**Theorem 7**

Let F be a finite field having q elements and characteristic p. Then $q = p^n$, for some positive integer n.

The proof of this result uses the concepts of a vector space and its basis. These are discussed in Block 1 of the Linear Algebra course. So, if you want to go through the proof, we suggest that you quickly revise Units 3 and 4 of the Linear Algebra course. If you are not interested in the proof, you may skip it.

**Proof of Theorem 7**

Since char F = p, F has a prime subfield which is isomorphic to **Z**p. We lose nothing if we assume 1hat the prime subfield is $Z_p$. We first show that F is a vector space over **Z**p with finite dimension.

Recall that a set V is a vector space over a field K if

i) we can define a binary operation + on V such that (V. +) is an abelian group,

ii) we can define a 'scalar multiplication' : K x V $\rightarrow$ V such that $\forall$ a, b $\in$ K and v,w $\in$ V,

a. (v + w) = a.v +a.w

(a + b). v =a.v + b.v

(ab). V = a. (b. v)

1.v = v.
Now, we know1hat (P, +)'is an abelian group. We also know that the multiplication in F will satisfy till the conditions that the scalar multiplication should satisfy. Thus, F is a vector space over $\mathbf{Z}_p$. Since F is a finite field, it has a finite dimension over $\mathbf{Z}_p$. Let $\dim_{Z_p} F = n$. Then we can find $a_l,\ldots, a_n \in F$ such that

$F = Z_p a_l + Z_p a_2 + ..+ Z_p a_n$.

We will show that F has $p^n$ elements.

Now, any element of F is of the form

$b_l a_l + b_2 a_2 +...+ b_n a_n$, where $b_l,..., b_n \in \mathbf{Z}_p$,

Now, since $o(\mathbf{Z}_p) = p$, $b_1$ can be anyone of its p elements.

Similarly, each of $b_2$, $b_3$, ... , $b_n$ has p choices. And, corresponding to each of these choices we get a distinct element of F. Thus, the number of elements in F is p x p x…xp(n times) = $p^n$.

The utility of this result is something similar to that of Lagrange's theorem. Using this result we know that, for instance, no field of order 26 exists. But does a field of order 25 exist? Does Theorem 7 answer this question? It only says that a field of order 25 **can** exist. But it does not say that it **does** exist. The following exciting result, the proof of which is beyond the scope of this course, gives us the required answer. This result was obtained by the American mathematician E.H. Moore in 1893.

**Theorem 8**

For any prime number p and $n \in \mathbf{N}$, there exists Ii field with $p^n$ elements. Moreover, any two finite fields having the same number of elements, are isomorphic

Now, you call utilize your knowledge of finite fields to solve tile following exercises. The first exercise is a generalization of E 13 in Unit 13.

E 14. Let F be a finite field with $p^n$ elements. Show that $a^{p^n} = a \; \forall \in F$. And hence,

show that $x^{p^n} - x = \prod_{a_i \in F} (x-a_i)$.

(**Hint**: Note that $(F \setminus \{0\},.)$ is a group of order $p^n$-l.)

E 15) Let F be a finite field with $p^n$ elements. Define $f : F \to F : f(a) = a^P$. Show that f is anutomorphism of F of order n; i e., f is an isomorphism such that f n = I, and $f^r \neq 1$ for r < n.

E 16) Let F be a field such that $a \in F$ iff a is a root of $x^{27} - x \in$

a) What is char F?
b) Is $\mathbf{Z} \subset$ F?
c) Is $\mathbf{Q} \subseteq$ F?
d) Is F $\subseteq \mathbf{Q}$? Why?

E 11) Any two infinite fields are isomorphic. True or false? Why? Remember that isomorphic structures must have the same algebraic properties.

We close our discussion on field extensions now. Let us go over the points that we have covered in this unit.

## 4.0 CONCLUSION

## 5.0 SUMMARY

We have discussed the following points in this unit.

1) Gauss; lemma, i.e., the 'product of primitive polynomials is primitive.

2) Eisenstein's criterion for polynomials over **Z** and **Q**. This states that if $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbf{Z}[x]$ and there is a prime $p \in Z$ such that

i) $p \mid a_i \; \forall \; i = 0,.1, ..., n-1.$

ii) $p + a_n$, and

iii) $p^2 + a_0$,

then f(x) is irreducible over **Z** (and hence over **Q**)

3) For any $n \in N$, we can obtain an irreducible polynomial over **Q** of degree n.

4) Definitions and examples of subfields and field extensions

5) Different ways of obtaining field extensions of a field F from F[x].

6) Every field contains a subfield isomorphic to a prime field.

The prime fields are **Q** or $\mathbf{Z}_p$, for some prime p.

7) The number of elements in a finite field F is $p^n$, where char F = p and $\dim_{Z_p} F = n$.

8) Given a prime number p and $n \in \mathbf{N}$, there exists a field containing $p^n$ elements. Any two finite fields with the same number of elements are isomorphic.

9) If F is a finite field with $p^n$ elements, then $xp^n - x$ is a product of $p^n$ linear polynomials over F.

Now we have reached the end of this unit as well as this course. We hope that we have been able to give you a basic understanding of the nature of groups, rings and fields. We also hope that you enjoyed going through this course.

**ANSWER TO SELFASSESSMENT EXERCISE**

1. a) 1, b) 7, c) 5

2. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and let the content of f(x) be d. Let $a_i = db_i \; \forall \; I = 0, 1, \ldots, n$. Then the g.c.d of $b_0, b_1, \ldots, b_n$ is 1. Thus, $g(x) = b_0 + b_1 x + \ldots + b_n x^n$ is primitive. Also, $f(x) = db_0 + db_1 x + \ldots + db_n x^n = d(b_0 + b_1 x + \ldots + b_n x^n) = d\, g(x)$.

3. $f(x) = x^n - P = a_0 + a_l x + \ldots + a_n x^n$,

where $a_0 = p$, $a_l = 0 = \ldots = a_{n-1}$, $a_n = 1$

Thus, $p \mid a_i \; \forall \; i = 0, 1, \ldots, n - l$, $p^2 \nmid a_0$, $p \nmid a_n$.

So, by the Eisenstein criterion, f(x) is' irreducible over **Q**.

4. Not necessarily

For example, there is no p that satisfies the conditions for f(x) in Example 3.

5. All of them (a) and (b), because of Eisenstein's criterion; and (c), because any linear polynomial is irreducible.

6. Since $a \neq 0, \pm 1, \exists$ a prime q such that q | a. Also $q^2 \nmid a$, since a is square-free. Then, using q as the prime, we can apply Eisenstein's criterion to find that $x^p + a$ is irreducible in **Z**[x]. Thus, it is a prime element of **Z**[x]. Hence, $\langle x^P + a \rangle$ is a prime ideal of **Z**[x].

   Hence the result,

7. By E 13 of Unit 13 we know that $\bar{a}^P = \bar{a} \forall \bar{a} \in$ **Z**p. Now consider

   $X^p + \bar{a} \in \mathbf{Z}_p[x]$

   $\overline{p-a}$ is a zero of this polynomial, since

   $(\overline{p-a})^p + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0}\ Z_p$

Thus, $x_P + \bar{a}$ is reducible over **Z**p.

8a. **Q** + i**Q** is a non-empty subset of **C**.

Now, let a + ib and c + id be in **Q**+i**Q**.

Then (a + ib) -(c + id) = (a – c) + i (b – d) $\in$ **Q** + i**Q**.

Further, let $c + id \neq 0$, so that $c^2 + d^2 \neq 0$.

Then $(c + id)^{-1} = \dfrac{c - id}{c^2 + d^2}$

Thus, $(a + ib)(c + id)\text{-}1 = (a + ib)\dfrac{(c - id)}{c^2 + d^2}$

$$= \frac{(ac - bd)}{c^2 + d^2} + i\frac{(ac - bd)}{c^2 + d^2} \in \mathbf{Q} + i\,\mathbf{Q}.$$

Thus, **Q** + i**Q** is a subfield of **C.**

b.) $2 \in \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ but $2^{-1} \notin \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$. Therefore,

$\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ is not a field, and hence not a subfield of R.

9. (a), (b) and (c).

10. Let F be a field ~d K be a subfield of F. Then, .we have just seen that both K and F have isomorphic prime subfields.

Thus, K contains the prime subfield of F.

Thus, we have shown that every subfield of F must contain its prime subfields. Hence, this is the smallest subfield of F.

11. F must contain a prime subfield. But it contains no proper subfield be its own prime subfield. That is, F must be isomorphic to a prime field.

12. $\mathbf{Q}$, $\mathbf{Z}_5$, $\mathbf{Z}_2$, since their characteristic's are 0,5 and 2, respectively.

13. F be a field. Firstly, let us assume that char F = p is known. Then, by Theorem 6, we know the prime subfield of F. Conversely, let K be the prime subfield of F. Then we know char K, and as shown before E 10, char F = char K. So we know char F.

14. Since (F\{0},.) is a group of order $p^n$ -1, $a^{P^n}$ -1 = 1

$\forall$ a $\in$ F \ {0}.

$\therefore$ $ap^n$ = a $\forall$ a $\in$ F\ {0}. Also $0^{P^n} = 0$.

Thus, $a^{P^n}$ = a $\forall$ a $\in$ F.

Now, $x^{P^n}$ - x $\in$ F[x] can have at the most $p^n$ roots in F (by Theorem 7 of Unit 13).

Also, each of the $p^n$ elements of F is a root. Thus, these are all the roots of $x^{P^n}$ - x.

$\therefore$ $x^{P^n}$ - x = $\prod_{a_i \in F} (x - a_i)$

15. f(a + b) = (a + b)P = $a^P + b^P$ (using E 10 of Unit 12)

= f(a) + f(b).

f(ab) = (ah)P = $a^P\, b^P$ = f(a) f(b).

f is 1 – 1, by E 10(c) of Unit 12.

Hence, Im f has the same number of elements as the domain of f, i.e., F. Further, Im $1 \subseteq F \ \therefore$ Im f = F, i.e., f is onto.

Hence, f is an automorphism.

Now, $f^n(a) = [f(a)]^n = (a^p)^n = a^{P^n} = a \ \forall \ a \in F.$

$\therefore \ f^n = I.$

Also, for r < n, $f^r(a) = a^{P^r}$

Now, we can't have $a^{P^r} = a \ \forall \ a \in F$, because this would mean that the polynomial $x^{P^n} - x \in F[x]$ has more than pf roots. This would contradict Theorem 7 of Unit 13. Thus, $f^r(a) \neq a$ for some $a \in F. \ \therefore f^r \neq I$ if r < n.

Hence, o(f) = n.

E 16) $a \in F$ iff $a^{27} = a$, i.e., $a^{33} = a$

a) Char F = 3.
b) No, since char $Z_2 \neq$ char F.
c) No.
e) No, since $F \subseteq \mathbf{Q} \Rightarrow$ char F = char **Q** = 0.

17. False.

For example, **Q** and **R** are both infinite, but **Q** has no proper subfields, while **R** does. Thus, **Q** and **R** are not isomorphic.

## 6.0 TUTOR-MARKED ASSIGNMENT

## 7.0 REFERENCES/FURTHER READING